KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | April 2014

Identity Provisioning

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

by **Martin Kuppinger**
mk@kuppingercole.com
April 2014

Leadership Compass
Identity Provisioning
By KuppingerCole

Content

Content Tables

Table of Figures

Related Research:

Leadership Compass: Enterprise Key and Certificate Management - 70961

Product Report: CA IdentityMinder™ - 70914

Advisory Note: Entitlement & Access Governance - 71109

Product Report: CrossIdeas IDEAS - 70620

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Vendor Report: Courion Corporation - 70920

Executive View: EmpowerID 2013 - 70005

Leadership Compass: Access Management and Federation - 70790

Executive View: Omada Identity Management Suite - 70783

Product Report: Beta Systems Software AG SAM Enterprise Identity Manager - 70274

Vendor Report: Atos DirX - 70741

Leadership Compass: Access Governance - 70735

Vendor Report: NetIQ – the complete portfolio - 70624

Leadership Compass: Identity Provisioning - 70151

Advisory Note: Access Governance Architectures - 71039

Advisory Note: The Open API Economy - 70352

Product Report: DirX Identity 8.2 - 70134

Scenario: Understanding Identity and Access Management - 70173

Vendor Report: Avatier - 70144

Product Report: Evidian Identity & Access Manager 9 – 70130

1. Management Summary

Identity Provisioning is still one of the core segments of the overall IAM market. Identity Provisioning is about provisioning identities and access entitlements to target systems. This includes creating and managing accounts in such connected target systems and associating the accounts with groups, roles, and other types of administrative entities to enable entitlements and authorizations in the target systems. Identity Provisioning is about automating these tasks, based on defined processes for creating, updating, and deleting identity-related information in the target systems. Despite the emergence of Access Governance solutions that focus on Access Request Management, Access Recertification, or SoD (Segregation of Duties) management and enforcement, Identity Provisioning remains a core capability of IAM infrastructures.

While there are a number of vendors that have integrated their Access Governance and Identity Provisioning offerings into a single solution, others continue offering separate products. More importantly, we see a large number of customers that either look for Access Governance or Identity Provisioning, but not for combined offerings. There are various reasons to do so, for instance when it is about updating just a part of the IAM infrastructure, adding Access Governance to an existing Identity Provisioning solution, or starting with the Identity Provisioning foundation before the next step of Access Governance is done.

KuppingerCole therefore has Leadership Compass documents for both **Identity Provisioning – 70151** and **Access Governance – 70735**. Both Leadership Compass documents also provide a view on the "other side". This Leadership Compass on Identity Provisioning provides ratings for both the pure-play Identity Provisioning applications as well as for added Access Governance capabilities, while the Leadership Compass on Access Governance also looks at the integrated provisioning capabilities. This allows customers to make a decision based on their current and future requirements, not based on the theoretical market segment definition of an analyst company.

Given that Identity Provisioning is one of the oldest IAM areas and remains a core segment of the IAM market, it comes as no surprise that this segment is more crowded with vendors than any other IAM market segment. This Leadership Compass provides an overview and analysis of all relevant players in the Identity Provisioning market segment and their products.

It shows that there are several established vendors with mature solutions, but also some very interesting smaller or regional vendors with a good potential for growth and for delivering what customers require.

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. However, this Leadership Compass will help identifying those vendors and products at which customers should take a closer look.

Fig. 1: Overall Leaders in the Identity Provisioning market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at the Overall Leaders, we see most of the expected large players in front. This is partially based on the fact that they are Market Leaders, which goes into the Overall Leadership rating. We see Oracle, Dell, NetIQ, IBM, SailPoint, and CA Technologies competing head-to-head in that rating. Microsoft is not an overall leader due to their rather weak position in the Innovation Leadership and Product Leadership ratings. SAP declined to participate in this edition of the KuppingerCole Leadership Compass Identity Provisioning due to upcoming major release changes.

The Overall Leadership rating also shows a number of other vendors in the Leaders category. These include Atos, Beta Systems, Courion, EmpowerID, Hitachi ID, and Omada. All of these vendors can build on a strong customer base and mature products. We also see Avatier, ForgeRock and Fischer as vendors being very close to entering the Overall Leadership section.

Behind these leading companies, we see a large number of other vendors in the Challenger segment. Especially the ones further to the right in that segment definitely are interesting candidates for any long list in product decisions, namely CrossIdeas, Evidian and Microsoft.

The other vendors also have interesting offerings but commonly lack in one or another area, such as market presence, customer base, and ecosystem, or are specialized vendors such as Ilex that provide solutions taking a somewhat different approach to Identity Provisioning. All of these vendors might be a fit for customers, depending on their specific needs such as looking for Open Source products or regional players.

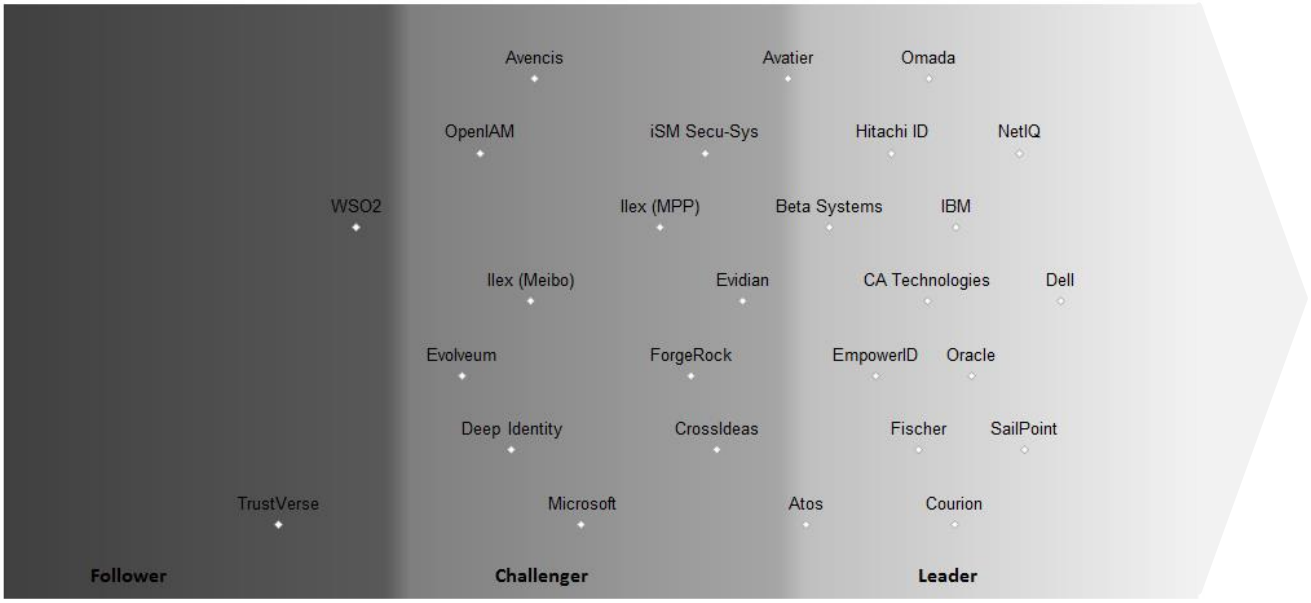

Fig. 2: Product Leaders in the Identity Provisioning market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

Product Leadership is the view where we look specifically at the functional strength and completeness of products. Again, we see the large vendors such as Dell, NetIQ, SailPoint, IBM, Oracle, and CA Technologies in that segment. IBM has become a Leader in that area due to the fact that they have shown very significant progress in their product recently. SailPoint has also significantly improved its capabilities.

Other vendors in that segment include Atos, Beta Systems, Courion, EmpowerID, Fischer, and Hitachi ID, all of them providing mature solutions that are well-established in the Identity Provisioning market.

Aside from these vendors, we see a number of others in the Challenger section, which provide good solutions, however typically falling short in one or another functional area. These vendors might be a good fit for customers anyway, depending on what the specific customer requirements are.

Some might be surprised to see Microsoft not in the Leader segment. However, their product lacks various common features, despite their strong market presence. SAP, as mentioned above, has declined participation in this KuppingerCole Leadership Compass Identity Provisioning due to an upcoming major release.

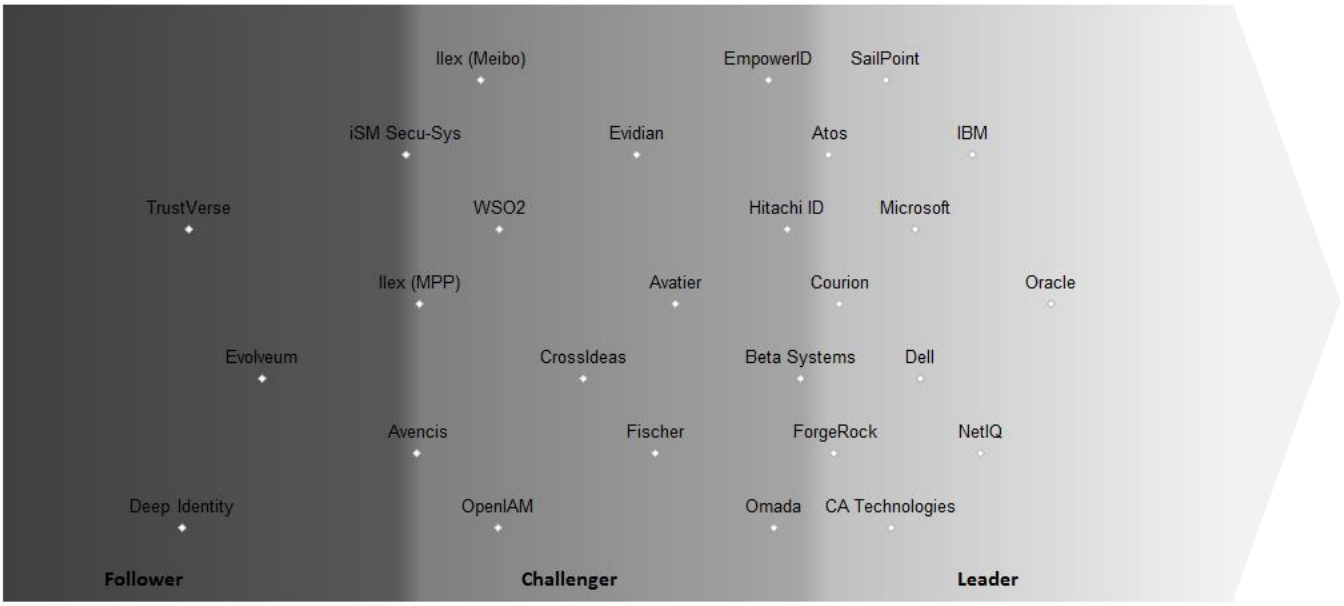

Fig. 3: Market Leaders in the Identity Provisioning market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

Looking at the Market Leadership chart, we see the expected large software companies in front, typically building on both a large customer base and a strong partner ecosystem with global presence. Oracle, NetIQ, and IBM are in the lead, closely followed by Microsoft, Dell, and CA Technologies. As mentioned above, SAP has declined participating in this edition of the KuppingerCole Leadership Compass on Identity Provisioning for product roadmap reasons.

New in that segment are four other players: Atos, Courion, ForgeRock, and SailPoint. All four showed progress in that area, with SailPoint – after acquiring the BMC Control-SA assets a while ago – massively increasing its position in the Identity Provisioning market segment. They are no longer primarily an Access Governance vendor but provide full functionality for both Identity Provisioning and Access Governance. ForgeRock benefits in that rating from its strong partner ecosystem.

Following the Leaders, we see a number of vendors in the Challenger segment, with Beta Systems, EmpowerID, Hitachi ID, and Omada being close to becoming Leaders in that area.

Again, there are many other Challengers and some Followers, showing the breadth of the market. Several of the vendors more to the left received their rating primarily based on the fact that they only act in regional markets. Furthermore, many of these have a rather limited partner ecosystem. They still might be a good fit for customers, especially in their home markets.

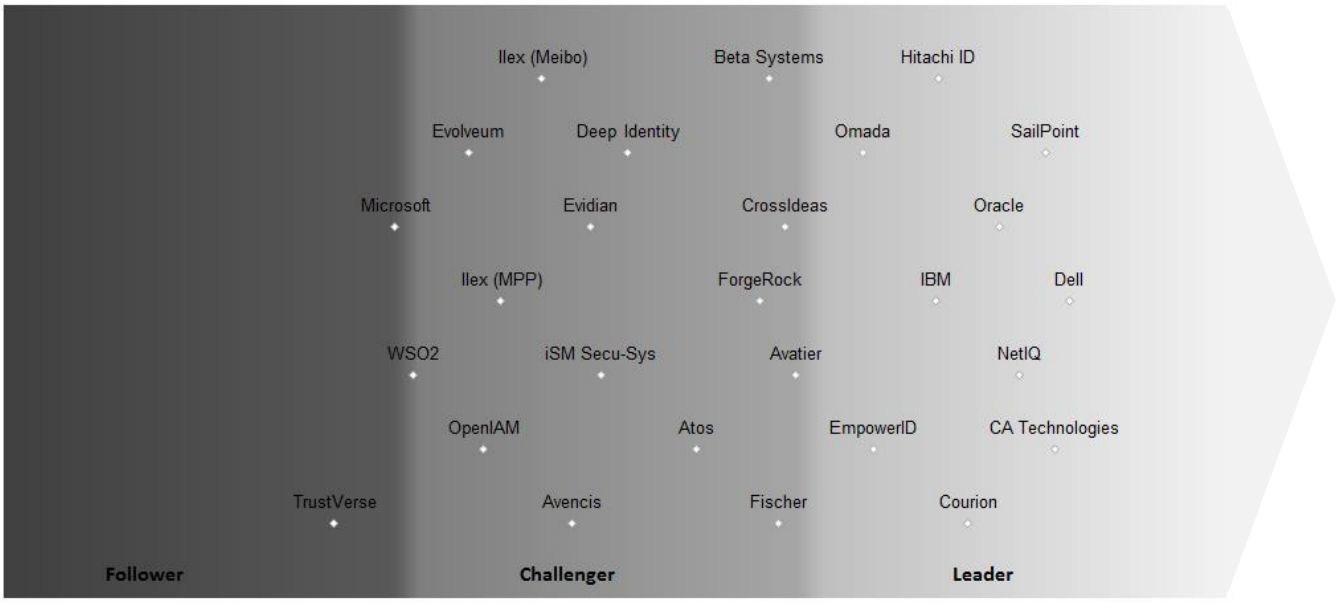

Fig. 4: Innovation Leaders in the Identity Provisioning market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at Innovation Leadership, we again see that some of the large vendors are in front. That is primarily due to the fact that they are strong in areas such as integration with Service Request Management systems and other technologies, that they provide a broad feature set, and that they can afford adding new features consistently. Also, being Market Leaders they also receive more customer feedback than others.

Thus we see Dell, SailPoint, CA Technologies, NetIQ, and Oracle in front here. IBM also is now in that section, compared to the 2012 edition of the KuppingerCole Leadership Compass Identity Provisioning. This is due to the fact that IBM showed significant progress recently, with various interesting and innovative features being added. Other leaders include Courion, EmpowerID, Hitachi ID, and Omada.

Again we see a lot of vendors in the Challenger section. Some of them are quite innovative in particular areas, such as CrossIdeas with both their business-centric approach and their way of integrating with target systems and other IT infrastructure technologies, Avatier with its strong emphasis on moving usability to the next level, or Fischer with their strong support for the Cloud. Some vendors score pretty well in that segment, compared to the Market Leadership or Overall Leadership. We provide additional comparisons in chapter 13 “Further Analysis”. In that chapter, for instance, we identify vendors that are significantly above average when comparing their innovativeness and current market position – such vendors might be a good choice when looking for innovative vendors.

These graphics provide an overview of the KuppingerCole rating of various vendors’ Identity Provisioning solutions. They are not advice recommendation to pick a specific vendor or product. 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 which weren’t “feature leaders” still were the better fit for specific customer scenarios.

2. Methodology

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

It should be noted that it is inadequate to pick vendors based only on the information provided within this report. Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

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 vendor which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the 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 all areas.

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

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

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

3. Product Rating

KuppingerCole as an analyst company regularly does evaluations of products and vendors. The results are, among 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 (**Scenario: Understanding Identity and Access Management - 70129**). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent 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 (**Advisory Note: The Open API Economy - 70352**) 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:

- Increase
  Participa
  participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly 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
initiatives adds
rating of innov

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 lead to a very low overall rating. This factor takes into account the vendor's presence in major markets.

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

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

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

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, Russia, or the US.

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

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

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

For this KuppingerCole Leadership Compass on Identity Provisioning, SAP declined its participation due to upcoming major release changes. We regret this, given that we see SAP amongst the important vendors in the Identity Provisioning market segment.

NetProf, a small US-based vendor, refrained from participation in this edition of the KuppingerCole Leadership Compass Identity Provisioning because they currently focus only on the education market. They plan to release a standard Identity Provisioning offering later in 2014.

Neither Econet nor Tools4ever participated in the evaluation process.

We provide a quick overview about these vendors and their Identity Provisioning offerings in chapter

15. Vendors and Market Segments to watch. In that chapter we also look at some other interesting offerings around the Identity Provisioning market and in related market segments.

6. Market Segment

This KuppingerCole Leadership Compass looks at the category of Identity Provisioning systems. Identity Provisioning products as we know them today are mostly organized around those four components:

- Connectors
- Reconciliation engine coupled with a repository engine
- Workflow engine
- Form generator to handle graphical user interface

Identity Provisioning products today also typically provide some basic, and sometimes more evolved, access governance functionality. This includes, for example, role management and reporting. Other typical features are user self-service, delegated administration, and password management. In addition to this, configurable workflows for request procedures and approvals are a key element.

It is impossible to understand Identity Provisioning complexity without having a quick look backward. Most historical Identity Provisioning products in the market date back to the late 1990's and early 2000's. They were designed back then and have evolved over time. That was the time of central authentication repositories and meta-directories, and the area of three-tier web architectures. In fact those years fit with the explosion of distributed systems which IT departments had to handle. On the one hand the number of systems (servers, desktops, applications, network hardware, etc.) to control was growing exponentially, while the number of skilled system administrators wasn't growing at the same rate.

On the other hand the number of requests from business units to add new users, grant privileges, enforces policies etc. was exploding. Last but not least everything had to be executed faster and faster and served at a lower cost.

As a result early Identity Provisioning systems were designed to help automate systems administration of IT. Before Identity Provisioning, it was common to wait days or even weeks for a user to get an account on a mainframe or network resource or application. With Identity Provisioning, business owners became able to serve end-user requests almost in real time from a small web interface, this without asking the permission of any mainframe or network administrator.

For those reasons, the first Identity Provisioning systems started to focus on connectivity with targeted systems: how to populate a user on an IBM-3270, how to enable someone on Cisco's VPN. Obviously as soon as the system administration bottleneck was handled, the problem moved to the next level. As it was now simple to grant access to any resource, users had accounts on multiple systems, and the issue moved from "how do I grant access to John on this or that system ?" to "how do I control what John has access to ?". To verify that grants were given on purpose, Identity Provisioning introduced the concept of workflow to verify authorizations before accepting a request.

Then in order to keep track of allocated resources a central repository was built, coupled with a reconciliation engine.

Last but not least as requests were now handled directly by business owners or end-users, traditional command lines became a "no go" option and a friendly GUI interface became one of the most important components of any Identity Provisioning implementation.

In recent years, compliance and basic access governance functions became a must have feature. Many regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, EU Privacy Protection Directive, etc. moved the responsibility of enforcing identity management policies from system and business administrators to the top management. As a direct result, key requirement for Identity Provisioning moved from "how to quickly enable my business?" to "how to make sure no one can sue me?" That put new challenges on Identity Provisioning.

With Access Governance, a new product category appeared that somewhat overlaps and somewhat integrates with classical Identity Provisioning (**Advisory Note: Access Governance Architectures - 71039**). While it remains obvious that – whatever some vendors claim – the provisioning requirement is not going to disappear any time soon, it will continue to evolve and change.

When looking at Identity Provisioning in this Leadership Compass, our expectations are that products provide mature basic capabilities as defined at the beginning of this section plus sufficient role management and basic access recertification capabilities. The emphasis clearly is on the Identity Provisioning capabilities. We don't necessarily expect full Access Governance functionality, i.e. access analytics, recertification, risk management, and related features. We also don't expect what some vendors call Access Intelligence, i.e. advanced analytical capabilities beyond what is commonly found in Access Governance products. However, we analyse these capabilities and provide additional analytics that also show the strength of solutions for solving the Access Governance challenge.

We also expect products to provide a strong and flexible internal security model, flexibility in customization, and other standard features any software product should provide like the ability not to lose customizations when updating a product.

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
- licensing models
- traditional core features of Identity Provisioning

we also considered some specific features. These include:

Connector toolkit	A toolkit for simple creation of custom connectors to target systems is highly recommended.

Heritage of connectors	Having connectors as OEM components or provided by partners is considered a risk for ongoing support and available know-how at the vendor.
ESB interfaces	Having interfaces to ESBs (Enterprise Service Bus) adds architectural options for integrating Identity Provisioning with existing systems and for connecting to target systems.
SRM interfaces	We expect that systems provide out-of-the-box integration to leading SRM (Service Request Management) systems for manual fulfilment of provisioning requests.
SPML/SCIM support	Support for these two standards (Service Provisioning Markup Language/ System for Cross-domain Identity Management) is highly recommended.
Deployment models	Supporting different deployment models like hard/soft appliances and cloud deployment gives customer a broader choice.
Customization	Systems that require little or no coding and that support scripting or, if programming is required, a range of programming languages, are preferred. We here also look for transport systems between development, test, and production, and the ability of keeping customizations unchanged after upgrades.
Authentication mechanisms	We expect Identity Provisioning systems to support different types of authentication to the system, including strong authentication options, to limit the risk of fraud using these systems.
Internal security model	All systems are required to have a sufficiently strong and fine-grained internal security model.
Multi tenancy	Given the increasing number of cloud deployments, but also specific requirements in multi-national and large organizations, support for multi-tenancy is highly recommended.
Role/SoD concept	Provisioning should be feasible based on role concepts and with support for the definition of SoD rules (Segregation of Duties), despite the fact that Access Governance tools are increasingly used on top of Identity Provisioning.
Shopping cart paradigm	These approaches are pretty popular for simplifying the access request management process by using shopping cart paradigms familiar to the users.

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 Identity Provisioning market segment. The market leaders are shown in figure 5.

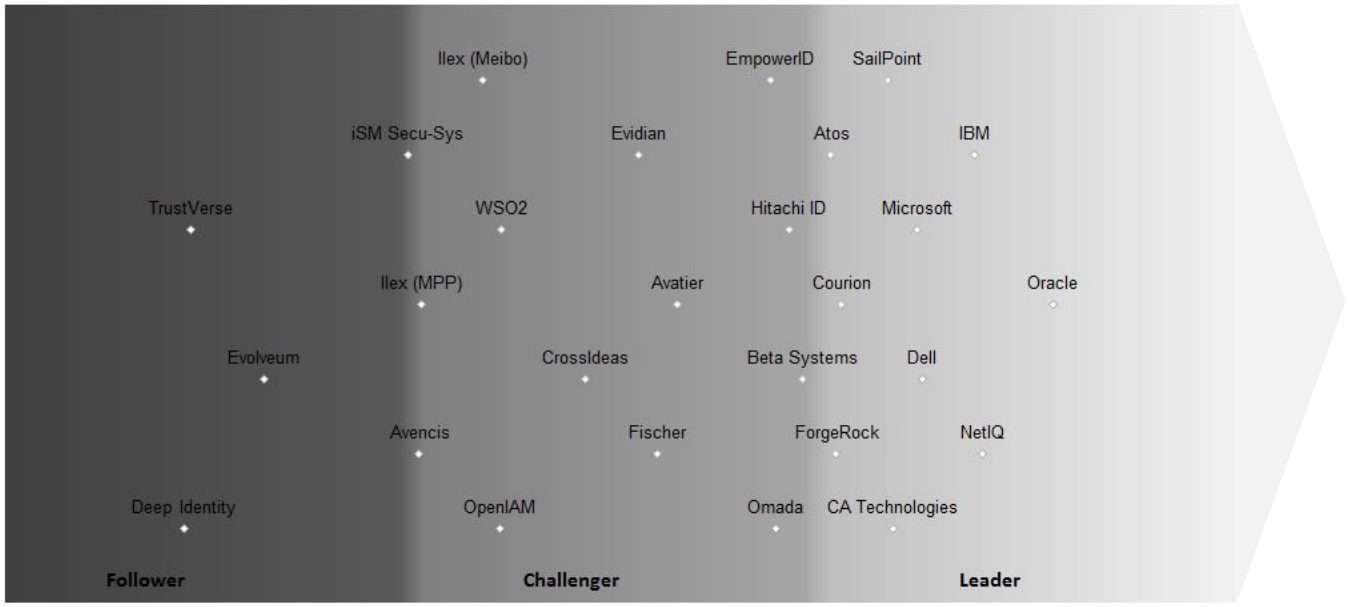

Fig. 5: Market leaders in the Identity Provisioning market segment.

Looking at the Market Leadership chart, we see the expected large software companies in front, typically building on both a large customer base and a strong partner ecosystem with global presence. Oracle, NetIQ, and IBM are in the lead, closely followed by Microsoft, Dell, and CA Technologies. As mentioned above, SAP has declined participating in this edition of the KuppingerCole Leadership Compass on Identity Provisioning for product roadmap reasons.

New in that segment are four other players: Atos, Courion, ForgeRock, and SailPoint. All four showed progress in that area, with SailPoint – after acquiring the BMC Control-SA assets a while ago – massively increasing its position in the Identity Provisioning market segment. They are no longer primarily an Access Governance vendor but provide full functionality for both Identity Provisioning and Access Governance. ForgeRock benefits in that rating from its strong partner ecosystem.

Following the Leaders, we see a number of vendors in the Challenger segment, with Beta Systems, EmpowerID, Hitachi ID, and Omada being close to becoming Leaders in that area.

Again, there are many other Challengers and some Followers, showing the breadth of the market. Several of the vendors more to the left received their rating primarily based on the fact that they only act in regional markets. Furthermore, many of these have a rather limited partner ecosystem. They still might be a good fit for customers, especially in their home markets.

The market is affected by a situation where several very large software vendors compete with a large number of smaller vendors, which, frequently, are only acting regionally. Market leadership is mainly a hint at the overall position of the vendor, its strength in sales, and its partner ecosystem. It has to be noted that this doesn't allow any conclusion about whether the products of the different vendors fit to the customer requirements.

Market Leaders are (in alphabetical order)

- Atos
- CA Technologies
- Courion
- Dell
- ForgeRock
- IBM
- Microsoft
- NetIQ
- Oracle
- SailPoint

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.

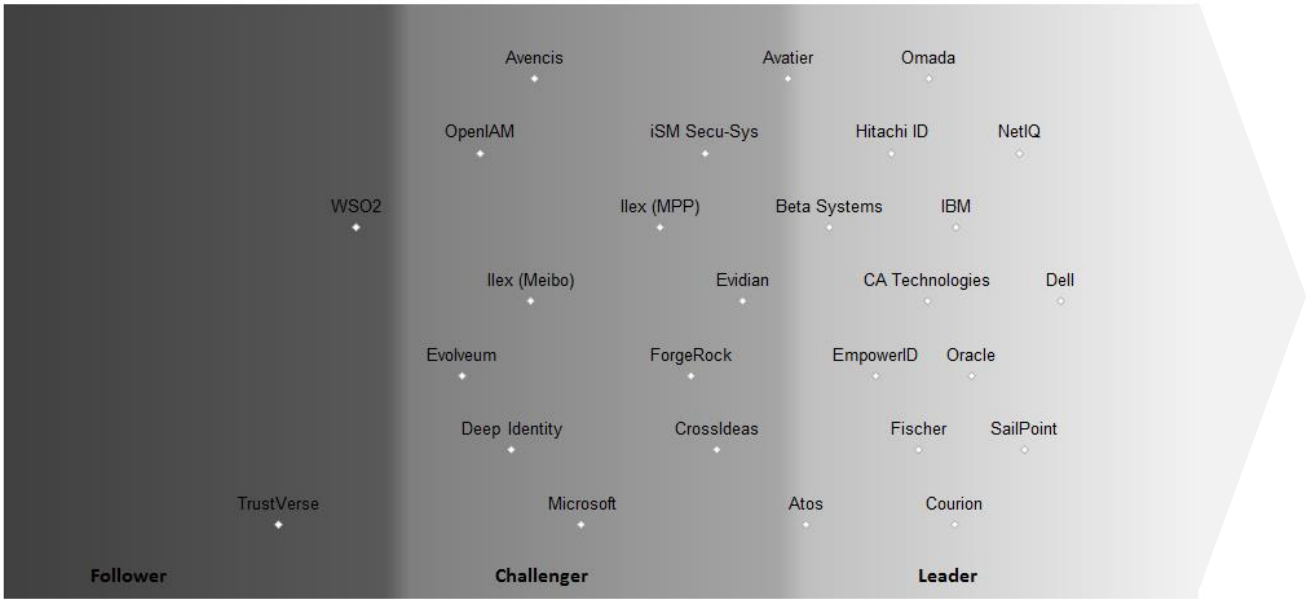

Fig. 6: Product leaders in the Identity Provisioning market segment.

Product Leadership is the view where we look specifically at the functional strength and completeness of products. Again, we see the large vendors such as Dell, NetIQ, SailPoint, IBM, Oracle, and CA Technologies in that segment. IBM has become a Leader in that rating due to the fact that they showed very significant progress in their product recently. SailPoint also significantly improved its capabilities for Identity Provisioning.

Other vendors in that segment include Atos, Beta Systems, Courion, EmpowerID, Fischer, and Hitachi ID, all of them providing mature solutions that are well-established in the Identity Provisioning market.

Aside from these vendors, we see a number of other vendors in the Challenger section, which provide good solutions, however typically falling short in one or another functional area. These vendors might be a good fit for customers anyway, depending on what the specific customer requirements are.

Some might be surprised to see Microsoft not in the Leader segment. However, their product lacks various common features, despite their strong market presence. SAP, as mentioned above, has declined participation in this KuppingerCole Leadership Compass Identity Provisioning due to an upcoming major release.

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 which weren't "feature leaders" still were the better fit for specific customer scenarios.

Product Leaders are (in alphabetical order):

- Atos
- Beta Systems
- CA Technologies
- Courion
- Dell
- EmpowerID
- Fischer
- Hitachi ID
- IBM
- NetIQ
- Omada
- Oracle
- SailPoint

10. Innovation Leaders

The third angle we took when evaluating products concerned innovation. Innovation is, from our perspective, a key capability 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.

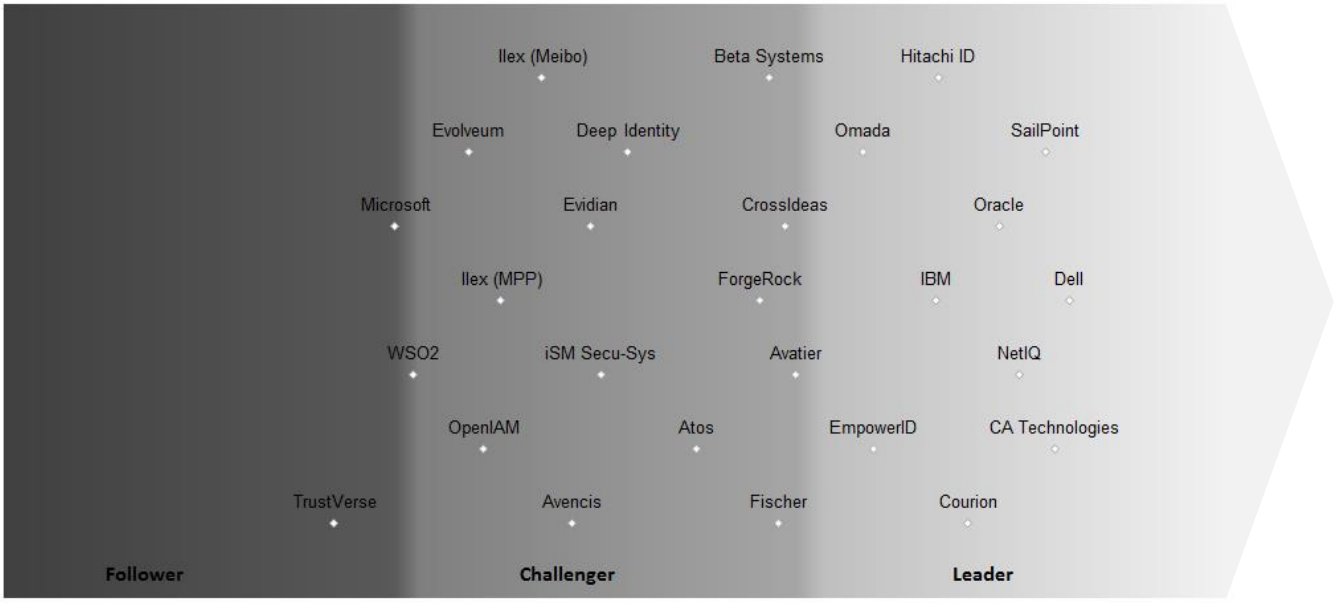

Fig. 7: Innovation leaders in the Identity Provisioning market segment.

When looking at Innovation Leadership, we again see that some of the large vendors are in front. That is primarily due to the fact that they are strong in areas such as integration with Service Request Management systems and other technologies, that they provide a broad feature set, and can afford adding new features consistently. Also, being Market Leaders they receive more customer feedback than others.

Thus we see Dell, SailPoint, CA Technologies, NetIQ, and Oracle in front here. IBM also is now in that section, compared to the 2012 edition of the KuppingerCole Leadership Compass Identity Provisioning. This is due to the fact that IBM has shown significant progress recently, with various interesting and innovative features being added. Other leaders include Courion, EmpowerID, Hitachi ID, and Omada.

Again we see a lot of vendors in the Challenger section. Some of them are quite innovative in particular areas, such as CrossIdeas with both their business-centric approach and their way of integrating with target systems and other IT infrastructure technologies, Avatier with its strong emphasis on moving usability to the next level, or Fischer with their strong support for the Cloud. Some vendors score pretty well in that segment, compared to the Market Leadership or Overall Leadership. We provide additional comparisons in chapter 13 “Further Analysis”. In that chapter, for instance, we identify vendors that are significantly above average comparing their innovativeness and current market position – such vendors might be a good choice when looking for innovative vendors.

Again, in some cases products which appear more to the left in that chart do not necessarily fail in innovation but are focused on specific requirements or very focused approaches, like Evidian with their focus on a more complete solution for SMBs and their tight integration of Access Management, Single Sign-On, and Identity Provisioning or Ilex with their toolset approach for quickly developing IAM applications plus a specific solution for the needs of SMBs.

Innovation Leaders are (in alphabetical order):

- CA Technologies
- Courion
- Dell
- EmpowerID
- Hitachi ID
- IBM
- NetIQ
- Omada
- Oracle
- SailPoint

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 available, providing more detailed information.

11.1 Atos DirX Identity

Atos acquired the former Siemens SIS (IT Solutions and Services) unit. As part of this acquisition, the DirX products became part of the Atos portfolio. DirX Identity is the Identity Provisioning solution within that portfolio. The product is well established in the market, with several very large installations. It is sort of a standard Identity Provisioning product covering the classical features commonly found in that market segment, like connectors to target systems, workflow functionality, role management, and additional access governance capabilities. In addition, Atos provides a number of vertical integrations for industries such as Facility Management and Healthcare, based on the specific domain knowledge and with technical integrations. Furthermore, Atos is pushing Cloud-based identity services, based on the DirX products.

Strengths/Opportunities	Weaknesses/Threats
Mature, well established product with proven ability to execute in very large scale deployments	Standard user interface WebCenter somewhat cumbersome to customize
Strong role- and rule-based approach for provisioning	Limited partner ecosystem
Consistent use of web services for interoperability	

Table 1: Atos DirX Identity major strengths and weaknesses.

The product has strong capabilities in core provisioning features including connectivity to target systems and scalability and high-availability features. It also provides a strong role management approach. Based on long experience in role management, the concepts implemented in that area are very mature and leading-edge. Atos has added additional capabilities for a more flexible management beyond roles, based, for example, on organizational structures and using rules to manage entitlements. Main features are exposed via web services, which allows for simple interoperability. The standard user interface WebCenter is very powerful but customization is considered cumbersome by some customers. However, relying on the web services provides an alternative to create and customize the user interfaces.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 2: Atos DirX Identity rating.

Overall, Atos DirX Identity is a mature and feature-rich product. Atos provides its own managed services and has a worldwide presence. The partner ecosystem is fairly limited, which is not surprising for a vendor that has its own professional services. Nevertheless, Atos should work on growing that ecosystem and ensure that sufficient professional services resources are available to their customers at any time.

11.2 Avatier Identity Management Software Suite

Avatier is a vendor which follows a different approach than most other vendors in the Identity Provisioning market. They call this "Assignment Management". The different components of its offering focus on providing a simple and familiar experience to end users along with an easy-to-use graphical configuration interface for administrators. This includes support for new types of mobile devices and a shopping cart approach for requesting access, assets and other resources. Overall, the paradigm is very much driven by a service request-oriented approach and a high degree of user centrism while still providing broad support for automation. The focus is clearly on a configuration approach providing lower time-to-value compared to more complex solutions.

Strengths/Opportunities	Weaknesses/Threats
Innovative, highly user-centric approach to Identity Provisioning	No support for multi-tenancy
Fast implementation focusing on end user service requests	Still limited but growing partner ecosystem
Potential use also as neat user interface on top of other Identity Provisioning solutions	Still limited footprint outside of North America

Table 3: Avatier Identity Management Software Suite major strengths and weaknesses.

This makes the Avatier solution an interesting alternative to the more common approach to Identity Provisioning. However it will not suit the needs of all customers. Security is good but some features such as flexible multi-tier identity models or rollback operations for changes are lacking. There is also no support for multi-tenancy. Avatier clearly is one of the products which either fit to what customers are looking for or not – it is different but worth having a look at. A shortcoming of Avatier clearly is their very limited partner ecosystem around IAM-centric system integrators. Avatier claims that the simplicity of the solution reduces this requirement and has furthermore increased its own professional services resources. They have expanded their partner network towards Service Management vendors, however that is more sales-centric.

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

Table 4: Avatier Identity Management Software Suite rating.

Overall, Avatier Identity and Access Risk Management Suite is an interesting choice for several customers, taking a different approach to Identity Provisioning than most of the other products. Currently, the vendor has a rather limited footprint outside of North America but is increasing its overall visibility in other regions.

11.3 Avencis Hpliance: IAM solution

Avencis is a French vendor that originally started in the E-SSO (Enterprise Single Sign-On) business. Later on they introduced their Hpliance solution for Identity Provisioning, originally targeted at the Healthcare business and based on Microsoft FIM (Forefront Identity Manager) for connectivity to target systems. Hpliance is a solution with a growing set of capabilities, including improved workflows and direct connectivity to target systems.

Strengths/Opportunities	Weaknesses/Threats
Tight integration with the Avencis SSOX product for E-SSO	No MSP/Cloud offerings, no virtual appliance
Well thought-out approach to managing access controls of users	No complete set of APIs exposing the functionality
Can simulate forthcoming changes	Limited global reach and partner ecosystem

Table 5: Avencis Hpliance: IAM solution major strengths and weaknesses.

The Hpliance IAM solution, being a newer product of Avencis, is still an emerging solution. While it supports the standard requirements in Identity Provisioning and has a well thought-out approach to managing entitlements of users, the workflow capabilities only recently have been expanded to meet the common expectations of the market.

Among the challenges we observe are the lack of MSP (Managed Service Provider) or Cloud offerings and a virtual appliance, potentially leading to a higher degree of complexity in implementation and roll-out. We also miss support for a comprehensive set of APIs exposing the functionality of the product. On the other hand, we see a strong potential for the product through its integration with the Avencis SSOX solution, allowing customers to manage both authentication and access controls.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	positive

Table 6: Avencis Hpliance: IAM solution rating.

Avencis still has a somewhat limited global reach, especially with their Hpliance IAM solution. They are addressing foreign markets primarily through technology partners from the authentication space, thus the focus is more towards the SSOX solution than the Hpliance solution. Overall, we see a need for investing both in further improvement of the technology as well as into a broader partner ecosystem. Nevertheless, Avencis appears to be an interesting option primarily for customers that are also looking for an E-SSO solution.

11.4 Beta Systems SAM Enterprise Identity Manager

Beta Systems, a German vendor, has been offering its SAM Enterprise Identity Manager for many years now. The company has a significant customer base, with some focus on the finance industry. It is, generally, a standard Identity Provisioning product covering the classical features commonly found in that market segment, like connectors to target systems, workflow functionality, and role management. Beta Systems recently started improving the integrated Access Governance/Intelligence functionality, based on a separate offering called Garancy Access Intelligence Manager, which is not within the scope of this analysis.

Strengths/Opportunities	Weaknesses/Threats
Very mature approach to role management Connector approach with tight application integration, supporting also Dynamic Authorization Management Strong support for mainframe environments	No out-of-the-box capability for assigning ownership for shared accounts Still a relatively small but sufficient partner ecosystem.

Table 7: Beta Systems SAM Enterprise Identity Management Suite major strengths and weaknesses.

Beta Systems SAM Enterprise Identity Management Suite supports a broad range of platforms, with exceptionally strong support for mainframe environments. Over the course of the last few years, Beta Systems has enhanced its functionality significantly, partially by adding components acquired or licensed from other vendors. With the recent release, the company has managed to integrate these functions quite well and is making progress in the area of usability. They also have started adding enhanced Access Governance and Intelligence functionality. Support for role management is strong, based on long experience. Besides this, Beta Systems is one of the few vendors offering connectors with tight application integration, allowing applications to request authorization decisions at runtime and thus enabling Dynamic Authorization Management as an integrated feature.

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

Table 8: Beta Systems SAM Enterprise Identity Management Suite rating.

Overall, Beta Systems SAM Enterprise Identity Management Suite is a mature and feature-rich product. Beta Systems has a presence in major markets and a sufficient partner ecosystem.

11.5 CA IdentityMinder

CA Technologies is among the largest infrastructure software vendors worldwide and offers a broad portfolio of products in the IAM market segment, including CA IdentityMinder (formerly CA Identity Manager) as its solution for Identity Provisioning. This is built on different tools CA Technologies had developed and acquired over time. The current version is well integrated and provides the full feature set to be expected from Identity Provisioning solutions.

Strengths/Opportunities	Weaknesses/Threats
Mature product with a broad range of features and good integration of these Efficient use through Xpress components Tight integration with other CA products including CA GovernanceMinder (Access Governance) Large customer base	Requires CA SiteMinder for advanced security of administrative console such as strong authentication beyond passwords Still a relatively small IAM-specific system integrator ecosystem, compared to other large vendors

Table 9: CA IdentityMinder major strengths and weaknesses.

Based on the long history of the product and the market position of CA Technologies, it is no surprise that CA has done a large number of deployments of CA IdentityMinder. As a consequence, there is - besides a mature and rich feature set - a number of additional solutions from CA Services available which add to this functionality. A particular strength of the product is the availability of the Xpress components such as the Policy Xpress for building logic without coding and Connector Xpress for configuring new connectors.

Like some other vendors, CA Technologies is following a concept which tries to avoid too many redundancies between the products in its portfolio. Thus most Access Governance features are part of CA GovernanceMinder, while CA SiteMinder acts as sort of the “first line of defense” when it comes to security. This approach is not uncommon and has its strengths (when building on the entire ecosystem) and potential weaknesses (when requiring just one of the products but some functionality beyond its core features).

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

Table 10: CA IdentityMinder rating.

Overall, CA IdentityMinder is a mature product with tight integration into a suite of products. CA Technologies has a global presence but only a fairly small number of specialized partners; however the company has its own service offerings on a global scale.

11.6 Courion Access Assurance Suite

Courion is a vendor which has evolved from supporting specific problems especially around password synchronization towards a company with a suite covering major areas of IAM today. The Courion Access Assurance Suite is their integrated offering which includes provisioning capabilities but also adds advanced Access Governance and Access Risk Management capabilities on top of that. Within that suite, AccountCourier for Identity Provisioning and PasswordCourier for self-service password management are the primary offerings within the scope of this Leadership Compass. Courion has chosen to extend the reach of its main product beyond core provisioning and take the path of providing a more comprehensive suite covering several capabilities.

Strengths/Opportunities	Weaknesses/Threats
Broad, integrated feature set for provisioning and access governance	Still limited footprint in the market outside of North America
Mature provisioning capabilities and large number of connectors	Limited Cloud support and no virtual appliance offering
Good connectivity also with more complex platforms like mainframe environments	Limited support for external authentication

Table 11: Courion Access Assurance Suite major strengths and weaknesses.

Courion has opted for an approach which focuses on providing a broad set of features and enhancing Identity Provisioning beyond its traditional scope. Given that the suite is sufficiently modular, that allows customers to rely on some or all portions of this feature set if required. Classical provisioning capabilities are strong, with a significant number of connectors also covering the more complex target platforms. Courion also provides exceptionally strong integration with other elements of IT infrastructure like SIEM platforms etc.

As of now, Courion offers only limited support for Cloud services, restricted to PasswordCourier, and no virtual appliance. We also see limited support for external authentication of administrators and users.

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

Table 12: Courion Access Assurance Suite rating.

Overall, Courion has a very strong product offering with a broad feature set. Their major weakness is the lack of a broad partner ecosystem and in consequence the limited footprint outside of the North American market.

11.7 CrossIdeas IDEAS

CrossIdeas is an Italian vendor which started as part of the largest Italian system integrator, Engineering spA. They have been in the market for several years now. Originally they provided a Dynamic Authorization Management system for externalizing authorization decisions from applications. Over time, strong role management and overall Access Governance capabilities have been added. Recently, CrossIdeas – beyond connecting to other provisioning tools – started adding its own connectors. Thus they also can directly provision to target systems now. However, they didn't start as a provisioning tool from scratch but took another, rather uncommon way.

Strengths/Opportunities	Weaknesses/Threats
Excellent business-oriented framework for managing access, including full Access Governance	Still somewhat limited number of own connectors, but growing
Supports Dynamic Authorization Management out-of-the-box	Still small but growing partner ecosystem
Well thought-out approach to providing connectors, both direct connectors and via other Identity Provisioning tools	Different approach than classical provisioning, based on Access Governance capabilities, will not fit to every use case

Table 13: CrossIdeas IDEAS major strengths and weaknesses.

Due to its history, IDEAS is not a typical Identity Provisioning solution. However, having a good base of provisioning capabilities available now qualifies them as a newcomer in this market, which is moving towards providing more increased Access Governance capabilities anyway. Besides their strong features in that area with a very business-centric approach, tying well into existing business processes, a rather rare feature in that market segment is the tight integration with Dynamic Authorization Management, allowing it to externalize authorization decisions instead of just statically provisioning access controls to target systems. CrossIdeas in the meanwhile has built its own connector framework, with support for the most relevant target systems. In addition they provide integration with other Identity Provisioning solutions for fulfillment, if required.

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

Table 14: CrossIdeas IDEAS rating.

Overall, IDEAS is clearly more a product for customers looking for an Access Governance solution and maybe a Dynamic Authorization Management tool with a good baseline capability in Identity Provisioning, then it is for customers looking only for Identity Provisioning. Thus it depends on the customer requirements whether this is a good fit. In sum, CrossIdeas clearly has improved its position in the IAM market as well as in the Identity Provisioning market.

11.8 Deep Identity IACM, IM, FsGA

Deep Identity is a company based in the APAC (Asia/Pacific) region. The company primarily focuses on its IACM (Identity Audit and Compliance Manager) product that is targeted at the IAG (Identity and Access Governance) market segment. However, with the additional IM (Identity Manager) and FsGA (File Server Governance and Administrator) tools, they provide additional functionality also for the Identity Provisioning market segment, in addition to their core capabilities.

Strengths/Opportunities	Weaknesses/Threats
Strong capabilities in Access Governance, with a layered approach for Identity Provisioning	Small vendor with limited number of customers
Support for ESB (Enterprise Service Bus) for technical integration	Certain features such as shopping cart or standard IAM processes still missing
Support for multi tenancy	No established partner ecosystem as of now

Table 15: Deep Identity IACM / IM / FsGA major strengths and weaknesses.

Deep Identity clearly is more focused on the IAG market segment. However, with their layered approach, including the FsGA component's support of file server management, they are well positioned for the emerging need for a comprehensive EAG (Entitlement and Access Governance) solution. In addition, their product follows a well thought-out architecture, with support for ESB (Enterprise Service Bus) as a communication mechanism, for example. In general, several of the more innovative areas such as multi-tenancy are covered.

On the other hand, we still see a lack of certain common features. For instance, there is no shopping cart provided for simple access request management by end-users, an increasingly common feature. The product does not come with pre-configured processes, a feature virtually all products in the market have. It also lacks a comprehensive set of APIs, exposing all functions of the products.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 16: Deep Identity IACM / IM / FsGA rating.

Deep Identity is one of the smaller vendors entering the IAM/IAG market. As of now, they are lacking a partner ecosystem that would help them grow faster. On the other hand, they show some interesting innovative features and an overall well thought-out architectural approach. Even while their strength is more around IAG, they might be an interesting vendor especially for organizations located in the APAC region and, if they succeed in building up their partner ecosystem, also in other regions.

11.9 Dell One Identity Manager

Dell One Identity Manager came to the Dell portfolio through the acquisition of Quest Software and the preceding acquisition of the German vendor Völcker Informatik. The Völcker tool formerly known as ActiveEntry is now a cornerstone of the entire Dell IAM portfolio. Dell One Identity Manager builds on a sophisticated, consistent concept which allows for fairly simple customization and manages all dependencies between different objects in a very advanced way. The standard user interfaces of the product are very well constructed. Customization is straightforward

Strengths/Opportunities	Weaknesses/Threats
Innovative, user-friendly interfaces Well-thought out, sophisticated architecture and concepts Leading-edge shopping cart paradigm and other innovative features	Product concept must be understood – different from standard approaches

Table 17: Dell One Identity Manager major strengths and weaknesses.

The product is designed with some rather uncommon features. While its shopping cart approach can now be found in an increasing number of products, other features like the ability to simulate the effect of changes or the ability to show the state of any point in time in the past are unique. Customization is fairly straightforward, mainly done through configuration or based on creating rules. However, the concept needs to be well understood given that it is different from typical approaches to Identity Provisioning. In addition, the consistent architecture might become a limitation in some cases for specific needs of customization. However, the flexibility for customization has been greatly increased over the past few years.

In addition, Dell has increased the functional capabilities of the product over the past years. The number of connectors has grown and there is broad support for EAG (Entitlement and Access Governance), both on the lower level through the Data Governance Edition, and on the upper level based on built-in support.

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

Table 18: Dell One Identity Manager rating.

Overall the product is among the most interesting and intriguing offerings in the Identity Provisioning market. It gets a clear recommendation for evaluation in product selections.

11.10 EmpowerID

EmpowerID with its product also named EmpowerID takes a unique approach to Identity Provisioning. It is built from scratch on a Business Process Management/Workflow platform. All standard components rely on that platform and customizations can be made using the same environment. That allows for great flexibility, while the product also delivers a broad set of out-of-the-box features.

Strengths/Opportunities	Weaknesses/Threats
Unique, business process-based approach to Identity Provisioning	Specific workflow-based concept differs from common approaches to Identity Provisioning, must be understood first
Functionality well beyond Identity Provisioning	Small partner ecosystem
Flexible customization based on the central workflow engine, supported by a large number of predefined processes	

Table 19: EmpowerID major strengths and weaknesses.

Customization of EmpowerID is very flexible, based on the approach chosen by The Dot Net Factory. The name implies that the technical platform is .NET. The product delivers a very broad feature set for Identity and Access Management, going well beyond Identity Provisioning but with tight integration to these core features. That includes Dynamic Authorization Management capabilities and integrated Identity Federation features. Overall, support for new technologies and standards like OAuth, OpenID, RESTful APIs, or integrated STS (Secure Token Service) features is broad.

However, the product also delivers a broad functionality for basic Identity Provisioning requirements. We have seen a lot of progress in that area with an increased number of connectors and a very large number of out-of-the-box workflows that allow for rapid deployments.

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

Table 20: EmpowerID rating.

Overall, EmpowerID is a very interesting and innovative solution. The approach taken might fit or not – that needs to be evaluated. It is definitely worth having a look at the product. A challenge is the still small partner ecosystem, with few partners as of now. We strongly encourage EmpowerID to grow their number of partners.

11.11 Evidian Identity & Access Manager

The French vendor Evidian is part of Groupe Bull, one of the leading European IT companies. Evidian has been in the IAM business for many years. Their product, Identity & Access Manager, has been developed over a number of years and provides a good set of features in Identity Provisioning. The target market of Evidian is mid-sized businesses for which they provide an integrated solution with all major required features. These go beyond pure Identity Provisioning, allowing customers to implement an integrated approach to core IAM requirements. Notably, however, Evidian also has several very large accounts, not being limited to smaller deployments.

Strengths/Opportunities	Weaknesses/Threats
Established product with good feature set in core functionality	Limited deployment models
Excellent integration to Evidian SSO/Access Management solutions	Conceptual approach might not be a perfect fit to some customer requirements
Integrated offering with a consistent concept for managing identities and access	No ESB and SRM integration out-of-the-box, but integrated Request Management capabilities
Integrated support for Dynamic Authorization Management	

Table 21: Evidian Identity & Access Manager major strengths and weaknesses.

Evidian has developed a tightly integrated product which covers all major aspects of Identity Provisioning. It is focused on providing a consistent set of processes for users. Besides the core provisioning capability, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian. A shortcoming is the lack of cloud/MSP deployment models and appliance offerings. There is also a lack of advanced integration, such as support for ESB (Enterprise Service Bus) concepts or SRM (Service Request Management) integration out-of-the-box. On the other hand the product can use existing external workflow systems. The product allows a quick start for many scenarios, especially in medium-sized businesses. However it might not be the perfect fit for some customer scenarios due to its tight integration of various capabilities.

Over the last few years, we have seen progress in various areas. The product includes its own, strong Service Request Management capabilities. Furthermore, there is built-in support for Dynamic Authorization Management now, externalizing authorization decisions out of applications.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 22: Evidian Identity & Access Manager rating.

Overall, Evidian delivers a mature product with a strong feature set and a well-thought out conceptual approach. Evidian provides an interesting alternative to the leading vendors and remains a challenger to them. The company is mainly focused on the European markets.

11.12 Evolveum midPoint

Evolveum is an Open Source IAM vendor based in Slovakia. Their midPoint product is rather new in the market and provided for free. The product relies on the same foundation as the ForgeRock OpenIDM product, but was forked away in development a while ago. As of now, midPoint still is in an early phase of its evolution, but with some promising potential.

Strengths/Opportunities	Weaknesses/Threats
Open Source solution, provided at no (license) cost	Several common features still missing, however various of them on the roadmap
Innovative features on roadmap	Limitation of delivery models
Broad support for connectors based on standard frameworks	Still small number of customers and limited partner ecosystem

Table 23: Evolveum midPoint major strengths and weaknesses.

When looking at the current version of the product, we observe a lack of several of the common features. Reporting has been improved and relies on a flexible engine now, but is limited regarding the standard reports. There is no shopping cart paradigm supported for requesting access, however other feasible approaches are supported. Also, other features such as rollback operations based on thresholds are still lacking. We also would like to see more integration of the administrative interfaces, such as fully integrating the workflow capabilities.

On the other hand we see a lot of strong capabilities and a number of interesting features on the roadmap. Evolveum midPoint has a potential to improve its position in the market when the vendor successfully executes on its roadmap. Among the planned improvements is Cloud-based delivery.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 24: Evolveum midPoint rating.

As of now, Evolveum midPoint is a rather new and still somewhat feature-limited offering in the Identity Provisioning market, but with interesting potential. On the plus side, there is the fact that many interesting features are planned for upcoming versions and the current release already shows significant improvements. Aside from that, Evolveum should have a good potential for growth relying on the Open Source communities and potential partners therein. However, as of now we see the product primarily as an option for companies specifically looking for an Open Source solution.

11.13 Fischer Automated Role & Account Management

Fischer International Identity is a vendor which is different from all other provisioning vendors in that the company from the very beginning focused on SaaS delivery models for IAM as a main go-to-market strategy and core competency. The product is available for on-premise deployment as well, which makes up a significant portion of the Fischer sales. However, the entire architecture has been defined for optimally supporting SaaS deployments, requiring only a gateway at the customer's sites. While this approach also suits well for on-premise, it gives Fischer a head start for cloud-based deployments, having, for example, full multi-tenancy support as a logical design principle.

Strengths/Opportunities	Weaknesses/Threats
SaaS delivery model as standard option	No ESB support yet
No coding required, customization is done via configuration and graphical design components	No shopping cart paradigm supported
	No approvals for configuration changes
Well-defined user interfaces for quick-start deployments	

Table 25: Fischer Automated Role & Account Management major strengths and weaknesses.

Their SaaS delivery model is supported by several MSPs, including Wipro as a global partner. Due to their SaaS-ready design approach, the clear focus is on providing a large set of features, well-defined standard configurations, and avoiding programming. There is no need for coding, but sometimes intensive configuration is needed. Besides that there are graphical tools for designing user interfaces and workflows.

Fischer has a good strategy for integration, supporting both an ETL-based approach and a comprehensive set of REST APIs. Furthermore, connectors are fairly simple to create. Thus, even complex scenarios are in scope of that solution. However, certain features are lacking, such as a standard shopping cart approach for access requests or approval workflows for configuration changes. The partner ecosystem of Fischer is still somewhat limited in size but growing and based on a few global, engaged partners.

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

Table 26: Fischer Automated Role & Account Management rating.

Overall, Fischer provides an interesting approach to Identity Provisioning supporting both on-premise and SaaS deployments. The approach might not suit the needs of every customer. On the other hand, customization is straightforward and the product focuses on avoiding coding at all.

11.14 ForgeRock OpenIDM

ForgeRock is a company providing Open Source IAM solutions. One of their products is OpenIDM, an Identity Provisioning solution. This is not built on the former Sun Identity Manager/Oracle Waveset product but leverages the OpenICF connector framework which adopted the former Sun Microsystems open source project "Identity Connector Framework". The product's features have been improved in the current release, however it is – in contrast to other offerings in the market – purely focused on core Identity Provisioning. With its feature set and focus, it is not only an option for companies looking for open source solutions only or focusing on approaches which they can greatly customize to suit specific needs, but also for customers that primarily are looking for a strong Identity Provisioning "core engine". The product strategy for OpenIDM is focused on a "one stack" approach with integration to other products and lightweight APIs for easy, accessible adoption. This also suits the needs of customers which need to heavily customize or very tightly integrate a provisioning tool with existing IT environments.

Strengths/Opportunities	Weaknesses/Threats
Open source product for Identity Provisioning Broad set of connectors based on OpenICF framework. Good interoperability based on a comprehensive set of REST APIs.	Somewhat limited regarding certain features, focused on core Identity Provisioning Growing partner ecosystem, but limited regarding deployment models as of now No support for role management

Table 27: ForgeRock OpenIDM major strengths and weaknesses.

ForgeRock provides a basic Identity Provisioning solution as of now. There are some fundamental features missing, including support for role management approaches. ForgeRock claims that this limitation can be addressed by mimicking it through their rule-based concept, however that would be fairly complex in most organizations. The partner ecosystem is also limited, as are deployment options. A strength is the breadth of available connectors based on the open source OpenICF project and, for some customers, the fact that the product is open source and flexible, making it easier to integrate and customize.

OpenIDM has a notion of being very scalable. A strength of the product is the comprehensive set of REST APIs, which is important for both interoperability and customization.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	neutral

Table 28: ForgeRock OpenIDM rating.

Overall, ForgeRock OpenIDM has made a significant step forward with its new release and shows interesting and innovative features. It is attractive not only for customers looking for an open source approach to Identity Provisioning, but for all types of customers, especially when focusing on a strong core engine for Identity Provisioning.

11.15 Hitachi ID Identity Manager

Hitachi ID provides a product called Identity Manager, which is a mature solution for managing identities and their access. It integrates Access Governance features, including SoD (Segregation of Duty) support and certification features. The product builds on an open, flexible architecture that also builds the foundation of other Hitachi ID IAM products. Hitachi ID provides a well-defined model for segregation of code and customizations, allowing the retention of customizations when applying release changes. However, managing changes between development, test, and production requires extracting and applying XML files from a separate revision control system.

Strengths/Opportunities	Weaknesses/Threats
Part of an integrated IAM Suite, beyond provisioning capabilities	No shopping cart paradigm supported.
Mature solution with broad connector support	No transport system for changes
Tight integration into Windows Explorer	Limited footprint outside of North America
Support for Active Directory Group Management	

Table 29: Hitachi ID Management Suite major strengths and weaknesses.

In general, the product provides a mature set of features, delivering what customers typically need. It delivers a large set of connectors. However, the architecture and access control model have to be carefully reviewed to understand whether they suit the needs of the organization. The architecture provides high flexibility and scalability and is well-thought out. There are a number of unique features available, plus good interoperability. On the other hand some features such as shopping cart paradigms are not supported out of the box.

The SoD approach implemented ensures that SoD violations and the impact of changes are handled correctly at all layers in a multi-layered role/entitlement model which is not the case with all products in the market. Some specific strengths are the integration with Microsoft SharePoint and Windows Explorer, allowing users to directly request access to resources from these environments. The product also supports managing Active Directory groups.

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

Table 30: Hitachi ID Management Suite rating.

Overall, Hitachi ID Management Suite is an interesting product with a well-thought-out architecture and feature set, providing good flexibility. It thus is an interesting alternative to established products. The vendor still has a limited footprint outside of North America.

11.16 IBM Security Identity Manager

IBM Security Identity Manager, formerly known as IBM Tivoli Identity Manager (ITIM), is one of the more mature products in the market. The name change is due to the formation of an IBM Security Business Unit some time ago, when Tivoli products were shifted to that new unit and the brand name changed. However, it is still the same well-known product. IBM has a very large installed base, ranging amongst the top 5 vendors in the worldwide market in that aspect.

Strengths/Opportunities	Weaknesses/Threats
Mature product with strong support for standard Identity Provisioning features Strong support for different target systems Embedded Access Governance capabilities Significantly improved user interface	Multi-tenancy requires significant additional configuration, but partners provide fully multi-tenant implementations

Table 31: IBM Security Identity Manager major strengths and weaknesses.

IBM Security Identity Manager is an established product supporting a broad range of different target systems with deep integration. IBM has greatly improved the usability and user interface recently, providing a good and well-integrated product now. IBM also has made a significant number of additions to the functionality of IBM Security Identity Manager, including support for role management and enhanced workflow capabilities. The product supports multi-tenancy based on configuration and scripting. Various solutions and Cloud offerings are available.

IBM always has been strong on the connector side, providing a large number of connectors to virtually all manner of target systems. In addition, IBM provides integration with other products in its IBM Security portfolio. This makes the product a good fit when customers are looking for a comprehensive package of overall governance and security.

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

Table 32: IBM Security Identity Manager rating.

Overall, IBM Security Identity Manager is a mature offering that has undergone significant updates recently. IBM Security Identity Manager is among the products that have seen the strongest evolution over the past two years, making it a very competitive and interesting offering in this market. IBM also benefits from its own strong professional services and excellent partner ecosystem, plus the integration with the overall IBM Security product portfolio.

11.17 ILEX Meibo/MPP

ILEX is a French vendor which provides two different but closely related tools in the area of Identity and Access Management. Both are somewhat different from other provisioning approaches in that one is in fact a tool called Meibo, which allows customers to quickly create an Identity Management solution, while the other is named MPP (Meibo People Pack) and is focused primarily on SMBs. MPP, in fact, is a solution based on Meibo. Due to these considerations, neither are directly competing with the leading-edge products in the Identity Provisioning market, but fill gaps left by some of them and thus might be interesting options for particular customers.

Strengths/Opportunities	Weaknesses/Threats
Meibo as a flexible tool for creating custom Identity Management solutions. Integration with SSO/Access Management solution MPP as an out-of-the-box solutions targeted primarily towards SMBs	Only packaged feature set available out-of-the-box in MPP (SMB product). Meibo is a tool, not a solution Very limited visibility outside of France

Table 33: ILEX Meibo/MPP major strengths and weaknesses.

The approach of Meibo is interesting, however it is more a tool for creating custom Identity Management solutions like management or request interfaces to existing directories than it is a typical Identity Provisioning product. Thus, it might be complementary to existing Identity Provisioning products when it comes to building custom add-ons. Its strength is the tight integration with the Access Management and Single Sign-On solutions offered by ILEX. There is also a Role Management tool available now which allows designing role management applications which can be natively plugged into other Meibo solutions.

MPP on the other hand is a standard Identity Provisioning solution that is becoming increasingly feature-rich, but still lacking some common features and falling short in others. It is somewhat limited in role management and provides only a small number of reports out-of-the-box. On the other hand, it provides an overall good feature set now for Identity Provisioning that will be sufficient for many customers.

Security	positive (Meibo)/strong positive (MPP)
Functionality	neutral (Meibo)/positive (MPP)
Integration	neutral (Meibo)/positive (MPP)
Interoperability	positive (Meibo/MPP)
Usability	positive (Meibo/MPP)

Table 34: ILEX Meibo/MPP rating.

Overall, ILEX Meibo should be considered more an add-on to existing Identity Provisioning solutions, while the MPP product might be a fit primarily for SMBs. As an add-on and to rapidly and flexibly implement custom solutions, Meibo could provide significant value even in existing IAM deployments. We strongly recommend that Ilex expand its partner ecosystem to gain better visibility in global markets.

11.18 iSM Secu-Sys bi-Cube Identity & Access Management

iSM Secu-Sys is a German vendor which offers an Identity Provisioning solution with a well-thought out approach to role management and processes. In contrast to other vendors, iSM also delivers out-of-the-box standard processes for setting up provisioning. Overall, the conceptual strength of iSM is considerable. However, that also might become a limiting factor in projects given that the methodology and customer requirements have to be a good fit.

Strengths/Opportunities	Weaknesses/Threats
Broad set of functionality provided	Conceptual approach needs to be well understood
Well-thought-out role model and delivery of standard processes	Still very small partner ecosystem
Integrated Single Sign-On and strong authentication support	No footprint in the market outside of Germany and Austria

Table 35: iSM Secu-Sys bi-Cube Identity & Access Management major strengths and weaknesses.

A positive aspect of the product clearly is that it delivers a broad set of functionality based on a well-thought-out conceptual approach and methodology. Specific strengths are the role model and, as mentioned above, the standard processes provided. The product also provides integrated Single Sign-On capabilities and support for strong authentication. On the other hand there is a lack of integration partners and of visibility outside of the local markets.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 36: iSM Secu-Sys bi-Cube Identity & Access Management rating.

Overall, iSM bi-Cube is an interesting product offering, but with limited visibility in the market and beyond the local markets. Even though iSM Secu-Sys recently started a partner program, we strongly recommend they further invest in building a partner ecosystem and visibility within and beyond the home market. Customers have to understand the conceptual approach taken by iSM which provides strong flexibility but is rather specific.

11.19 Microsoft Forefront Identity Manager

Microsoft's offering in the Identity Provisioning market segment is the Microsoft Forefront Identity Manager (FIM), which has been recently extended with Access Governance capabilities that have been acquired in an asset deal from BHOLD. The product is pretty popular in Windows/Active Directory centric environments where it has its strengths. Despite the addition of Access Governance capabilities, FIM still follows a relatively technical approach to Identity Provisioning with focus more on synchronization than on workflows.

Strengths/Opportunities	Weaknesses/Threats
Microsoft recently has added Access Governance functionality Strong integration with Windows/Active Directory environments	Coding is required in many situations Still a pretty technical approach to Identity Provisioning No Cloud offering

Table 37: Microsoft Forefront Identity Manager major strengths and weaknesses.

With the addition of the BHOLD functionality Microsoft takes a significant step forward. However, these are in fact two different products with significant conceptual differences. It is not a fully integrated solution. A shortcoming of FIM is that it requires coding in many situations, more frequently than many other products in the market. Besides this, due to its concept, simple user interfaces and workflow-driven approaches frequently are implemented by either customization or using 3rd party products.

There is no Cloud offering of the product available. However, Microsoft recently has launched its Microsoft Azure Active Directory as a comprehensive Cloud IAM solution. Notably, Azure Active Directory is a fully separate solution, focusing on different capabilities from Microsoft FIM.

Security	strong positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 38: Microsoft Forefront Identity Manager rating.

Overall, Microsoft FIM is mainly an option either as part of some integrated provisioning products, focusing on Windows/Active Directory environments or environments which are heavily Windows/Active Directory-centric. Another option is deployment together with additional 3rd party solutions which add the missing features.

11.20 NetIQ Identity Manager

NetIQ Identity Manager is the former Novell Identity Manager which became part of NetIQ after the acquisition of Novell by The Attachmate Group. The product has one of the largest user bases globally. It is very mature, supporting a broad range of target systems with specific connectors. NetIQ Identity Manager is clearly targeted as an Identity Provisioning product with integrated role management and reporting capabilities. The product provides good baseline capabilities in Access Governance out-of-the-box.

Strengths/Opportunities	Weaknesses/Threats
Very large customer base and ecosystem Strong, mature functionality covering all major aspects of Identity Provisioning Strong support for a variety of target systems.	No full support for Access Governance yet, but good baseline capabilities Rich functionality sometimes complex to understand

Table 39: NetIQ Identity Manager major strengths and weaknesses.

NetIQ Identity Manager is a rock-solid workhorse for Identity Provisioning with mature and comprehensive capabilities in that area. Its approach for managing the environment based on the Designer tool is still widely unmatched in the industry, allowing for efficient management even of complex environments. The breadth of available functionality is somewhat complex when starting to work with the product, but that is true for other products as well.

NetIQ also offers a stand-alone Access Governance solution, NetIQ Access Governance Suite, which is tightly integrated with NetIQ Identity Manager for full Access Governance capabilities. That suite is based on a combination of NetIQ intellectual property and SailPoint IdentityIQ. Lastly, NetIQ Identity Manager integrates with complementary NetIQ Access Management and SIEM products for in-depth user activity monitoring.

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

Table 40: NetIQ Identity Manager rating.

Overall, Identity Manager from NetIQ remains a leading-edge product in the Identity Provisioning market segment with its broad, mature functionality. NetIQ also can build on an excellent partner ecosystem on global scale.

11.21 Omada Identity Suite

Omada, a Danish vendor, provides the Omada Identity Suite. Omada focuses on adaptable business-centric and collaborative features such as workflows, attestation and advanced access analysis, role management, reporting, governance and compliance and application management. This product is built on a Microsoft platform and offers an out-of-the-box integration with Microsoft Forefront Identity Manager Server (FIM Synchronization Server) for provisioning with backend systems. However this is not a mandatory component. Omada potentially also can use ESB (Enterprise Service Bus) integrations or connect to other provisioning systems. There are also some direct connectors to target systems. Furthermore, for extracting information from target systems for Access Governance requirements, the product also can rely on Microsoft SQL Server Integration Services (SSIS). However, the common deployment model remains the integration with Microsoft FIM.

Strengths/Opportunities	Weaknesses/Threats
Mature solution with strong workflow and role management capability	Limited out-of-the-box connectivity to target systems, typically requires an additional fulfillment layer
Efficient approach for onboarding new applications	No out-of-the-box integration with Service Request Management (SRM) systems
Enhances Microsoft FIM in various areas, including SAP connectivity	

Table 41: Omada Identity Suite major strengths and weaknesses.

In the common deployment model, Omada offers a modularized solution, fully based on the Omada web portal that supports the core features. Actual data are imported directly form target systems to Omada's Identity & Access Data Warehouse, and provisioning is done via FIM Synchronization Services (FIM Server) or other fulfilment technologies. Omada offers its own connectors (Management Agents) for FIM Server to connect to strategic environments such as SAP systems. These features can be provided for any other underlying provisioning technology as well.

This approach has its strengths and weaknesses. Opting for Omada Identity Suite commonly, but not necessarily, implies opting for Microsoft FIM Server, requiring licensing of both products (but no FIM CALs). In virtually any case for Identity Provisioning, it requires an additional fulfillment layer. The features of Omada Identity Suite are potentially available for other fulfillment options (i.e. other provisioning solutions) but with no out-of-the-box integrations as of now. This is expected to change over time and has been done by Omada on a project basis. The strong support for SAP environments and the added features for workflows, role management, Access Governance, and other business-centric functions, on the other hand, is a strength. Another interesting option is the ability of Omada to quickly onboard new applications in a structured process.

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

Table 42: Omada Identity Suite rating.

Overall, Omada Identity Suite is a very interesting solution for enterprise customers but especially those with focus on Microsoft and/or SAP environments, and in combination, yields a leading-edge offering in the Identity Provisioning and Governance market. Besides that the product might be used as an integration layer on top of other or even multiple Identity Provisioning tools. The rating is based on the integrated approach with Microsoft FIM Server.

11.22 OpenIAM Identity Manager

OpenIAM Identity Manager is one of the Open Source offerings in the Identity Provisioning market and counts among the more mature of these products. The product provides a significant number of connectors, including a restful service connector allowing quick connection to Cloud services. In addition, there are a number of out-of-the-box connectors to leading Cloud services.

Strengths/Opportunities	Weaknesses/Threats
Open Source solution with a good baseline functionality for IAM	Shortcomings in the self-service interfaces
Integrated SSO and Federation capabilities	No support for managing roles
Support for provisioning to Cloud services	Still relatively small partner ecosystem
Available as hardware appliance	

Table 43: OpenIAM Identity Manager major strengths and weaknesses.

In contrast to other Identity Provisioning solutions, OpenIAM Identity Manager also provides integrated capabilities for Identity Federation and web-based Single Sign-On. This comes together with strong support for various authentication methods, allowing customers to securely access the administrative interfaces. A rather rare feature in the market is the availability of the product as a hardware appliance, which might be interesting especially for smaller organizations.

OpenIAM Identity Manager as of now is largely focused on the administrators. It provides a good interface for these, allowing them to manage the environment. However, it lacks strong self-service capabilities for end users, such as shopping cart functionality. We see room for improvement in that area. Also currently lacking is baseline support for role management.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	positive
Usability	neutral

Table 44: OpenIAM Identity Manager rating.

OpenIAM Identity Manager is an interesting option in the Identity Provisioning market, especially when it comes to managing hybrid environments. It provides good connectivity to Cloud services. We still see room for improvement for user self-services, but the overall administrative interface leaves a positive impression. OpenIAM still has a relatively small partner ecosystem and should work on growing that globally.

11.23 Oracle Identity Governance Suite

Oracle Identity Governance Suite is the Identity Provisioning component within the Oracle IAM portfolio. It provides mature capabilities in that area which have again been significantly improved with the 11g R2 release. Oracle over the years has acquired a lot of different products. However, the company had defined a clear strategy for integration and is successfully delivering on that strategy. This includes providing a consistent approach to service interfaces and other integrations. A consequence of that strategy is that Oracle tries to avoid redundancies and overlap of products. Thus, in some areas other Oracle products might be required to provide specific functionality – which is not uncommon for the IAM portfolios of large vendors.

Strengths/Opportunities	Weaknesses/Threats
Mature, feature-rich product focused on Identity Provisioning Clear separation of functionality from other modules of Oracle IAM portfolio Very broad support for different environments and enterprise-level architectures	Depending on use cases there exist several dependencies on other components of the Oracle IAM portfolio

Table 45: Oracle Identity Governance Suite major strengths and weaknesses.

Oracle Identity Governance Suite, being a powerful solution, has been considered a relatively complex product regarding installation, basic configuration, and customization. With the new release, Oracle has made significant progress in these areas. Important changes include an extensible data model. Customizations can be done without coding in many situations and are clearly segregated from Oracle code. Features like shopping cart approaches have been implemented. Still a shortcoming is the fact that some few connectors are provided by third parties, which might lead to issues regarding implementation support. On the other hand, Oracle Identity Governance Suite gains by its enterprise-level design, supporting modern architectural concepts like externalized workflow systems and other features.

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

Table 46: Oracle Identity Governance Suite rating.

Overall, Oracle Identity Governance Suite counts among the leading-edge products in the market. It provides a broad set of features focused on Identity Provisioning and good support for enterprise-level architectures, including external workflow systems. Oracle has an excellent partner ecosystem.

11.24 SailPoint IdentityIQ

SailPoint originally started as a vendor specialized in Access Governance. However, since 2010 they have invested in the Identity Provisioning market on one hand by taking over the former BMC Control-SA team and licensing assets and on the other hand by extending the technical capabilities of their IdentityIQ flagship product. The SailPoint IdentityIQ product now is a solution that integrates Access Governance and Identity Provisioning capabilities into a single product. In contrast to most other vendors, SailPoint provides its own Identity Provisioning connector technology but also provides out-of-the-box connectivity to Identity Provisioning solutions of other vendors.

Strengths/Opportunities	Weaknesses/Threats
Strong integrated Identity Provisioning and Access Governance capabilities Integration capabilities with other provisioning systems and SRM out-of-the-box User-friendly interfaces	No multi-tenancy support, but delivering separate Cloud solution IdentityNow

Table 47: SailPoint IdentityIQ major strengths and weaknesses.

Due to its origin in the Access Governance market, the IdentityIQ user interfaces are geared towards business users. The approach in general is very much business-driven and less technology-focused than what some of the “classical” vendors in that market provide. The user interfaces are quite flexible configurable.

SailPoint has made significant progress with respect to the Identity Provisioning capabilities. They not only extended the number of connectors, but also the depth of various connectors such as the one for SAP systems. Only few mainframe connectors rely on BMC Control-SA technology, however that is an area where these connectors have been leading-edge. Besides supporting connectivity to target systems via Identity Provisioning, the product also directly supports integration with SRM (Service Request Management) tools. Among the shortcomings is the lack of multi-tenancy support.

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

Table 48: SailPoint IdentityIQ rating.

SailPoint has become a leading-edge vendor in the Identity Provisioning market now. They are providing a feature-rich and increasingly mature solution. In addition, they have excellent support for Access Governance capabilities as part of the offering.

11.25 TrustVerse Cube

TrustVerse is a vendor based in Moscow, Russia. Their Cube solution is a standard IAM product that allows provisioning changes to various systems. Trustverse currently only provides a Russian user interface but is working on supporting other languages as well. The customer base still is limited and based in Russia and adjacent countries.

Strengths/Opportunities	Weaknesses/Threats
Provides baseline functionality for Identity Provisioning	Limited localization, no English version as of now
Allows managing entitlements at the system-level	Very small partner ecosystem and limited customer base
Provides APIs to access functionality	No support for delegated administration

Table 49: TrustVerse Cube major strengths and weaknesses.

TrustVerse Cube provides baseline functionality for Identity Provisioning, with acceptable support for connectors to target systems. A strength is their ability to support managing of the fine-grained rights at the system-level with continuous monitoring of target systems. It furthermore allows accessing the product functionality as services through the use of APIs.

On the other hand, the product lacks several common features. It is focused primarily on managing employees, not focusing that much on other types of identities such as consumers. However, aside of the standard deployment with strong HR focus, other implementation models are supported on a per-project basis. In the standard product, it still lacks the ability to delegate administration, which is a key requirement of many customers. Again, there are per-project implementations including that capability. We also see room for improvement in various other areas such as out-of-the-box reports or additional deployment models. The product also currently lacks a graphical workflow engine.

Security	neutral
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	weak

Table 50: TrustVerse Cube rating.

TrustVerse Cube is clearly not a leading-edge product as of now and lacks localization to address markets in other regions. However, there is potential in extending the product and scale to other markets, especially when focusing on the Eastern European and APAC (Asia/Pacific) markets and on medium-sized businesses. We will continue watching TrustVerse and their progress.

11.26 WSO2 Identity Server

WSO2 is a company based in Palo Alto, CA. They provide a platform for connecting businesses, based on SOA (Service Oriented Architecture) concepts. The approach differs from common approaches by not focusing only on IAM. They deliver a product called Identity Server that provides IAM capabilities, including Identity Provisioning features. Due to their concept of targeting more towards connecting businesses with partners and customers, their support for on-premise Identity Provisioning requirements is somewhat limited.

Strengths/Opportunities	Weaknesses/Threats
Full support for SCIM	Still limited number of connectors, primarily targeted towards Cloud services
Built-in support for multi-tenancy	Lack of support for certain standard features such as reconciliation, but strong workflow capabilities on customization
Full support for APIs	No integrated reporting with standard reports

Table 51: WSO2 Identity Server major strengths and weaknesses.

When looking at the WSO2 Identity Server from the Identity Provisioning perspective, there are some strengths. One is that the product has good capabilities in supporting Cloud services, with SCIM being the standard approach for connectivity to target systems. There is also out-of-the-box support for multi-tenancy and full support for managing and using the capabilities of the product via APIs. Other features to mention positively are the broad support for authentication mechanisms and their integrated support for Dynamic Authorization Management. Also, they provide strong workflow capabilities and well thought-out security concepts.

However, when looking at core Identity Provisioning capabilities, there are various shortcomings. There are no standard IAM processes deployed. A shopping cart for access request management is missing. There are no Access Governance capabilities yet. The WSO2 Identity Server provides a foundation and we find several of these features on the roadmap, but as of now there are various gaps. The more customers are looking for a service engine for Identity Provisioning, the better WSO2 Identity Server and the overall WSO2 platform fit. Customers looking for a strong out-of-the-box feature set will not find everything they want.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	positive
Usability	neutral

Table 52: WSO2 Identity Server rating.

Customers have to carefully analyze whether WSO2 Identity Server meets their requirements. While the product is an interesting pick when looking at the entire WSO2 platform for integrating businesses with partners and customers, there are shortcomings for pure-play Identity Provisioning. If flexibility and adaptability count, the WSO2 platform is definitely interesting, especially for building an identity service layer.

12. Products at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Identity Provisioning. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

12.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 53.

Product	Security	Functionality	Integration	Interoperability	Usability
Atos DirX Identity	strong positive	positive	positive	positive	positive
Avatier Identity Management Software Suite	positive	positive	strong positive	positive	strong positive
Avencis Hpliance: IAM solution	positive	neutral	neutral	neutral	positive
Beta Systems SAM Enterprise Identity Management Suite	strong positive	strong positive	positive	positive	positive
CA IdentityMinder	strong positive	strong positive	positive	strong positive	positive
Courion Access Assurance Suite	strong positive	strong positive	strong positive	strong positive	positive
CrossIdeas IDEAS	strong positive	positive	neutral	neutral	strong positive
Deep Identity IACM/IM/FsGA	positive	neutral	positive	neutral	positive
Dell One Identity Manager	strong positive	strong positive	strong positive	positive	strong positive
EmpowerID	strong positive	strong positive	positive	positive	strong positive
Evidian Identity & Access Manager	strong positive	positive	positive	positive	positive
Evolveum midPoint	positive	positive	neutral	neutral	neutral
Fischer Automated Role & Account Management	strong positive	positive	strong positive	strong positive	strong positive
ForgeRock OpenIDM	positive	positive	strong positive	positive	neutral
Hitachi ID Management Suite	strong positive	positive	strong positive	strong positive	positive
IBM Security Identity Manager	strong positive	strong positive	strong positive	strong positive	strong positive
ILEX Meibo	positive	neutral	neutral	positive	positive
ILEX MPP	strong positive	positive	positive	positive	positive
iSM Secu-Sys bi-Cube Identity & Access Management	strong positive	positive	positive	neutral	positive
Microsoft Forefront Identity Manager	strong positive	positive	neutral	neutral	neutral

Product	Security	Functionality	Integration	Interoperability	Usability
NetIQ Identity Manager	strong positive	strong positive	positive	strong positive	strong positive
Omada Identity Suite	strong positive	positive	strong positive	positive	strong positive
OpenIAM Identity Manager	positive	neutral	neutral	positive	neutral
Oracle Identity Governance Suite	strong positive	strong positive	strong positive	strong positive	positive
SailPoint IdentityIQ	strong positive	strong positive	strong positive	strong positive	strong positive
TrustVerse „Cube“	neutral	neutral	neutral	neutral	weak
WSO2 Identity Server	positive	neutral	neutral	positive	neutral

Table 53: Comparative overview of the ratings for the product capabilities.

In addition we provide in table 54 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Atos	positive	positive	strong positive	neutral
Avatier	positive	positive	positive	neutral
Avencis	positive	neutral	neutral	weak
Beta Systems	positive	positive	positive	positive
CA Technologies	strong positive	strong positive	strong positive	positive
Courion	strong positive	strong positive	positive	positive
CrossIdeas	positive	neutral	neutral	positive
Deep Identity	positive	critical	critical	weak
Dell	strong positive	strong positive	strong positive	strong positive
EmpowerID	positive	positive	positive	positive
Evidian	positive	positive	positive	neutral
Evolveum	positive	critical	weak	weak
Fischer International	positive	positive	positive	neutral
ForgeRock	positive	positive	positive	strong positive
Hitachi ID	strong positive	positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
ILEX	positive	neutral	neutral	weak
iSM Secu-Sys	positive	weak	weak	weak
Microsoft	neutral	strong positive	strong positive	strong positive
NetIQ	strong positive	strong positive	strong positive	strong positive
Omada	positive	positive	positive	positive
OpenIAM	neutral	neutral	neutral	neutral
Oracle	strong positive	strong positive	strong positive	strong positive
SailPoint	strong positive	positive	positive	strong positive
TrustVerse	neutral	weak	weak	critical
WSO2	neutral	neutral	weak	neutral

Table 54: Comparative overview of the ratings for vendors.

Table 54 requires some additional explanation regarding the “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, and others.

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

In 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 is also based on some other criteria. This doesn’t imply that the vendor is in a critical financial situation; however the potential for massive investments for quick growth appears to be limited. On the other hand, it’s also possible that vendors with better ratings might fail and disappear from the market.

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

12.2 The Market/Product Matrix

Beyond that analysis, we’ve 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.

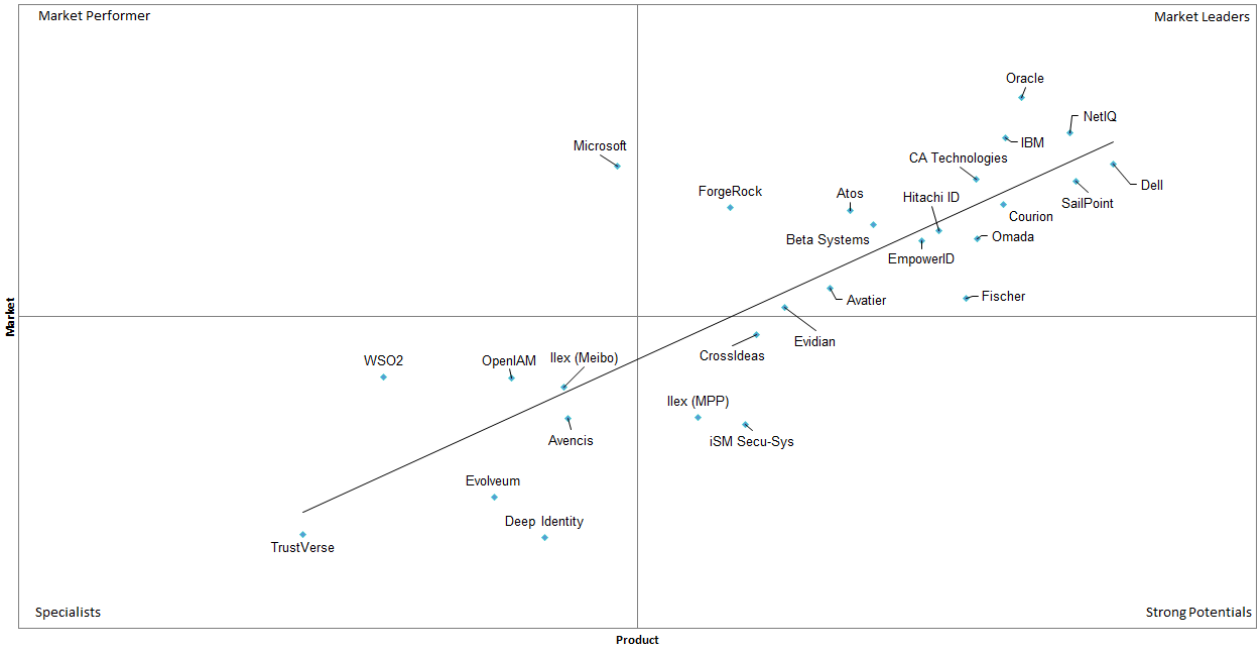

Fig. 8: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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

In the Market Leaders segment, we see a large number of vendors. Vendors towards the upper right are the ones that have both strong product features and a significant market presence.

In the Strong Potentials section, we see only three vendors. CrossIdeas, Ilex with their MPP offering, and iSM Secu-Sys all are players that show a strong overall product functionality but have a relatively limited number of customers and/or a small partner ecosystem. This is commonly combined with limited global presence. All three of these vendors appear to be interesting alternatives to the Market Leaders.

On the other hand, we see only Microsoft in the Market Performer section of the graphic. This indicates vendors that are not leading-edge in product functionality but pretty good in sales. Microsoft builds on its success in "Microsoft shops" where FIM frequently is the product of choice.

Finally, there is the Specialists section that is also somewhat crowded. Here we find a number of players. While some are rather new and still evolving their products, such as TrustVerse and Evolveum, others take a different approach to Identity Provisioning or deliver Identity Provisioning more as a by-product to other functionality. The latter include WSO2, Ilex with its Meibo product, and Deep Identity. All specialists might be a perfect fit for some customers, but require careful evaluation. In some cases they even might be the best fit, due to the fact that they frequently provide rather specialized tools that might suit some use cases better than standard Identity Provisioning tools.

12.3 The Product/Innovation Matrix

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

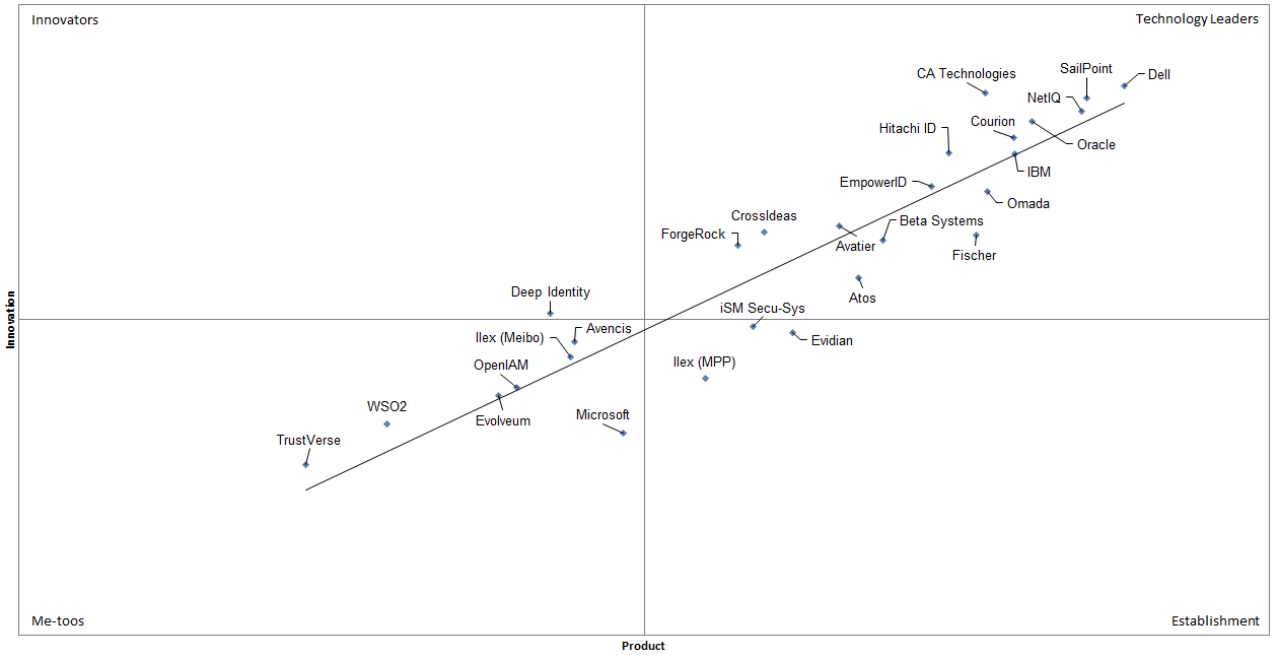

Fig. 9: The Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.

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 this 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 provide specialized point solutions. However, in most cases this is more about delivering what others have already created.

Again we see a large number of vendors in the upper right segment of the matrix, which we define as the Technology Leaders segment. These vendors show good to excellent innovation and provide strong product capabilities.

When looking at the Establishment segment, we see three vendors. Both iSM Secu-Sys and Evidian are close to the Technology Leaders segment. Their rating is based on the fact that we miss some of the more innovative features in both offerings, while they provide other interesting features. Ilex with its MPP product has shown significant progress over the past two years but still lacks several of the more innovative features.

The Innovators segment contains only one vendor, Deep Identity. They are rather innovative, even with respect to some Identity Provisioning features, but fall short of providing the full baseline capability for Identity Provisioning we expect to see.

The Me-Too section not only contains me-too-vendors, but also some vendors that are taking a somewhat different approach to Identity Provisioning, such as WSO2 and Ilex with their Meibo product. Vendors in that segment might be interesting anyhow, being local players or providing solutions that are targeted well for SMBs.

12.4 The Innovation/Market Matrix

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

Fig. 10: The Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relative 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 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 this 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 given 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 among the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Again, this matrix contains several large players in the Big Ones section – vendors that both hold a significant market share and execute well in adding innovative features to their products.

In the Top Sellers segment we find three vendors. Evidian is very close to the Big Ones segment, but lacks some of the more innovative features we'd like to see. Microsoft delivers a product with little innovation, but succeeds well in the market, especially within their established customer base.

More interesting is the Hidden Gems segment. We only see two vendors there, CrossIdeas and Deep Identity. Both show a significant potential for further success. Some other vendors, primarily iSM Secu-Sys and Avencis, are close to entering that segment.

These two, among others, form the Point Vendors segment that contains smaller, regional, and specialized vendors. Again, these vendors might be a good choice for many customers, but are not yet ready to fully compete with the large players for all Identity Provisioning scenarios.

13. Further Analysis

Beyond looking at the overall capabilities of the products, we provide additional views looking at the particular strength of products for specific use cases. For this Leadership Compass on Identity Provisioning, there are two distinct areas we look at:

- Identity Provisioning capabilities, focusing on the traditional pure-play Identity Provisioning features provided by the products. Vendors that are exceptionally strong in that area but not as strong in the overall product rating might still be a good fit for customers looking only for an Identity Provisioning solution, but not for Access Governance features. That might for instance be the case when an Access Governance solution is already in place.
- Access Governance capabilities, for those customers looking for a solution that is good enough in Identity Provisioning but exceptionally strong in Access Governance. This is of particular interest for customers looking for a single solution covering both their Identity Provisioning and Access Governance requirements at a high level. However, many customers will not need outstanding Access Governance capabilities, given that Access Governance requires a strong organizational backing in guidelines and processes and many organizations are not mature enough yet to successfully implement advanced Access Governance within their organization.

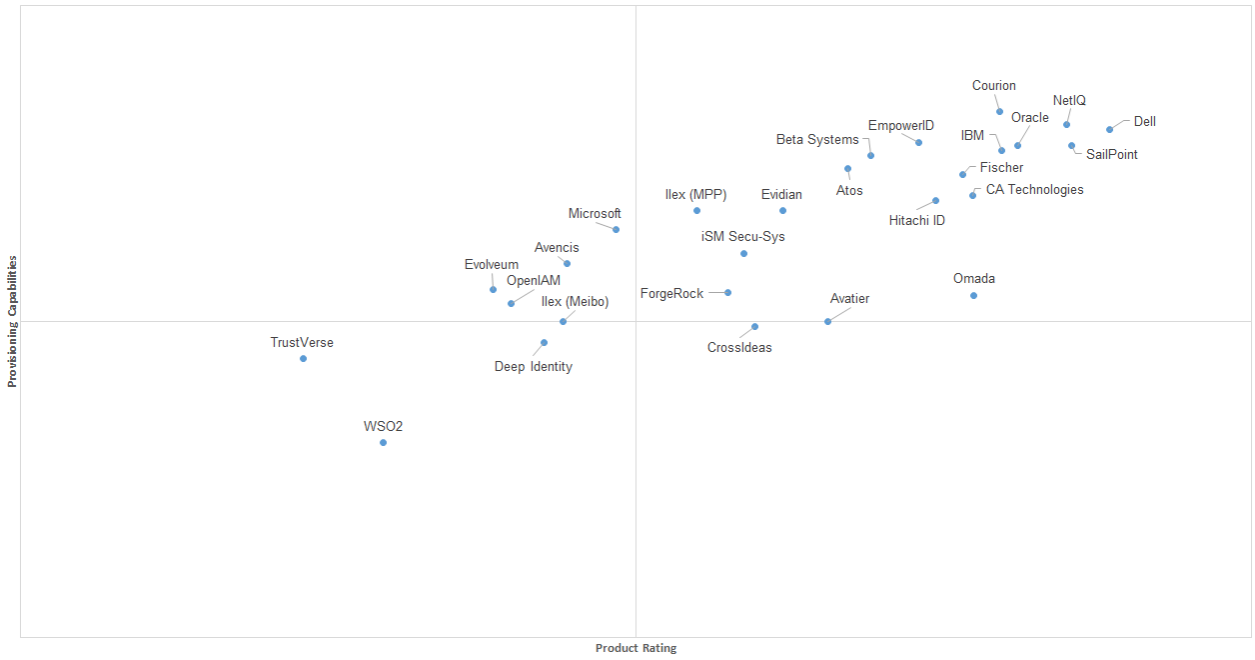

Fig. 11: The Provisioning Capabilities/Product Matrix. Vendors towards the top are performing well in Provisioning, while vendors towards the right are performing well in overall product capability.

Both matrixes (Fig. 11 and Fig. 12) show a strong correlation between the overall product capabilities and the specific capabilities for Identity Provisioning and Access Governance. However, when looking at these figures in more detail it becomes obvious that some vendors are stronger in the one or the other area. To analyse the figures it is important to particularly look at the vendors on top. Vendors near the top but more to the left have their strength in Identity Provisioning.

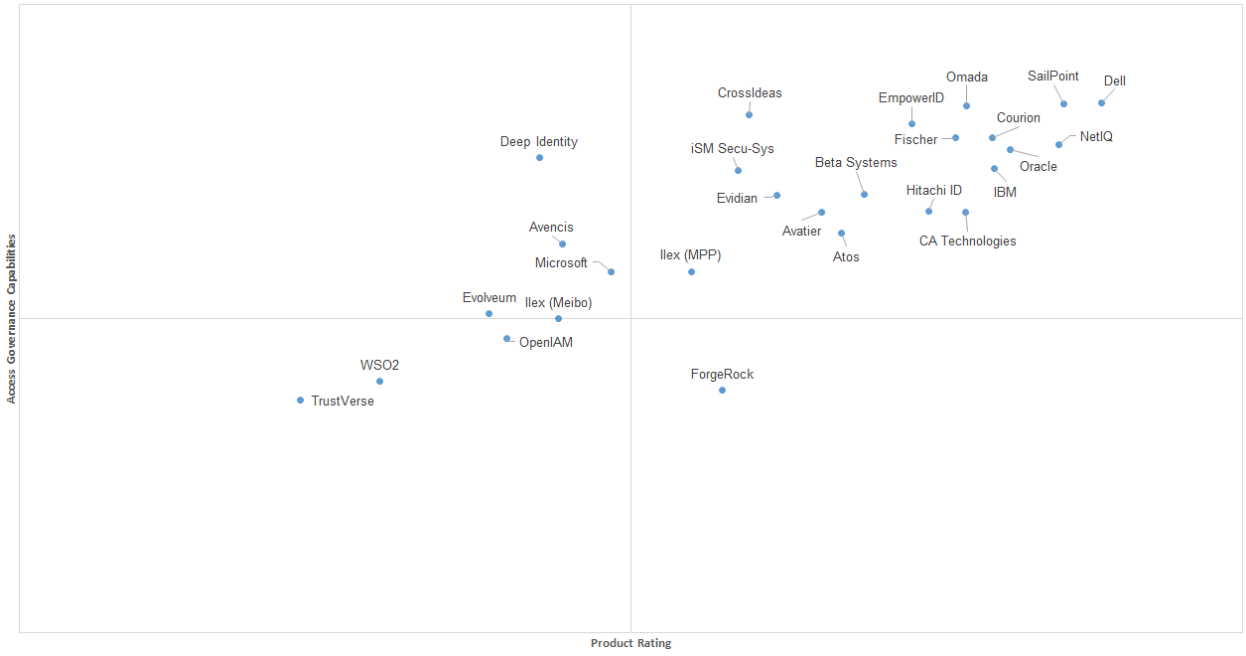

Fig. 12: The Access Governance Capabilities/Product Matrix. Vendors towards the top are performing well in Access Governance, while vendors towards the right are performing well in overall product capability.

This becomes even more visible in the comparison of Access Governance capabilities and the overall product capabilities.

Some vendors such as CrossIdeas, Deep Identity, and to some extent also iSM Secu-Sys are clearly stronger in Access Governance. These are, among the established players with strong Access Governance capabilities more to the right, the logical picks for customers looking for integrated solutions or – for the ones more to the left, which are not leading in overall product capabilities – for implementations where only basic Identity Provisioning capabilities but strong Access Governance features are required.

Again, product decisions must not be made solely based on these matrixes but always require a thorough analysis of the requirements and the products, beyond the information provided in this document.

14. Overall Leadership

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 13.

Fig. 13: The Overall Leadership rating for the Identity Provisioning market segment.

When looking at the Overall Leaders, we see most of the expected large players in front. This is partially based on the fact that they are Market Leaders, which goes into the Overall Leadership rating. We see Oracle, Dell, NetIQ, IBM, SailPoint, and CA Technologies competing head-to-head in that rating, Microsoft is not an overall leader due to their rather weak position in the Innovation Leadership and Product Leadership ratings. SAP declined participating in this edition of the KuppingerCole Leadership Compass Identity Provisioning due to upcoming major release changes.

The Overall Leadership rating also shows a number of other vendors in the Leaders category. These include Atos, Beta Systems, Courion, EmpowerID, Hitachi ID, and Omada. All of these vendors can build on a strong customer base and mature products. We also see Avatier, ForgeRock and Fischer as vendors being very close to entering the Overall Leadership section.

Behind these leading companies, we see a large number of other vendors in the Challenger segment. Especially the ones further to the right in that segment definitely are interesting candidates for any long list in product decisions, namely CrossIdeas, Evidian and Microsoft.

The other vendors also have interesting offerings but commonly lack in one or another area, such as market presence, customer base, and ecosystem, or are specialized vendors such as Ilex that provide solutions taking a somewhat different approach to Identity Provisioning. All of these vendors might be a fit for customers, depending on their specific needs such as looking for Open Source products or regional players.

Again: Leadership doesn't 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):

- Atos
- Beta Systems
- CA Technologies
- Courion
- Dell
- EmpowerID
- Hitachi ID
- IBM
- NetIQ
- Omada
- Oracle
- SailPoint

15. Vendors and Market Segments to watch

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

15.1 SAP

SAP with its NetWeaver Identity Management product is one of the established players in the Identity Provisioning market. They have gained a significant market share, particularly among customers heavily relying on SAP for their business applications. NetWeaver Identity Management is a solid Identity Provisioning solution. However, due to upcoming major releases with significant changes in functionality, SAP declined participating in this edition of the KuppingerCole Leadership Compass on Identity Provisioning. We nevertheless see SAP, also with its current product, as an option in this market segment. We also recommend that customers closely follow upcoming SAP announcements in this field to take them into account when selecting Identity Provisioning solutions.

15.2 RSA Aveksa

RSA Aveksa Identity Management & Governance (RSA Aveksa IMG Platform) is based on the former Aveksa Access Governance Platform. The product consists of five components:

- Access Certification Manager
- Business Role Manager
- Access Request Manager
- Data Access Governance

- Access Fulfillment Express (AFX)

The Access Certification Manager is the component that supports recertification as one of the key functionalities within Access Governance. However, it is not limited to the recertification process itself, which can be based on configurable workflows. This component also provides the collection features that allow accumulating the current entitlements from target systems and correlating the user identities based on various attributes. Furthermore, it is the module where controls are defined. These business rules and compliance policies allow identifying risks and violations, especially around SoD conflicts (Segregation of Duties).

The Business Role Manager is the second component, which allows managing business roles. It supports role mining features, by collecting and correlating entitlements across systems and identifying potential roles. It allows defining role models top-down, with a flexible role model that can hold multiple levels and types of roles, depending on the customer requirements. It also supports further analytics and reporting, for instance for identifying critical roles that have excessive entitlements.

The Access Request Manager is another key component, enabling business users to request access through a self-service interface. Depending on configuration, they can request access and make changes at various role levels. Policies are checked when access is requested. That enables proactive policy enforcement, before entitlements are actually granted at the system level.

All access requests run through configurable workflows, allowing the definition of approval policies as required. Furthermore, the system keeps control of the status of these processes, even when these are handed over for manual fulfillment. It even delivers an interface for the operators that have to perform the manual fulfillment requests. In addition, there is support for integrating with existing SRM products. Again, there are reporting and analysis capabilities provided for that portion of the product's functionality.

The Data Access Governance module in fact is the component that enhances the functionality of the RSA Aveksa IMG Platform towards EAG. It provides visibility and management for connected systems. As of now, Microsoft Windows file servers, several flavors of network-attached storage, and Microsoft SharePoint servers are supported. For these platforms, detailed analytics of the current entitlements are provided. Compliance policies can be defined and enforced.

Finally, there is the AFX (Access Fulfillment Express). This is the provisioning component of the RSA Aveksa IMG Platform. The product is increasingly moving towards a full-featured Identity Provisioning product, but uses another approach for connecting to target systems than most of the other systems in the market. AFX is based on a modular architecture that allows quickly creating connectors to target systems, for writing changes to these systems. Thus, automated changes can be implemented if required. The number of standard connectors is increasing. In addition, it can integrate with existing Identity Provisioning systems to leverage these as an "execution layer". This allows customers to maintain existing investments and add an Access Governance layer on top for new functionality and business integration.

15.3 Econet

Econet is a German provider of an IAM solution, that provides Identity Provisioning capabilities, but also functions for consolidating and managing file services and auditing file system access controls. While their set of connectors is somewhat limited, they provide a number of capabilities for managing other types of resources and IT services out-of-the-box.

15.4 Tools4ever

Tools4ever is a provider of various IAM solutions. With their UMRA Identity and Access Management Software, they provide an interesting option with a significant number of connectors and features such as Role-based Access Control (RBAC). From our perspective, they are an interesting option for both SMB customers and organizations looking at Identity Provisioning primarily from a system-administrator perspective. We consider Tools4ever an interesting alternative to established players that might be taken into account in vendor selection processes.

15.5 NetProf

NetProf as of now is focused on a specialized Identity Provisioning solution targeting the Education market segment. Thus, their offering is rather specialized, however providing some interesting specific capabilities. NetProf plans to offer a standard Identity Provisioning solution towards the end 2014.

15.6 ITConcepts Cognitum

Cognitum is a development platform for IAM solutions that allows quickly creating IAM solutions, based on connectivity to target systems and integrated workflow capabilities. Cognitum is based on the former BMC Calendra product. Based on Cognitum, ITConcepts has started offering a highly standardized IAM solution for SMBs as well, allowing for rapid deployment of a standardized solution. While Cognitum itself is attractive as a complementary tool for all IAM deployments, the standard solution is primarily targeted on SMBs.

16. Copyright

The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought Leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

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

Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

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