kuppingercole ANALYSTS

KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | November 2017

Identity Provisioning

Leaders in innovation, product features, and market reach for Identity Provisioning. Delivering the capabilities for managing accounts and entitlements across heterogeneous IT environments on premises and in the cloud. Your compass for finding the right path in the market.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2017

Leadership Compass
Identity Provisioning
By KuppingerCole

KuppingerCole Leadership Compass
Identity Provisioning
Report No.: **71139**

Content

Content of Tables

Content of Figures

Related Research

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

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

Advisory Note: Enterprise Role Management - 70285

Executive View: Avatier Identity Management Suite - 71510

Executive View: EmpowerID - 70894

Executive View: Hitachi ID IAM Suite - 72540

Executive View: Omada Identity Suite v11.1 – 70835

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

Executive View: SailPoint IdentityIQ - 71319

Executive View: SAP HANA Cloud Platform Identity Authentication and Provisioning - 70290

Executive View: Saviynt Identity Governance and Administration (IGA) 2.0 - 71506

Executive View: Cloud Standards Cross Reference - 71124

Leadership Compass: Privilege Management - 72330

Leadership Compass: CIAM Platforms - 70305

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings in a certain market segment. This Leadership compass focuses on the market segment of Identity Provisioning. While there are many vendors that have integrated offerings, combining Access Governance and Identity Provisioning into what today frequently is named IGA (Identity Governance and Administration), others continue offering separate products for the two areas of IGA or cover only one of the two.

More important, still many customers are looking either for an Identity Provisioning solution with only baseline Access Governance capabilities or they focus on Access Governance. The latter can be the case if they already have Identity Provisioning in place or when their starting point is Access Governance. Some of the scenarios we observe in the market are based on service infrastructures, where Access Governance is run by the organization itself, while fulfillment through Identity Provisioning is a managed service. Reality is that there are various scenarios and many customers that either only need Identity Provisioning or Access Governance, but not a combined solution.

Therefore, we decided to create three distinct Leadership Compass documents in that area:

- LC Identity Provisioning: This Leadership Compass focuses on solutions with strong support for Identity Provisioning. We expect some baseline Access Governance capabilities. However, we also look at complete IGA offerings if they have strong Identity Provisioning support.
- LC Access Governance: Here, the focus is on Access Governance capabilities, with only the required integration into Identity Provisioning tools. Again, we also look at complete IGA offerings if they have strong Access Governance capabilities.
- LC Identity Governance and Administration: In the third Leadership Compass, our focus is only on offerings that are strong in both their Identity Provisioning and their Access Governance capabilities. This includes single product offerings, but also offerings that are combinations of separate offerings from the same vendor and, in combination, deliver strong IGA capabilities.

These three LCs are complemented by two other Leadership Compass documents. One focuses on comprehensive IAM suites, which add further capabilities such as Privilege Management, Enterprise SSO, Identity Federation and Web Access Management to IGA in integrated offerings. The other focuses on IGA for SMBs (small and medium businesses), which have different requirements on IGA solutions than large organizations commonly have.

With the various LCs, we provide customers the information they need to select vendors based on their specific use cases, whether these are IGA-driven, provisioning-driven, or e.g. focused on one comprehensive, integrated IAM suite.

1.1 Market Segment

Identity Provisioning is, despite the rise of integrated IGA offerings, one of the core segments of the overall IAM market – and it is an essential part of IGA anyway. 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.

Identity Provisioning products are commonly organized around some key components:

- Workflow engine for supporting request and approval processes and automation of the management of identities and access
- Connectors that allow interfacing with a variety of target systems
- Connector toolkits for rapidly adding custom connectors
- Identity repository, managing the links between the identities managed by the provisioning system and the accounts in the connected systems
- Reconciliation engine for identifying unauthorized changes in target systems
- User self-services for e.g. password resets and managing their own identities
- Delegated administration capabilities

Most solutions also provide some level of Access Governance capabilities. However, for this Leadership Compass, we only looked at very baseline capabilities in that area, not expecting sophisticated features.

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

Finally, as requests were now handled directly by business owners or end-users, traditional command lines became a "no go" option and a friendly graphical UI became one of the most important components of any Identity Provisioning implementation.

Identity Provisioning has changed over the years. But Identity Provisioning still is an essential capability for organizations, not only for managing user accounts and their access in on premises systems, but also in cloud services. Whether such solutions are implemented isolated, as pure-play Identity Provisioning, or in combined offerings, depends on the current IT infrastructure, the IT service and delivery model, and the specific requirements of the customer. But some form of Identity Provisioning is inevitable for any mid-sized and large IT infrastructure.

1.2 Delivery models

This Leadership Compass is focused on offerings that run on premises, either at the customer or at a Managed Service Provider (MSP). We do not look at IDaaS (Identity as a Service) offerings in that Leadership Compass.

KuppingerCole has published Leadership Compass documents on IDaaS, including IDaaS B2E, which is focused on IDaaS solutions supporting IGA for hybrid environments, delivered as a service.

1.3 Required Capabilities

When evaluating the products, we look, generally speaking, 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

Within the area of functionality, the required capabilities are centered around the key components listed above:

- Workflow support for request and approval processes
- Workflow/process support for automating the management of identities and access, i.e. the flow of data back and forth from and to target systems
- Tools that graphically support creating and customizing workflow
- Breadth and depth of connectors that allow interfacing with a variety of target systems
- Cloud connectors, adding provisioning support for common cloud services
- Connector toolkits for rapidly adding custom connectors
- Identity repository, managing the links between the identities managed by the provisioning system and the accounts in the connected systems
- Customization of mapping rules between central identities and the accounts per target system
- Reconciliation engine for identifying unauthorized changes in target systems
- User self-services for e.g. password resets and managing their own identities
- Delegated administration capabilities

Beyond that, we also considered some specific features. These include, amongst others:

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) and in particular SCIM is recommended.
Deployment models	Supporting different deployment models like hard/soft appliances and optional MSP services 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.
Mobile interfaces	Secure apps providing access to certain key capabilities of the product.
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.
Baseline Access Governance	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.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 1: The Overall Leadership rating for the Identity Provisioning market segment

When looking at the Overall Leader segment in the Overall Leadership rating, we see a picture that is common for mature market segments, where a significant number of vendors delivers solutions with a rich feature set. The market is very crowded, with close to 30 vendors we have considered in our rating plus several other vendors we have listed in the “vendors to watch” section.

For Overall Leadership, we find SailPoint slightly in front, closely followed by a group of three vendors, consisting of Micro Focus, Oracle, and CA Technologies. Next to them we find IBM and EmpowerID, followed by ForgeRock, One Identity, and Hitachi ID. All these vendors have an established market presence in the Identity Provisioning market segment, with EmpowerID and Hitachi ID being the two least known of these vendors, but both delivering comprehensive offerings, positioning them clearly in the Overall Leaders segment.

SAP also made its entry into the Overall Leader segment, after maturing and enhancing their product significantly over the past years. Further vendors we find in this segment include Avatier, Beta Systems, Omada, Evidian, Pirean, and Core Security. All provide solutions which move them, in combination with their ratings on Market Leadership and Innovation Leadership, into the Overall Leader segment.

The Challenger segment is also well-populated. The vendors in this segment also provide strong offerings, which challenge the established players. Some of the vendors in this segment benefit more from their strong market position, while others such as Beta Systems are higher placed in Product Leadership. We strongly recommend thoroughly reviewing both the other Leadership charts and the detail descriptions on these vendors.

In the Challenger section, we find OpenIAM and Fischer International slightly ahead, followed by two other vendors, Ilex and Tools4ever. Other vendors in the section are Systancia, a vendor which started in the Healthcare market; iSM Secu-Sys, a German vendor with an interesting product offering but limited market reach; Econet, Evolveum, and Propentus all as smaller vendors with specific focus areas. All of them can be interesting alternatives to the established players. We also find FSP in this segment, another German vendor, which shows its strength in the combination of Identity Provisioning and Access Governance, while having several gaps when looking at Identity Provisioning capabilities only.

Finally, we see one vendor in the Follower segment, which just recently entered the market and still shows gaps in the products' capabilities, plus having only initial customers. This is Login Alliance. They show potential in this market, but still have some way to go.

Overall Leaders are (in alphabetical order):

- Avatier
- Beta Systems
- CA Technologies
- Core Security
- EmpowerID
- Evidian
- ForgeRock
- Hitachi-ID Systems
- IBM
- Micro Focus
- Omada
- One Identity
- Oracle
- Pirean
- SailPoint
- SAP

2.2 Product Leadership

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

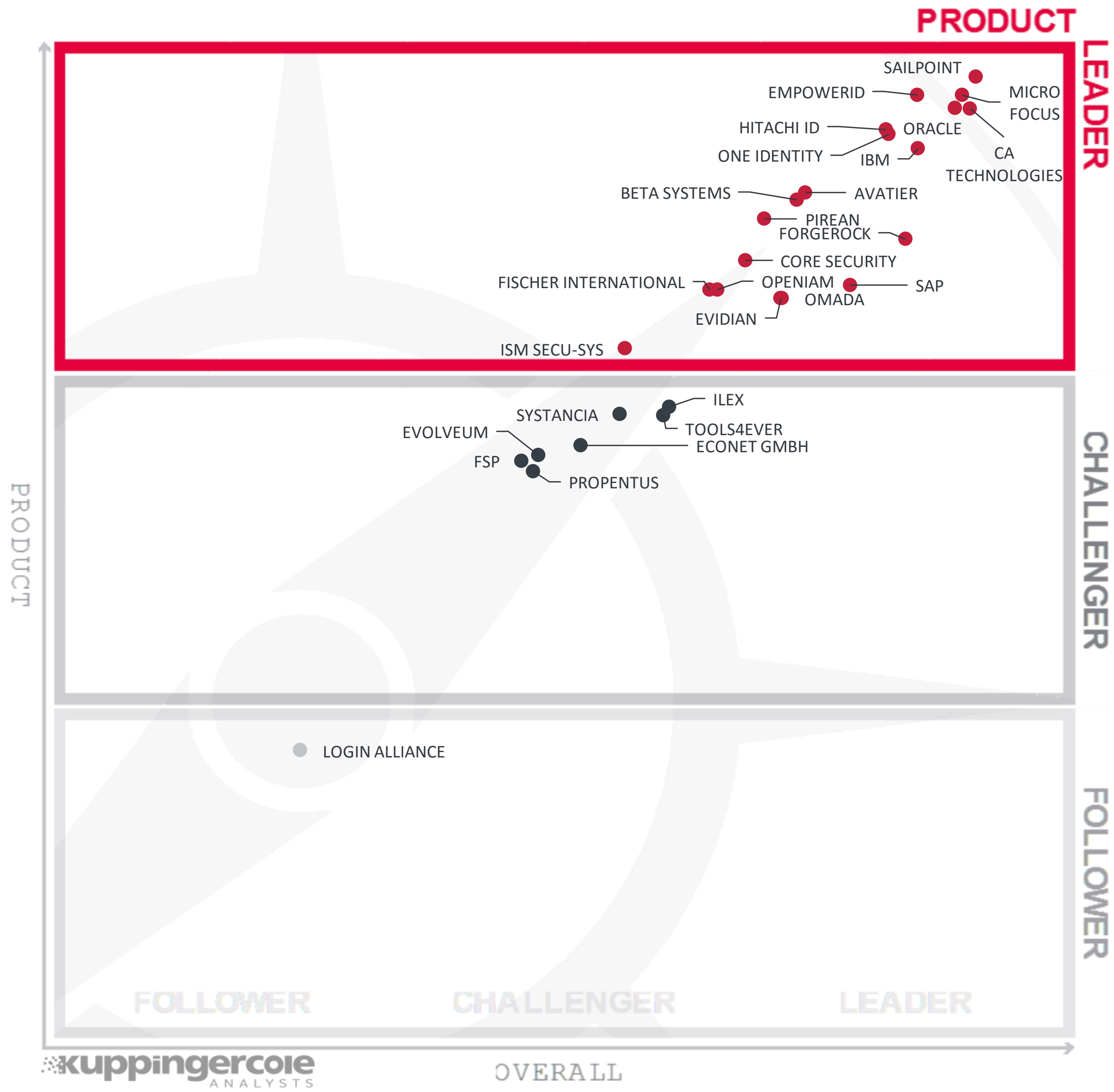


Figure 2: Product leaders in the Identity Provisioning market segment

Product Leadership, or in this case Service Leadership, is the view where we look specifically at the functional strength and completeness of products. As Identity Provisioning is an established and mature market segment, we find a significant numbers of vendors which qualify for the Leaders segment.

On top, we find a group of vendors, all placed close to each other. This group of eight vendors consists, in alphabetical order, of CA Technologies, EmpowerID, Hitachi ID, IBM, Micro Focus, One Identity, Oracle, and SailPoint. All these vendors deliver leading-edge products for on premises Identity Provisioning and score high in our rating.

Following these, we find Avatier, which have made significant progress over the past years with regards to the maturity and depth of functionality of their product. Beta Systems also is ranked close to the top vendors. Pirean follows slightly apart, an UK-based vendor that comes with a strong IAM and IGA offering with a lot of innovative capabilities. Close to them we find ForgeRock, which focus more on delivering an Identity platform than a traditional Identity Provisioning solution. Thus, they fall short in some areas such as out-of-the-box self-service interfaces, but are exceptionally strong with respect to customization, scalability, and other capabilities.

Also in the Leaders Segment, we find (in alphabetical order) Core Security, Evidian, Fischer International, iSM Secu-Sys, Omada, OpenIAM, and SAP, with iSM Secu-Sys just having passed the line between challengers and leaders.

Several of the other vendors are very close to becoming Leaders, being rated on top of the Challengers segment. These vendors include Ilex, Systancia, and Tools4ever. Most of these vendors have some form of specialization, such as Ilex with their focus on delivering a development environment for Identity Provisioning and IGA solutions, Systancia with their focus on the healthcare market, and Tools4ever as a vendor that started in the SMB market segment and evolved from there.

Following these vendors, we find Econet with their strong capabilities for IT Service Automation, Evolveum as an open source provider for Identity Provisioning, and Propentus, which have some specific capabilities such as a leading-edge HR and employee contract management integration. FSP is another vendor in that market segment. FSP, a German vendor, also shows several gaps, but will score stronger when looking at deep integration with RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control) capabilities in the KuppingerCole Leadership Compass on IGA.

All challengers are interesting vendors for certain use cases, while they lack certain features that would move them into the Leaders segment.

Finally, we have Login Alliance as a new player in the market, which still must show progress in their overall product capabilities. While they provide certain interesting capabilities, which make them an interesting option for selected use cases, they still lack overall breadth and depth of features.

Product Leaders (in alphabetical order):

- Avatier
- Beta Systems
- CA Technologies
- Core Security
- EmpowerID
- Evidian
- Fischer International
- ForgeRock
- Hitachi-ID Systems
- IBM
- iSM Secu-Sys
- Micro Focus
- Omada
- One Identity
- OpenIAM
- Oracle
- Pirean
- SailPoint
- SAP

2.3 Innovation Leadership

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

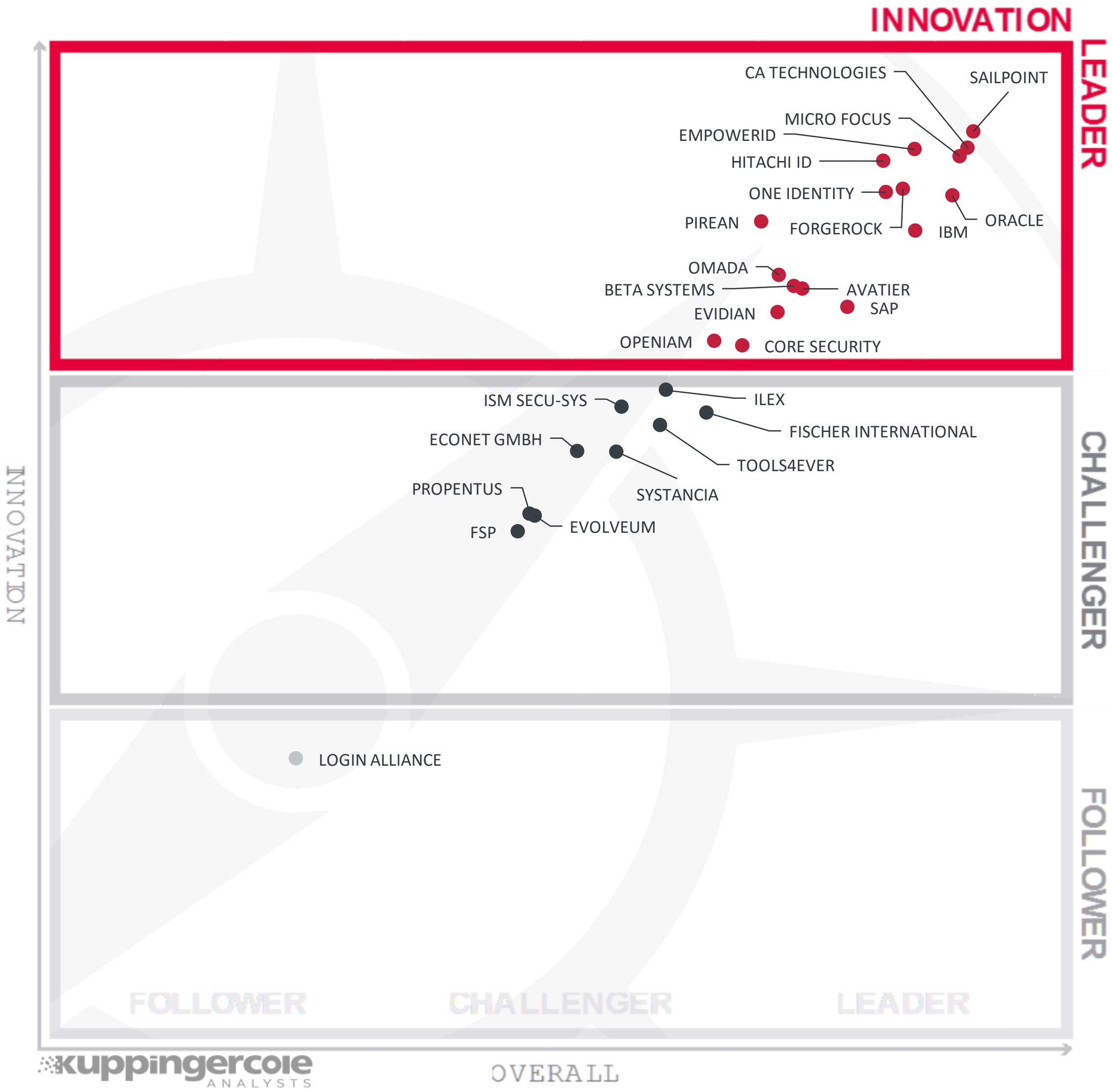


Figure 3: Innovation leaders in the Identity Provisioning market segment

Again, we rate many vendors as Innovation Leaders in the Identity Provisioning market. Given the maturity of Identity Provisioning, the amount of innovation we see is somewhat limited, but vendors still try differentiating themselves by innovation in various areas, from modern UIs and improved API layers to more specific details such as advanced rollback and simulation capabilities.

Again, we find a group of vendors being positioned close to each other in the upper right area of the chart. These include (in alphabetical order) CA Technologies, EmpowerID, ForgeRock, Hitachi ID, Micro Focus, One Identity, Oracle, and SailPoint. All of them count amongst the leading-edge vendors in the Identity Provisioning market, with all of them delivering some innovative capabilities.

Closely following them, we find Pirean and IBM, followed by Beta Systems, Omada, Avatier, SAP, Evidian, OpenIAM, and Core Security, which all also qualify for a rating as Innovation Leaders for Identity Provisioning.

As with most of the other Leadership charts for this Leadership Compass, we also find a couple of vendors close to becoming rated as Innovation Leaders, including Ilex and Tools4ever. While Ilex focuses on a development environment, Tools4ever comes from the SMB market for IAM, but now has significantly matured.

Following them is a group of vendors which are rated close to each other. These include, in alphabetical order, Econet, Fischer International, iSM Secu-Sys, and Systancia. Again, this is a very mixed group of vendors with different focus. We refer to the vendor pages further down in this report for details.

Propentus, Evolveum, and FSP are as well positioned in the Challengers segment. FSP delivers a good baseline offering, but currently more in the process of catching up with other vendors than driving innovation.

Finally, we again find Login Alliance in the Followers section, which are new in the market and also are primarily catching up with the leading players, while also demonstrating some innovative features that differentiate them from others. Again, we refer to the vendor pages in the report for details.

Innovation Leaders (in alphabetical order):

- Avatier
- Beta Systems
- CA Technologies
- Core Security
- EmpowerID
- Evidian
- ForgeRock
- Hitachi ID Systems
- IBM
- Micro Focus
- Omada
- One Identity
- OpenIAM
- Oracle
- Pirean
- SailPoint
- SAP

2.4 Market Leadership

Finally, we looked at Market Leadership, i.e. the number of customers, the partner ecosystem, the global reach, and related factors affecting the leadership in a market. Market Leadership, from our point of view, requires global reach.

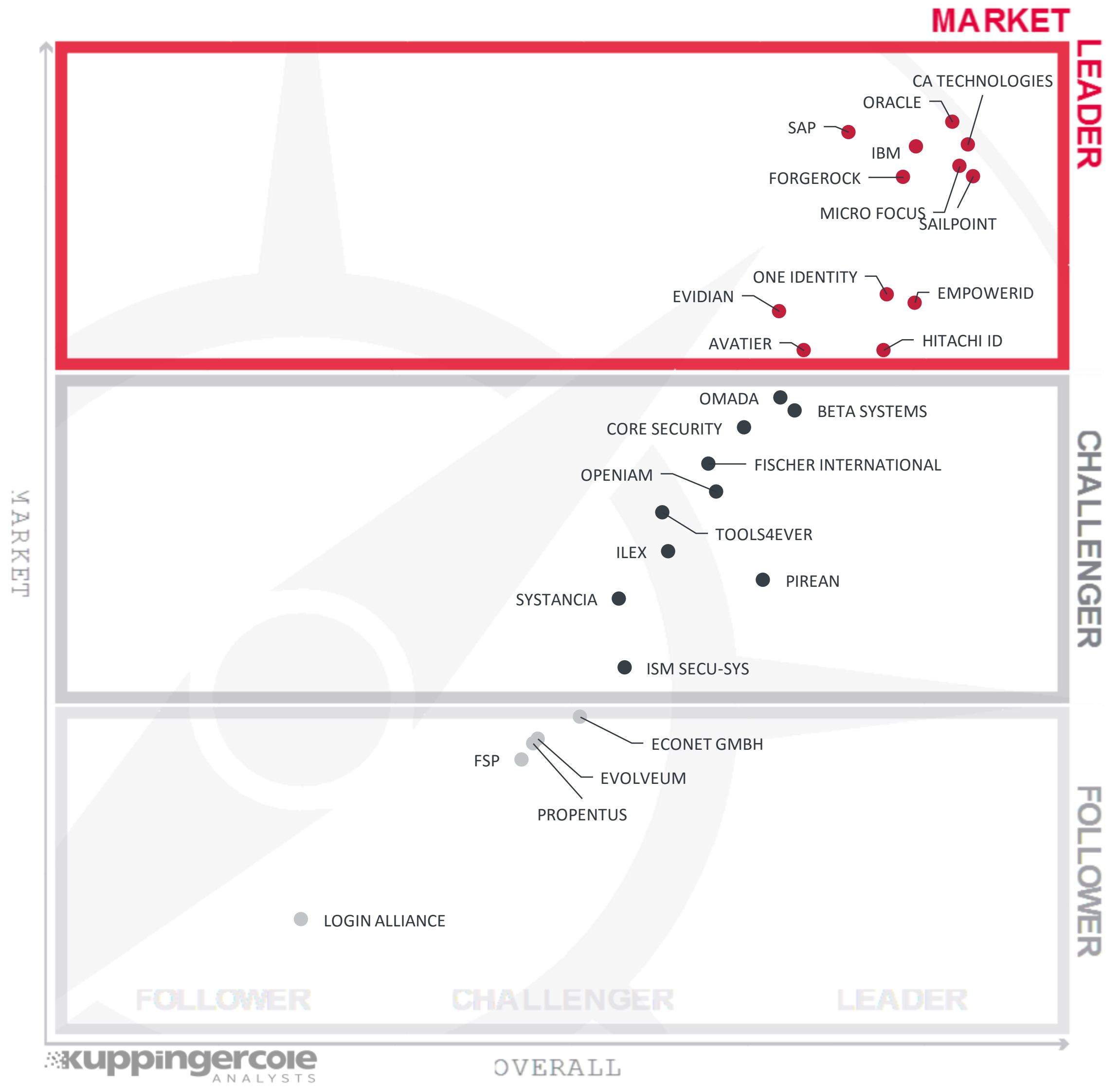


Figure 4: Market leaders in the Identity Provisioning market segment

In the Market Leaders rating, we get a somewhat different picture. While there is a group of leading, well-established vendors, others rate lower, given that they are either only regional vendors or have a low number of customers.

In the top right corner of the Leaders segment, we find a group consisting of seven vendors. This group, in alphabetical order, consists of CA Technologies, ForgeRock, IBM, Micro Focus, Oracle, SailPoint, and SAP.

We also rated EmpowerID, Evidian, and One Identity as Market Leaders. Furthermore, Avatier and Hitachi ID just made it into this segment, both showing some gaps particularly regarding their partner ecosystem at global scale.

In the Challenger section, we find Omada close to entering the Leader segment. While we count them amongst the Market Leaders in other areas of the overall IGA market, for Identity Provisioning they are not yet, given that they added their own Identity Provisioning capabilities in version 11.0 (current version is 12.x), while relying on Microsoft Identity Manager as integration tool before.

Following these vendors, we find many other vendors such as Beta Systems, Core Security, OpenIAM, Tools4ever, Fischer International, Ilex, Pirean, and Systancia, which all show gaps in some of the areas we expect seeing in Market Leadership, such as either the number of customers, the average size of their customers, their partner ecosystem, etc.

Also iSM Secu-Sys is rated as a challenger, but just passing the line. They are focused on the German-speaking countries and have a relatively low number of customers, combined with a very limited partner ecosystem.

Finally, we see six vendors in the Followers section, all of them being very small and commonly focused on certain geographies. Aside of the new entrant, Login Alliance, we find Econet, Evolveum, FSP, and Propentus here.

Market Leaders (in alphabetical order):

- Avatier
- CA Technologies
- EmpowerID
- Evidian
- ForgeRock
- Hitachi ID
- IBM
- Micro Focus
- One Identity
- Oracle
- SailPoint
- SAP

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

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

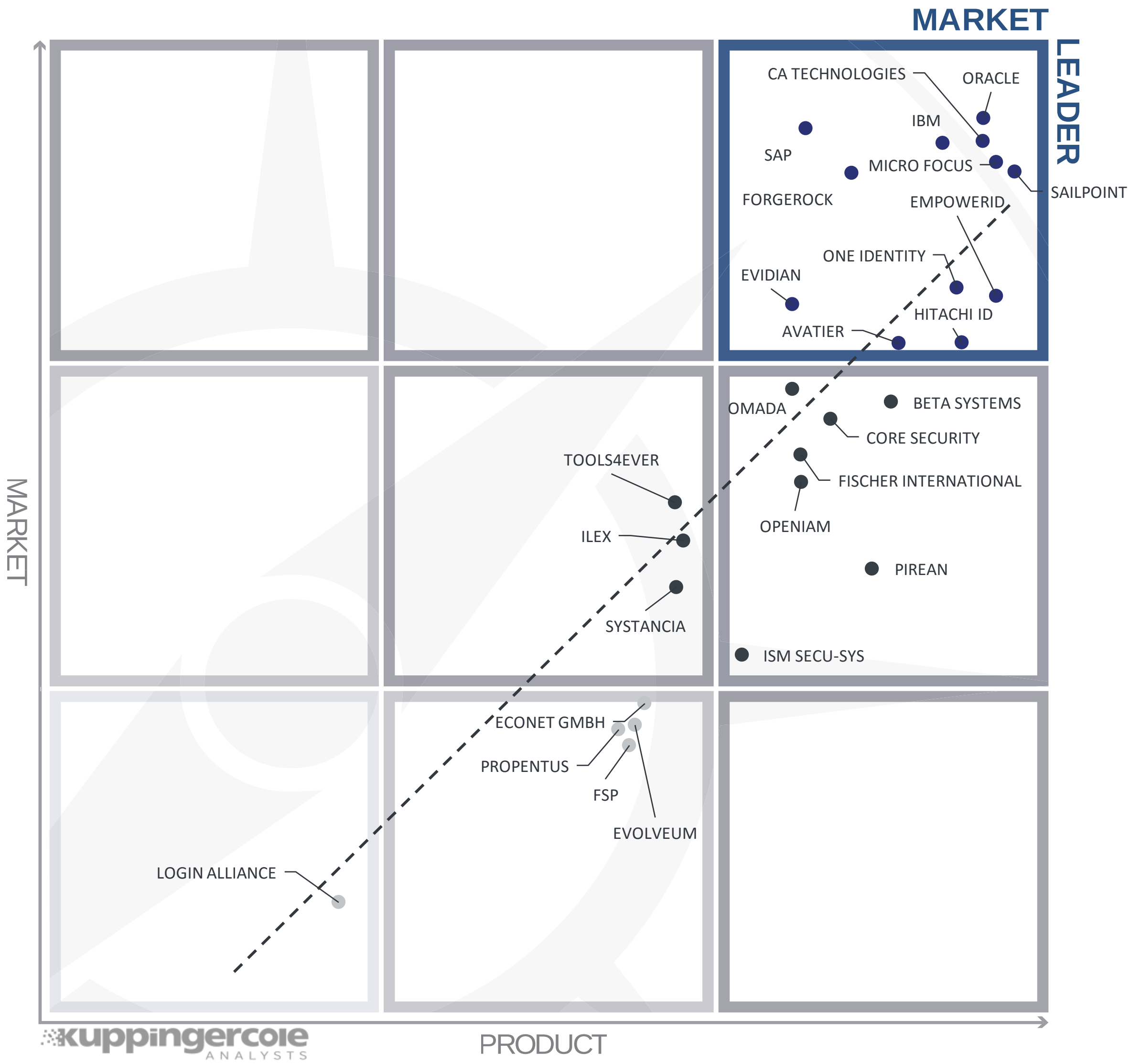


Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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.

In the upper right segment, we find the “Market Champions”. Given that the Identity Provisioning market is mature, we find several vendors in that area, with (in alphabetical order) CA Technologies, IBM, Micro Focus, SailPoint, and Oracle being top-right. SAP and ForgeRock also count amongst the Market Champions, however being stronger regarding their market success than in the (still strong) product functionality for Identity Provisioning. On the other hand, we find some vendors in the lower area of the Market Leaders box, which are (in alphabetical order) Avatier, Evidian, EmpowerID, Hitachi ID, and One Identity.

Below that box, in the middle-right box, we see the vendors that deliver strong product capabilities for Identity Provisioning but are not yet considered Market Leaders. All these vendors have a strong potential for improving their market position due to the product capabilities they deliver. These vendors are, from top to bottom, Omada, Beta Systems, Core Security, Fischer International, OpenIAM, Pirean, and iSM Secu-Sys.

In the middle of the chart, we see some vendors that all provide good but not leading-edge capabilities and are not Market Leaders. These include Tools4ever, Ilex, and Systancia.

Below them, we find smaller, specialized vendors, with Econet, Evolveum, FSP, and Propentus.

Finally, we find one vendor, Login Alliance, in the bottom-left box, being a new entrant to the market with very few customers and, despite some innovative features, the need for catching up in various feature areas.

3.2 The Product/Innovation Matrix

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

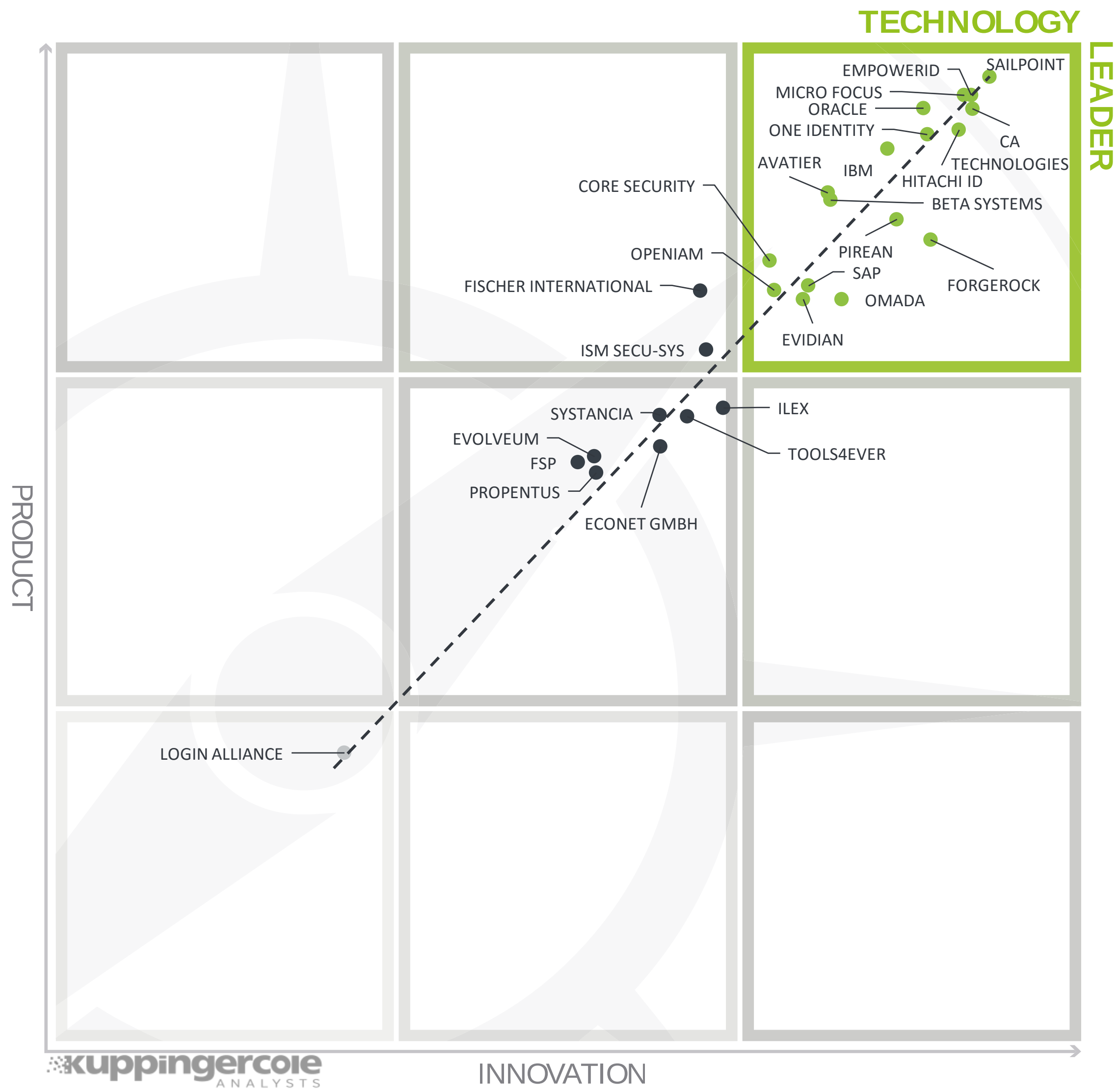


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line. When looking at the "Technology Leaders" segment, we find the leading vendors all in the upper right corner, placed close to each other. The top-notch vendors are SailPoint, Micro Focus, EmpowerID, Oracle, Hitachi ID, One Identity, CA Technologies, and IBM.

Closely following, and also in the "Technology Leaders" box, we see Avatier, Beta Systems, Pirean, and ForgeRock. Further vendors that made it into this group are Core Security, SAP, OpenIAM, Evidian, and Omada.

To the right of them, we find two other vendors that are rated amongst the Product Leaders, but not the Innovation Leaders. The vendors here are Fischer International and iSM Secu-Sys.

Most of the other vendors are positioned in the box in the middle of the chart, being challengers for both the product rating and the innovation rating. Here we find Ilex, Systancia, Tools4ever, Econet, Evolveum, Propentus, and FSP.

Again, the new entrant to the Identity Provisioning market, Login Alliance, is positioned in the lower left corner.

3.3 The Innovation/Market Matrix

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

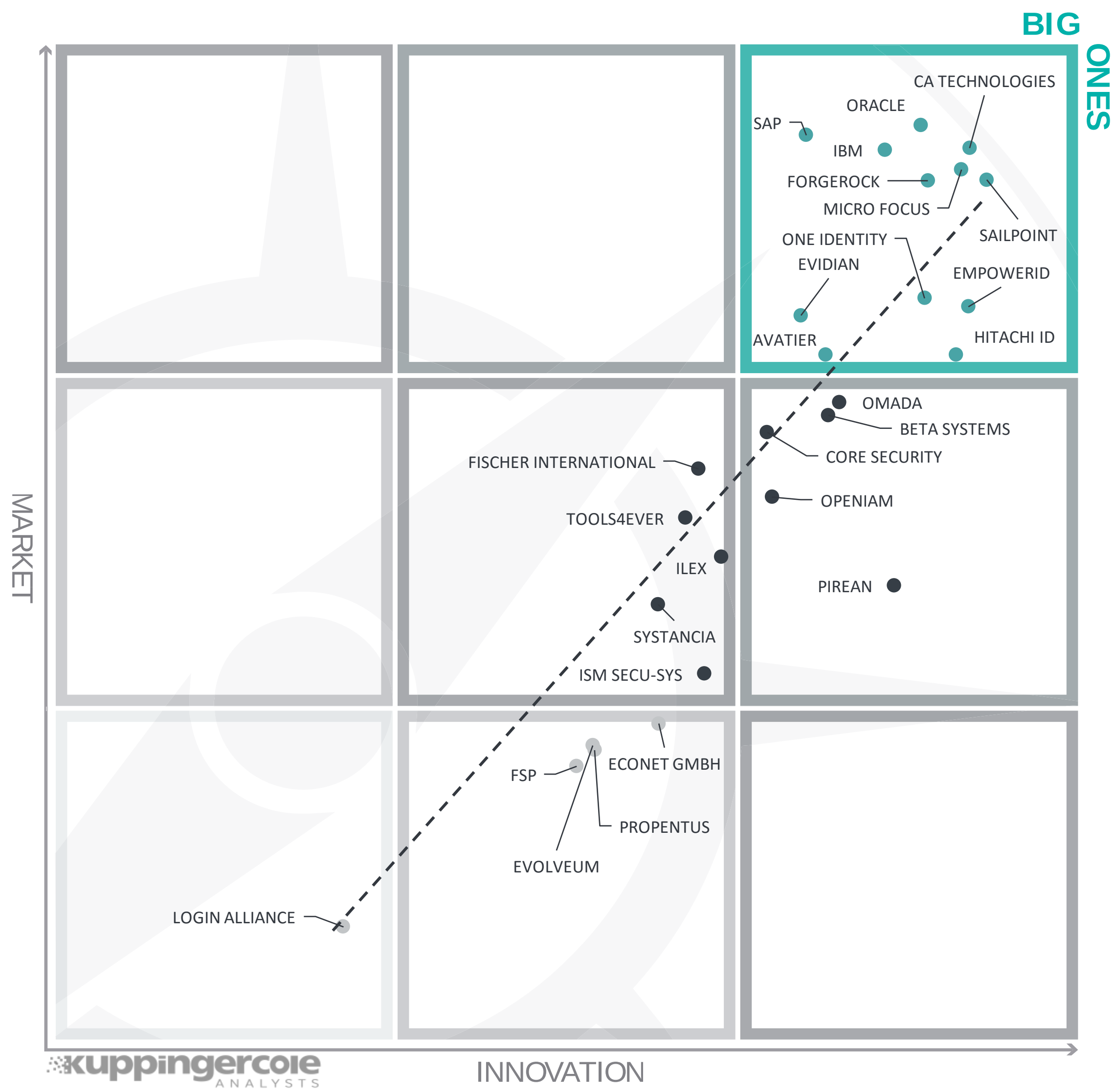


Figure 7: The Innovation/Market Matrix

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

In the upper right corner we find the “Big Ones” in Identity Provisioning, with a significant number of vendors being positioned at that level. We find the large ones more on top, including (in alphabetical order) CA Technologies, ForgeRock, IBM, Micro Focus, Oracle, SailPoint, and SAP.

More to the bottom of the upper right box, we see One Identity, EmpowerID, Evidian, Hitachi ID, and Avatier.

Below the “Big Ones”, in the middle-right box, we find some innovatie vendors that are not rated amongst the Market Leaders. Here we see Beta Systems, Core Security, Omada, OpenIAM, and Pirean.

The segment in the middle of the chart contains the vendors rated as challengers both for market and innovativeness, with Tools4ever, Fischer International, Ilex, Systancia, and iSM Secu-Sys.

Below them, we see a group of small vendors showing good but not leading-edge innovativeness. These are Econet, Evolveum, Propentus, and FSP.

Finally, we again find the new entrant to the market, Login Alliance, in the lower-left box.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on 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.

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
AVATIER	positive	positive	strong positive	positive	strong positive
BETA SYSTEMS	strong positive	strong positive	neutral	positive	strong positive
CA TECHNOLOGIES	strong positive	strong positive	positive	strong positive	strong positive
CORE SECURITY	positive	positive	positive	positive	positive
ECONET GMBH	positive	positive	neutral	neutral	positive
EMPOWERID	strong positive	strong positive	strong positive	positive	strong positive
EVIDIAN	strong positive	positive	neutral	positive	positive
EVOLVEUM	positive	positive	positive	neutral	positive
FISCHER INTERNATIONAL	positive	positive	strong positive	neutral	strong positive
FORGEROCK	strong positive	positive	strong positive	positive	positive
FSP	positive	positive	positive	neutral	positive
HITACHI ID	strong positive	strong positive	strong positive	strong positive	strong positive
IBM	strong positive	strong positive	positive	positive	strong positive
ILEX	positive	positive	neutral	neutral	positive
ISM SECU-SYS	strong positive	positive	strong positive	positive	positive
LOGIN ALLIANCE	positive	neutral	weak	neutral	neutral
MICRO FOCUS	strong positive	strong positive	positive	strong positive	strong positive
OMADA	positive	positive	strong positive	positive	strong positive
ONE IDENTITY	strong positive	strong positive	strong positive	positive	strong positive
OPENIAM	positive	positive	strong positive	neutral	positive
ORACLE	strong positive	strong positive	positive	strong positive	strong positive
PIREAN	strong positive	positive	positive	positive	strong positive
PROPENTUS	positive	neutral	positive	neutral	positive
SAILPOINT	strong positive	strong positive	strong positive	strong positive	strong positive
SAP	strong positive	positive	positive	positive	positive
SYSTANCIA	positive	positive	positive	neutral	positive
TOOLS4EVER	positive	neutral	positive	neutral	positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
AVATIER	positive	neutral	positive	positive
BETA SYSTEMS	positive	neutral	positive	neutral
CA TECHNOLOGIES	strong positive	strong positive	strong positive	positive
CORE SECURITY	positive	neutral	positive	neutral
ECONET GMBH	positive	weak	neutral	weak
EMPOWERID	strong positive	positive	positive	neutral
EVIDIAN	strong positive	positive	strong positive	positive
EVOLVEUM	positive	weak	weak	neutral
FISCHER INTERNATIONAL	strong positive	neutral	positive	neutral
FORGEROCK	strong positive	positive	positive	strong positive
FSP	neutral	weak	neutral	weak
HITACHI ID	strong positive	neutral	strong positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
ILEX	positive	weak	neutral	neutral
ISM SECU-SYS	positive	weak	neutral	weak
LOGIN ALLIANCE	neutral	critical	weak	weak
MICRO FOCUS	strong positive	positive	strong positive	strong positive
OMADA	strong positive	neutral	positive	neutral
ONE IDENTITY	strong positive	positive	positive	positive
OPENIAM	positive	neutral	neutral	positive
ORACLE	strong positive	strong positive	strong positive	strong positive
PIREAN	strong positive	weak	neutral	neutral
PROPENTUS	neutral	weak	neutral	weak
SAILPOINT	strong positive	positive	strong positive	strong positive
SAP	strong positive	strong positive	strong positive	positive
SYSTANCIA	positive	neutral	neutral	weak
TOOLS4EVER	positive	neutral	positive	neutral

Table 2: Comparative overview of the ratings for vendors

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

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

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

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

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

5 Product/service evaluation

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

5.1 Avatier

Avatier has evolved from a vendor that focused primarily on providing smart user interfaces, but sometimes lacked the underlying depth of capabilities, to a vendor delivering mature offerings in the IAM space, including Identity Provisioning. Within the Avatier Identity Management Suite, the component responsible for Identity Provisioning is identity Enforcer.

Strengths	Challenges
• Innovative, highly user-centric approach to Identity Provisioning • Fast implementation focusing on end user service requests • Overall strong feature set in both breadth and depth of features	• No full support for multi-tenancy requirements • Still limited but growing partner ecosystem • Still limited footprint outside of North America

Table 3: Avatier major strengths and challenges

While Avatier has made strong progress in both the breadth and depth of features they support, they still benefit from their roots in being innovative when it comes to the user interface for both end users and administrators. Their main emphasis is on simplifying and automating the fulfillment of user requests or, for manual fulfillment, providing interface for these fulfillments. ,

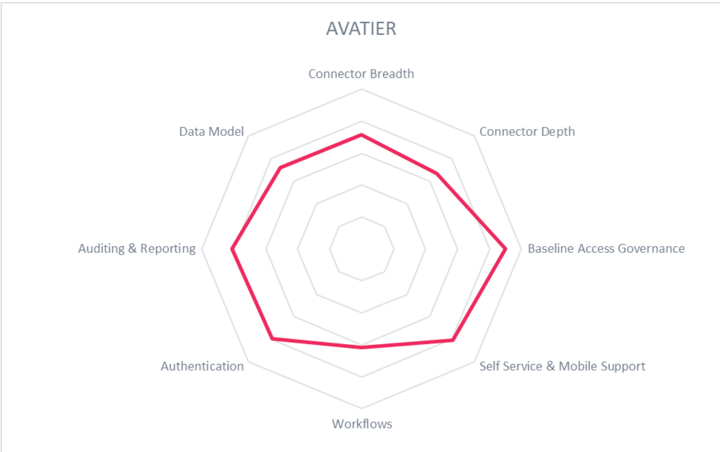
This makes the Avatier Identity Management Suite an interesting alternative to the established players, with strong functionality, leaving few gaps in what we'd love to see from an Identity Provisioning solution. Such gaps are commonly very specific, e.g. a lack of support for workflow standards and other features that are only required by few customers. A bigger challenge might be the lack of advanced rollback capabilities and the missing support for multi-tenancy requirements we see at some customers, particularly in highly-regulated industries and in multi-national corporations.

On the other hand, Avatier has made great progress when it comes to breadth of connectors and the support for a broad variety of systems, delivering a strong solution with an excellent user interface.

The biggest challenge for international customers remains the rather small partner network and the still limited presence outside of North America.

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

Table 4: Avatier rating



Overall, Avatier Identity and Access Risk Management Suite is an interesting choice for several customers, which is fully competitive to the established, leading players in the market. For customers outside of North America, we strongly recommend carefully evaluating the support Avatier can deliver for deployment and operations.

5.2 Beta Systems

Beta Systems, a German vendor, is amongst the vendors with the longest market presence in the Identity Provisioning market. Their offering has gone through some name changes and is branded Garancy Identity Manager today, being a part of the Garancy IAM Suite which adds additional capabilities such as Access Intelligence.

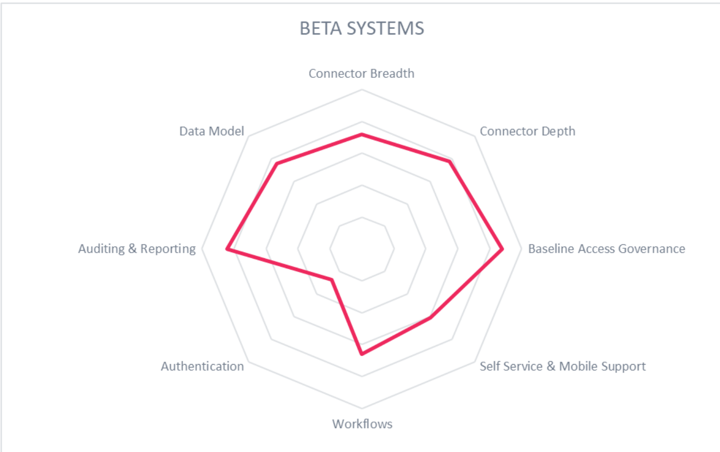
Strengths	Challenges
• Very mature solution with strong role management support • Connector approach with tight application integration, supporting also Dynamic Authorization Management • Strong support for mainframe environments	• Workflow as an OEM component, but tightly integrated • Still a relatively small but sufficient partner ecosystem.

Table 5: Beta Systems major strengths and challenges

Beta Systems Garancy Identity Manager counts amongst the very mature offerings for Identity Provisioning, with a broad set of connectors being available. One of the strengths is the depth of integration they provide with their connectors. Beta Systems is one of the rare 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. Furthermore, they deliver a flexible approach for customizing connectors for specific applications.

Another strength are their built-in role management capabilities, which allow for efficient, highly automated assignment of entitlements. The product also comes with a workflow component, which is based on an OEM component but well integrated into the overall Garancy IAM Suite.

Beta Systems is one of the very few vendors that offers a fixed-price implementation of its offering within defined environments and connecting to a defined set of target systems. That is proof for their ability to rapidly deploy the product and their long expertise in the market.



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

Table 6: Beta Systems rating

Overall, Beta Systems Garancy Identity Manager is a mature and feature-rich product. Beta Systems has a presence in major markets and a small, but overall sufficient partner ecosystem plus an own, strong professional services unit.

5.3 CA Technologies

CA Technologies is among the largest infrastructure software vendors worldwide and offers a broad portfolio of products in the IAM market segment, including CA Identity Management and Governance as its solution for Identity Provisioning (and Access Governance). 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	Challenges
• Mature product with a broad range of features and good integration of these • Efficient use through Xpress components • Tight integration with other CA products in the field of security • Large customer base • Modernized, leading-edge UI	• Requires CA SSO 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

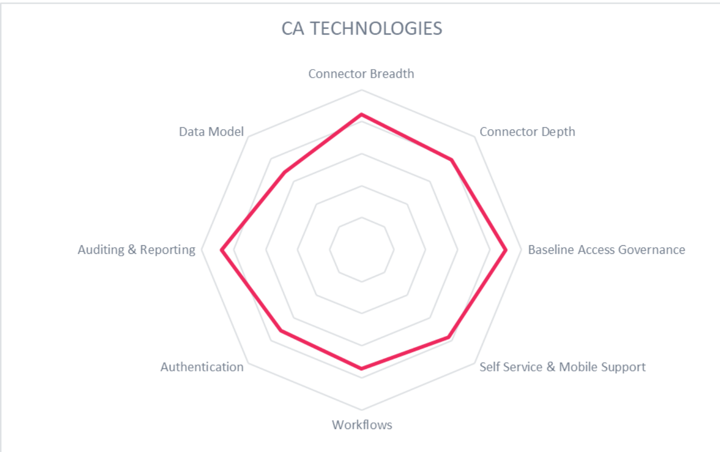
Table 7: CA major strengths and challenges

Based on the long history of the product and the market position of CA Technologies, it is no surprise that CA has done many deployments of CA Identity Management and Governance. Therefore, there are - besides a mature and rich feature set - several additional solutions from CA Services available which add to this functionality. A 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. Furthermore, the product now comes with a modern, well-thought-out user interface.

Like some other vendors, CA Technologies is following a concept which tries to avoid too many redundancies between the products in its portfolio. Thus, advanced authentication capabilities e.g. are delivered via CA SSO, formerly known as CA SiteMinder, which 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	strong positive

Table 8: CA rating



Overall, CA Identity Maagement and Governance 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.

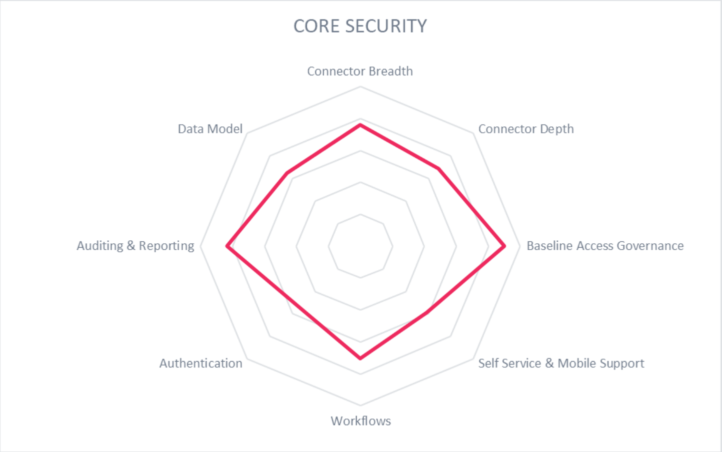
5.4 Core Security

Core Security is a vendor that is a result of various acquisitions, including the one of Courion. Courion, on the other hand, had evolved from supporting specific problems especially around password synchronization towards a company with a suite covering major areas of IAM today. The Core Security 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, Core Provisioning for Identity Provisioning and Core Password for self-service password management are the primary offerings within the scope of this Leadership Compass. Core Security 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	Challenges
• Broad, integrated feature set for provisioning and access governance • Mature provisioning capabilities and large number of connectors • Deliver best practice workflows out-of-the-box • Strong connectivity also with more complex platforms like mainframe environments and Connector API	• Still limited footprint in the market outside of North America • Limited support for external authentication

Table 9: Core Security major strengths and challenges

Core Security 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 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. They furthermore have added a Connector API for rapid connector development. Core Security also provides good integration with other elements of IT infrastructure like SIEM platforms etc. Furthermore, Core Security has updated the user interface, following modern UI paradigms now.



Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 10: Core Security rating

Overall, Core Security 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 plus the uncertainty that has been raised in the market for a certain period after the merger.

5.5 econet

econet is a German software company, which is delivering IAM solutions for many years. Their core product is named Identity & Service Manager and is focused on automation in IT Service Management, with Identity Provisioning being the core component of the product. In contrast to many other tools, econet Identity & Service Manager also provides features such as automated creation of mailboxes in eMail systems as a standard feature.

Strengths	Challenges
• Good baseline feature set and connectors for Identity Provisioning • Support for managing mailboxes and file shares • Standard processes for Identity Provisioning delivered out-of-the-box	• Small vendor, focused on Germany, Switzerland, and Austria • Very small partner ecosystem • Limited support for provisioning to cloud services

Table 11: econet major strengths and challenges

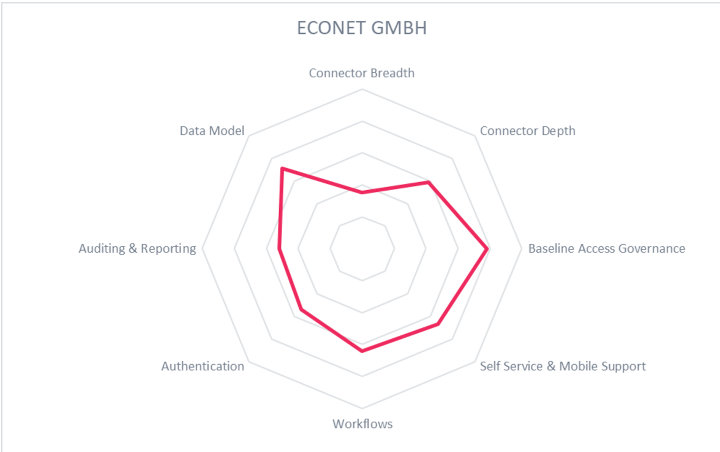
The focus of econet is on optimizing the core IAM processes such as creating users, job change processes, and leaver processes. The solution comes with pre-defined, standardized processes for a variety of typical requirements in organizations, thus reducing the implementation effort. As mentioned above, econet goes beyond typical Identity Provisioning tools in supporting features such as the creation of mailboxes, but also delivering Data Governance capabilities for managing file services or Microsoft SharePoint.

On the other hand, it goes well beyond the administrative tools targeted at mid-sized companies in both its overall in both its feature set and the connectors provided. Features e.g. include role based access control and a variety of user self-services. Connectors include such for PBX systems and SAP environments. Furthermore, it can integrate with Microsoft Identity Manager to extend its provisioning capabilities.

The core market of econet are the German-speaking countries. The company has only a small partner ecosystem, which is a limiting factor for their ability to execute in large-scale, global projects.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 12: econet rating



In sum, econet is an interesting alternative to other Identity Provisioning systems due to its broader scope, with support for managing mailboxes, file shares, and overall Data Governance. However, due to the small size of the company and its small partner network, it is primarily an option for mid-sized and family-owned businesses in their core markets.

5.6 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	Chellenges
• Unique, business process-based approach to Identity Provisioning • Functionality well beyond Identity Provisioning • Flexible customization based on the central workflow engine, supported by a large number of predefined processes • Strong Identity Provisioning feature set	• Runs on Microsoft platform only • Small partner ecosystem, but some large partners with global scale

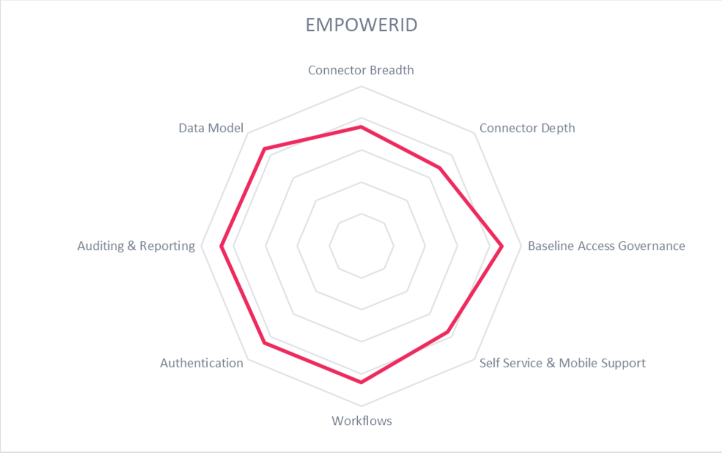
Table 13: EmpowerID major strengths and challenges

Customization of EmpowerID is very flexible, based on the architectural approach chosen by them. The product runs on the Microsoft infrastructure, which might turn out be a challenge for some companies. It 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 Privilege 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	strong positive
Interoperability	positive
Usability	strong positive

Table 14: EmpowerID rating



Overall, EmpowerID is a very interesting and innovative solution. This is even more true if one IAM solution covering a broad range of requirements with a well-thought-out architectural approach is requested. It is definitely worth having a look at the product. A challenge is the still small partner ecosystem, with few partners as of now. However, some of the partners can support customers at global scale. We anyway encourage EmpowerID to grow their partner ecosystem.

5.7 Evidian

The French vendor Evidian is part of Atos, one of the leading European IT service companies. Evidian has been in the IAM business for many years. Their product, Evidian IAM Suite, has been developed over a number of years and provides a good set of features in Identity Provisioning. It is a combination of components derived from the traditional Evidian product portfolio and other derived from the former Siemens DirX portfolio, which is now also owned by Atos. The solution goes beyond pure Identity Provisioning, allowing customers to implement an integrated approach to core IAM requirements.

Strengths	Challenges
• Established product with good feature set in core functionality • Suite provides strong SSO and Access Management capabilities • Integrated offering with a consistent concept for managing identities and access	• Conceptual approach might not be a perfect fit to some customer requirements • No ESB and SRM integration out-of-the-box, but integrated Request Management capabilities

Table 15: Evidian major strengths and challenges

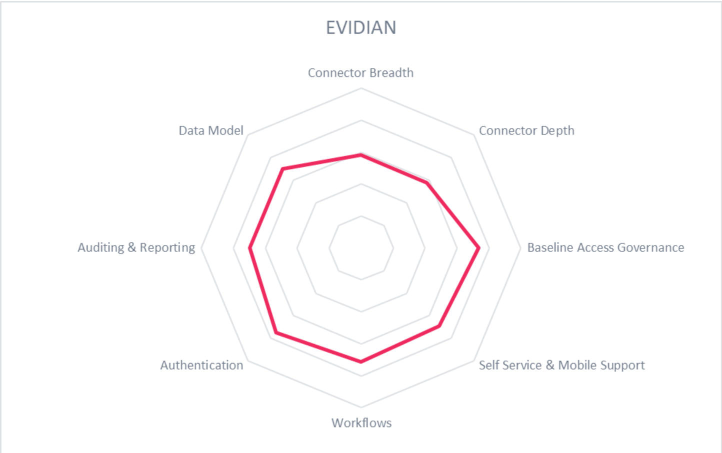
Evidian delivers a tightly integrated product which covers all major aspects of Identity Provisioning. It is focused on providing a consistent set of processes for users. Besides the core provisioning capability, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian.

There is a lack of advanced integration in few areas such as support for ESB (Enterprise Service Bus). On the other hand, der is an integration toolkit for ITSM tools available. Furthermore, 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	neutral
Interoperability	positive
Usability	positive

Table 16: Evidian 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 contender to them. The company is mainly focused on the European markets.

5.8 Evolveum

Evolveum is an Open Source IAM vendor based in Slovakia. Their midPoint product is provided for free, but with subscription for professional services available. The product has same roots as the ForgeRock OpenIDM product, but was forked away in development a while ago. While it has matured over the past years, midPoint still isn't leading-edge in all areas of Identity Provisioning, but delivers on its promising potential.

Strengths	Challenges
• Open Source solution, provided at no (license) cost • Innovative features on roadmap, but mostly focused on Access Governance • Broad support for connectors based on standard frameworks	• Several common features still missing, however various of them on the roadmap • Still small number of customers and limited partner ecosystem

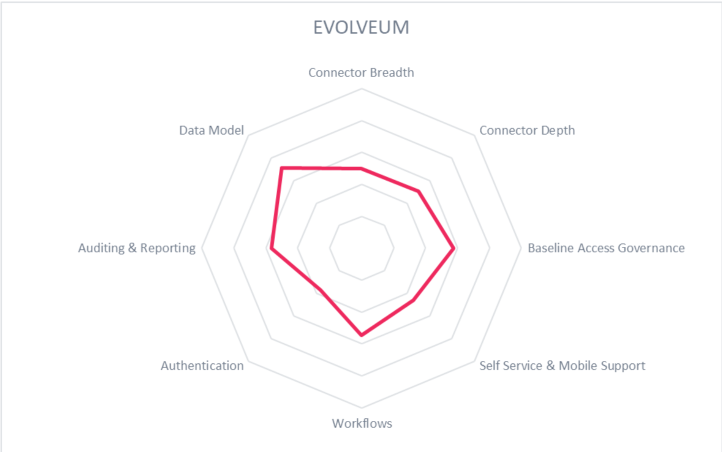
Table 17: Evolveum major strengths and challenges

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 users can choose from a role catalog. 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 and more flexibility in customization, particularly when it comes to workflows. While there are various workflows supported out-of-the-box, adapting these to the customer's need is still complex.

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.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 18: Evolveum rating



As of now, Evolveum midPoint is a still a rather young and in some areas still not feature-complete 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.

5.9 Fischer International Identity

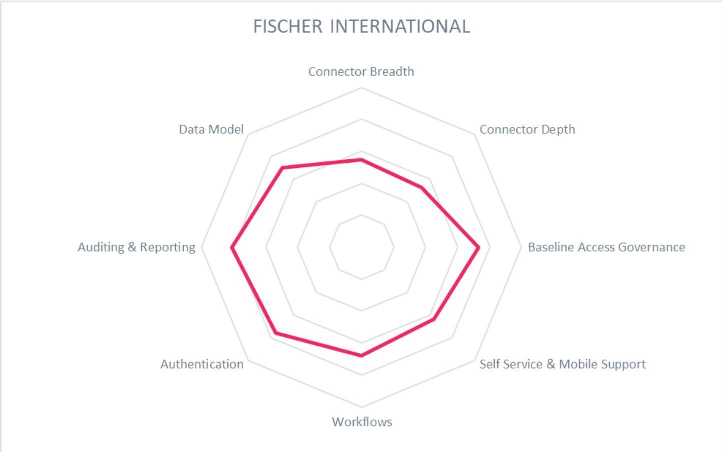
Fischer International Identity is a vendor which is different from all other provisioning vendors in that the company from the very beginning focused on SaaS delivery models for IAM as a main go-to-market strategy and core competency. The product is available for on-premise deployment as well, which 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	Challenges
• SaaS delivery model as standard option • No coding required, customization is done via configuration and graphical design components • Well-defined user interfaces for quick-start deployments	• No ESB support yet • No shopping cart paradigm supported • No approvals for configuration changes

Table 19: Fischer International major strengths and challenges

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 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	positive
Functionality	positive
Integration	strong positive
Interoperability	neutral
Usability	strong positive

Table 20: Fischer International 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.

5.10 ForgeRock

ForgeRock has established itself as a leading provider of IAM solutions, based on a common IAM platform. The company started its business as a provider of Open Source IAM solutions. The products today are still "commercial open source", i.e. they are fully maintained by ForgeRock and not a community project anymore. One of the products in their ForgeRock Identity Platform is Forgerock Identity Management, the commercial version of and successor to OpenIDM. This is the ForgeRock product which serves the Identity Provisioning market.

Strengths	Challenges
• Overall strong Identity Provisioning feature set • Well-thought-out architecture of IAM platform • Broad set of connectors based on OpenICF framework • Good interoperability based on a comprehensive set of REST APIs	• Access Governance features below baseline • No graphical configuration of workflows, but support of open workflow standards

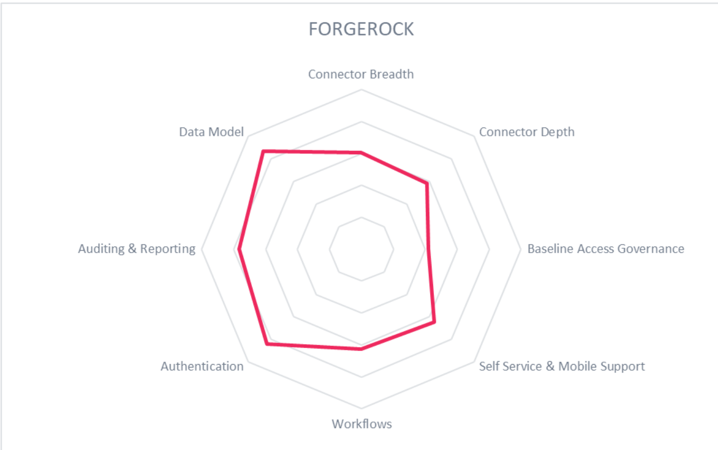
Table 21: ForgeRock major strengths and challenges

ForgeRock has made great progress in functionality over the past years. On one hand, they consequently moved towards a platform approach, with central components being reused across the entire IAM portfolio and with a great level of flexibility for customization to specific customer requirements. ForgeRock today is frequently used in organizations that need for highly flexible IAM solutions, which they integrate tightly with their IT infrastructure and business applications.

On the other hand, ForgeRock Identity Management matured from an entry-level IAM solution to an enterprise-class offering for Identity Provisioning, covering most of the requirements. It comes with a strong set of connectors, overall strong provisioning capabilities, and excellent scalability. Amongst the weaknesses, we find the lack of Access Governance capabilities even at the baseline level we expect from Identity Provisioning solutions. ForgeRock has made significant progress on their user interfaces over the past years. However, their strength is in the platform approach, which targets customers that customize and integrate the product into their environments. This is where ForgeRock Identity Manager excels, e.g. by its comprehensive APIs and the flexibility in customization.

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

Table 22: ForgeRock rating



ForgeRock has made a significant step forward in Identity Provisioning over the past years and is well-positioned in the market, with many large customers. We rate it amongst the leading offerings in the Identity Provisioning market, particularly for customers that are looking for large scale and need to customize and integrate Identity Provisioning with other solutions. These will most benefit from the platform approach.

5.11 FSP

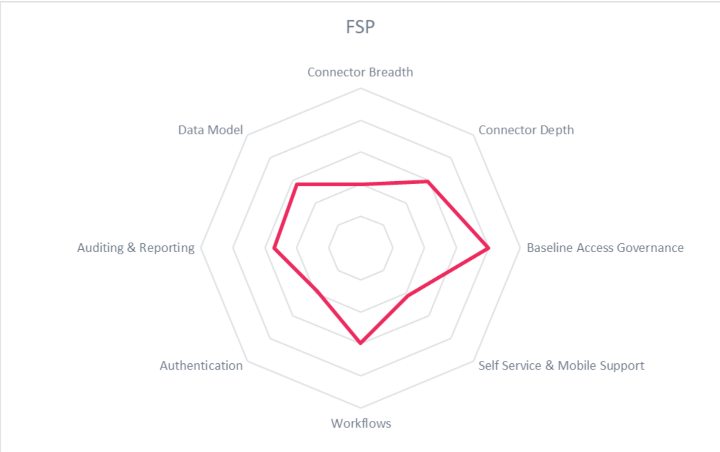
The German software vendor FSP provides an integrated IGA solution named "IGA Suite ORG". As an integrated suite, the product covers both Identity Provisioning and Access Governance, with its strengths being more in the Access Governance area and the integrated support for both role-based and attribute-based access control. However, the product also comes with baseline support for Identity Provisioning.

Strengths	Challenges
• Well-thought-out concept for Identity Provisioning and Access Governance • Flexible control of automated assignment of entitlements • Close interaction with vendor	• Lack of flexibility in customization • Limited set of out-of-the-box connectors, but flexible and straightforward customization of custom connectors • Small vendor with presence only in Germany, still small partner ecosystem

Table 23: FSP major strengths and challenges

While the breadth of out-of-the-box connectors is fairly low, the FSP offerings delivers a good depth in integration into the various target environments, based on a script connector that allows for rapid customization of connectors. For Identity Provisioning, customers benefit from the strong access control support, which allows for a high degree of automation of the assignment of entitlements. FSP IGA Suite ORG supports both role-based access control (RBAC) and attribute-based access control (ABAC) out-of-the-box. Based on that support, entitlement assignment can be managed at a very granular level within the provisioning workflows. Furthermore, flexible integration to external workflows is supported.

On the other hand, IGA Suite ORG is less flexible in customization than many other tools in the market. There are still some feature areas that can only be customized by the vendor's professional services. Furthermore, it lacks the breadth in user self-services we expect, as well as a high flexibility in its workflows.



Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 24: FSP rating

FSP IGA Suite ORG is an alternative for customers in the home region of the vendor, which are looking for close interaction with the software vendor and have a need for a granular management of entitlements with a high degree of automation, such as it is common for insurance companies and in other highly-regulated industries. FSP as a small vendor lacks from its very small partner ecosystem, which limits its ability to provide services to customers outside of the German-speaking countries. The company is actively working on expanding their partner ecosystem.

5.12 Hitachi ID

Hitachi ID provides a product named Identity Manager, which is a mature solution for managing identities and their access. It integrates Access Governance features, including SoD (Segregation of Duties) 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	Challenges
• Part of an integrated IAM Suite with strong functionality, beyond provisioning capabilities • Mature solution with broad connector support • Strong authentication and mobile support • Support for Active Directory Group Management	• Limited footprint outside of North America • Still relatively small partner ecosystem

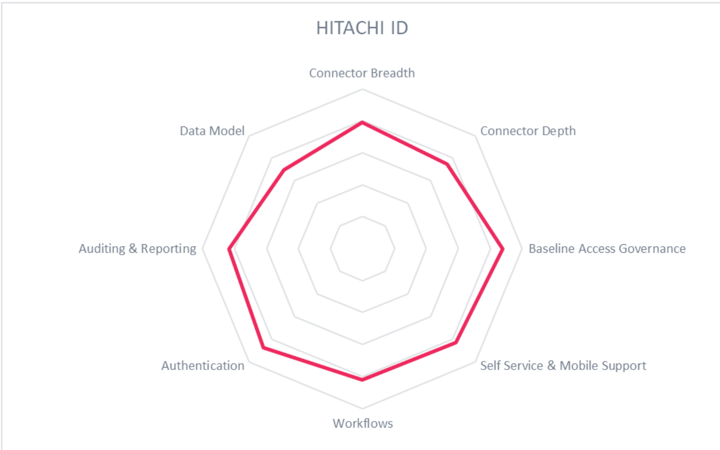
Table 25: Hitachi ID major strengths and challenges

In general, the product provides a mature set of features, delivering what customers typically need. It delivers a large set of connectors. The architecture provides high flexibility and scalability and is well-thought out. There are several unique features available, plus good interoperability. Hitachi-ID also has improved the user interface, adding a variety of new capabilities.

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	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 26: Hitachi ID rating



In sum, 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 that should be evaluated when looking for Identity Provisioning solutions. The vendor still has a somewhat limited footprint outside of North America.

5.13 IBM

IBM Security Identity Governance & Intelligence is the successor of former IBM Security/Tivoli Identity Manager (ISIM/ITIM) and one of the more mature products in the market. IBM has integrated the capabilities of ISIM into ISIGI and further enhanced these. IBM has a very large installed base, ranging amongst the top 5 vendors in the worldwide market in that aspect.

Strengths	Challenges
• Mature product with strong support for standard Identity Provisioning features • Strong support for different target systems • Significantly modernized by integrating into ISIGI • Significantly improved user interface	• Multi-tenancy requires significant additional configuration, but partners provide fully multi-tenant implementations

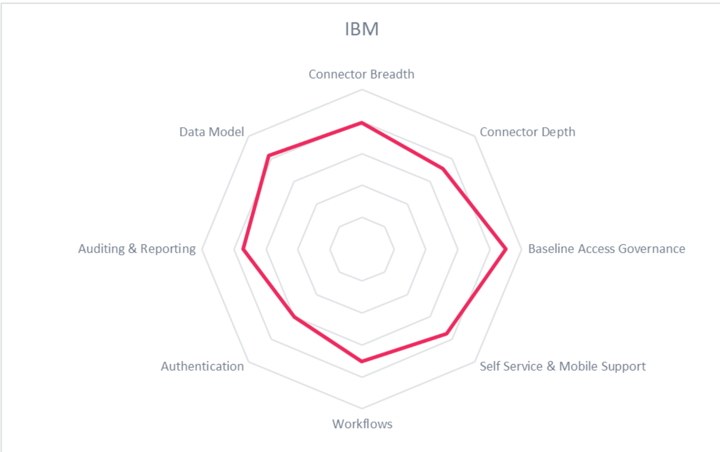
Table 27: IBM major strengths and challenges

IBM Security Identity Governance & Intelligence builds on 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. ISIGI also provides full Access Governance capabilities, 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 many 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	positive
Interoperability	positive
Usability	strong positive

Table 28: IBM rating



Overall, IBM Security Identity Governance & Intelligence is a mature offering that has undergone significant updates. It counts amongst the products that have seen the strongest evolution over the past 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.

5.14 ILEX

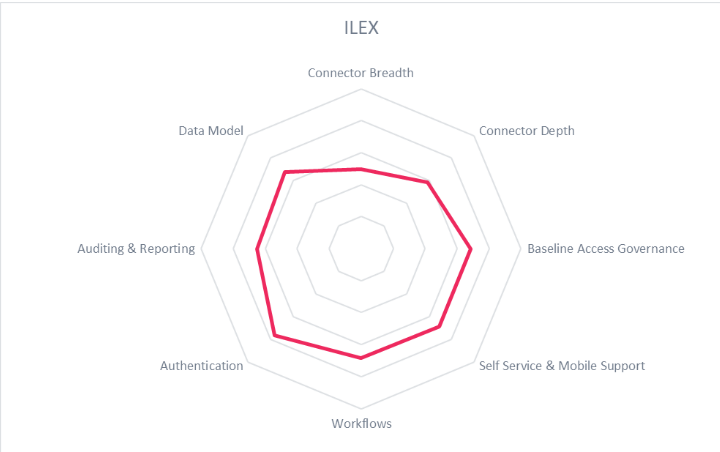
ILEX is a French vendor which provides two different but closely related tools around Identity and Access Management. Both are somewhat different from other provisioning approaches. The main offering is named Meibo, which allows customers to quickly create an Identity Management solution, while the other is named MPP (Meibo People Pack) and is focused primarily on SMBs. MPP, in fact, is a solution based on Meibo. Due to their specific focus, 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. The product in scope for this Leadership Compass is Meibo.

Strengths	Challenges
• Meibo as a flexible tool for creating custom Identity Management solutions. • Integration with SSO/Access Management solution • High flexibility and good overall feature set	• Meibo is a tool, not a solution, but allows for flexible customization of Identity Provisioning • Still limited visibility outside of French-speaking countries

Table 29: ILEX major strengths and challenges

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 also might be used complementary to existing Identity Provisioning products when it comes to building custom add-ons. One of its strengths is the tight integration with the Access Management and Single Sign-On solutions offered by ILEX. There is also a Role Management tool available which allows designing role management applications which can be natively plugged into other Meibo solutions.

The strength of Meibo is the central development component named Meibo Studio. From there, IAM solutions can be built rapidly, based on numerous pre-configured elements. It supports features such as multi-lingual UIs, white pages, integration to various identity sources, configuration of identity flows, role management and further features. All processes are graphically configured with in the development environment.



Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 30: ILEX rating

Overall, ILEX Meibo can be both the tool to build a custom Identity Provisioning solution and an add-on to existing Identity Provisioning solutions. 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.

5.15 iSM Secu-Sys

iSM Secu-Sys is a German vendor which offers an Identity Provisioning solution named bi-cube 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 must be a good fit.

Strengths	Challenges
• Broad set of functionality provided • Well-thought-out role model and delivery of standard processes • Available as SaaS deployment	• Conceptual approach needs to be well understood • Still very small partner ecosystem • No footprint in the market outside of Germany and Austria

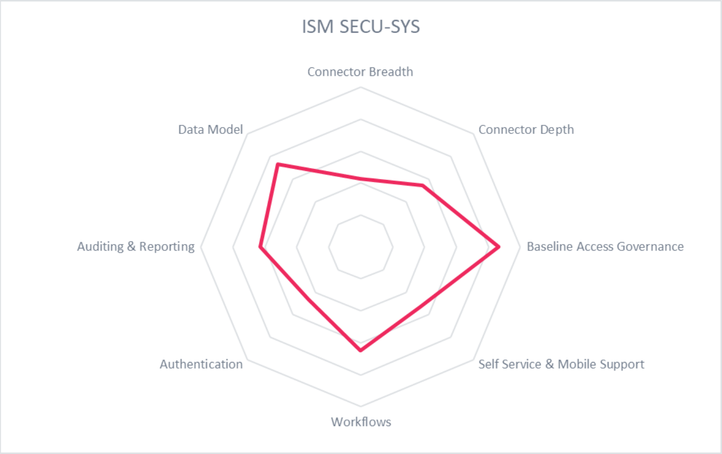
Table 31: iSM Secu-Sys major strengths and challenges

A positive aspect of the product clearly is that it delivers a broad set of functionalities based on a well-thought-out conceptual approach and methodology. Specific strengths are the role model and, as mentioned above, the standard processes provided. While the Identity Provisioning capabilities are good, customers of iSM Secu-Sys commonly look for an integrated IGA offering, given that the role management capabilities and related features are what distinguishes the offering from several of the other vendors in the market.

The biggest challenge of the vendor is their still rather limited market presence. There is a lack of integration partners and of visibility outside of the local markets.

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

Table 32: iSM Secu-Sys 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 must understand the conceptual approach taken by iSM which provides strong flexibility but is rather specific.

5.16 Login Alliance

Login Alliance is a German software vendor that just recently entered the IAM market. The companies behind the product, Syntlogo and Intension, originally started as consultants and system integrators, before they moved into the standard software business. Their offering for the Identity Provisioning market is named Login Master. It comes in various editions and targets both employee IAM and Consumer IAM (CIAM).

Strengths	Challenges
• Above-average of level of out-of-the-box processes • Integrated workflow, role management and rule-based entitlement assignement • Long-standing experience of vendor in integration projects	• Product is based on own and open source modules • Mandatorily requires involvement of vendor's professional services for deployment • Various gaps in functionality

Table 33: Login Alliance major strengths and challenges

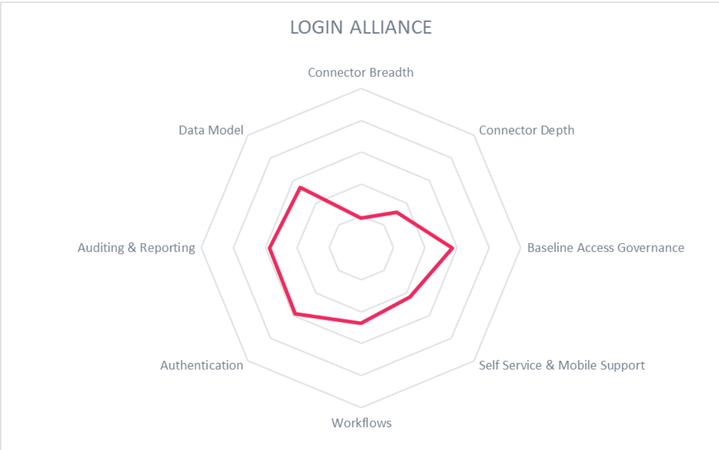
The product is based on several technical components, which come from different sources, including open source components. Login Alliance combines them to a framework that delivers baseline Identity Provisioning and some Access Governance capabilities. However, in the current format, the implementation of the solution mandatorily requires professional services for customizing it to the specific requirements of the customer.

As common in the field of Identity Provisioning, the focus is on automating processes around the employee lifecycle. The solution is above average when it comes to standard processes. In that area, it benefits from the integrator background of the vendor. They also show strength when it comes to managing complex access controls for external partners.

Currently, Login Alliance addresses primarily the German-speaking countries. There is a lack of a larger partner ecosystem of both technology and implementation partners. For growing such ecosystem, the vendor will have to move towards a more standardized implementation and a well-defined set of APIs for customization.

Security	positive
Functionality	neutral
Integration	weak
Interoperability	neutral
Usability	neutral

Table 34: Login Alliance rating



While Login Alliance has some interesting capabilities such as their features for Compliance Management by analyzing the current state of entitlements, the solution overall lacks both breadth and depth of features. That is not surprising, given that it is an initial release. Together with the professional services, it also might be rated as a good fit for certain customers with focus on B2B business in the DACH region. However, to become fully competitive in the Identity Provisioning and IGA market, the vendor will have to define a well-thought-out roadmap and need to execute on it.

5.17 Micro Focus

Micro Focus Identity Manager is the former NetIQ and Novell Identity Manager which became part of Micro Focus after the acquisition of NetIQ, which again had acquired Novell via 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. Micro Focus 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	Challenges
• Very large customer base and ecosystem • Strong, mature functionality covering all major aspects of Identity Provisioning • Strong support for a variety of target systems	• Rich functionality sometimes complex to understand

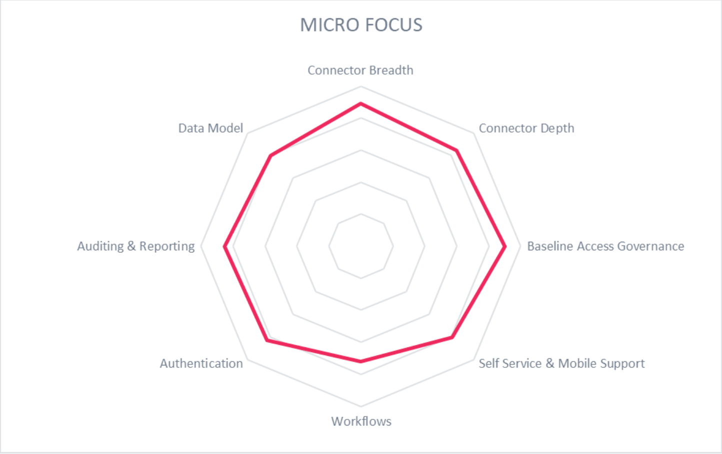
Table 35: Micro Focus major strengths and challenges

Micro Focus 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.

The product covers virtually all features we love to see in a pure-play Identity Provisioning solution. While the concept of their "drivers", as they call the connectors, is somewhat different from other vendors, it is straightforward. Furthermore, Micro Focus has a very long experience in building and maintaining drivers, delivering both breadth and depth of integration into target systems.

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

Table 36: Micro Focus rating



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

5.18 Omada

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. Over the past years, Omada has decided for a major strategic shift by adding its own Identity Provisioning layer, instead of solely relying on the integration with Microsoft Identity Manager (MIM). Thus, Omada nowadays also competes in the pure-play Identity Provisioning market, but shows its full strength in IGA and Access Governance use cases.

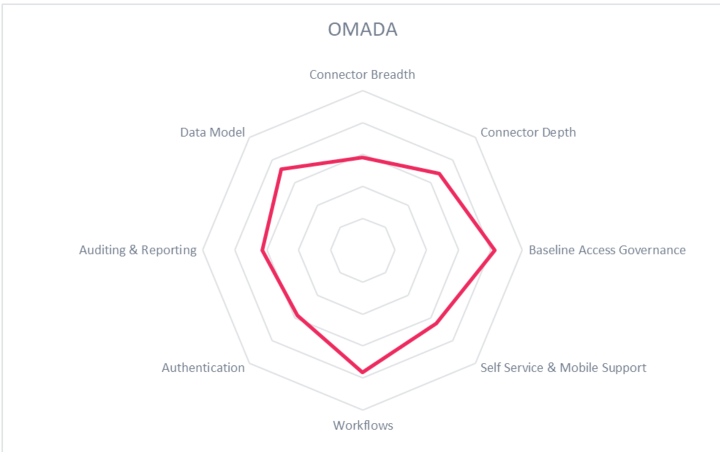
Strengths	Challenges
• Mature solution with strong workflow and role management capability • Efficient approach for onboarding new applications • Good SAP connectivity features • Can enhance Microsoft Identity Manager	• Good but not leading-edge support of out-of-the-box connectors • No out-of-the-box integration with Service Request Management (SRM) systems, but experience from custom integrations

Table 37: Omada major strengths and challenges

Omada Identity Suite has undergone major changes over the past years. Aside of adding its own Identity Provisioning layer and removing the former dependency on Microsoft Identity Manager, Omada also has re-architected the solution, changing the data model and massively enhancing scalability. Also, the UIs have undergone major modernization.

Looking at the Identity Provisioning capabilities, Omada now comes with a good set of connectors including strong connectivity to SAP and Microsoft environments, but not yet a leading-edge breadth in that area. On the other hand, customer connectors can be created rapidly based on support for various common interfaces and standards. A strength of Omada is their well-thought-out approach for rapid onboarding of applications, which is supported by pre-defined processes.

Omada shows its full strength in environments that look for both Identity Provisioning and Access Governance capabilities. It also remains an interesting option for extending Microsoft Identity Manager deployments.



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

Table 38: Omada rating

Overall, Omada Identity Suite is a very interesting solution for enterprise customers, beyond extending Microsoft Identity Manager and the Access Governance capabilities. It has become a strong contender for the Identity Provisioning market segment, based on the additions Omada has added in recent years.

5.19 One Identity

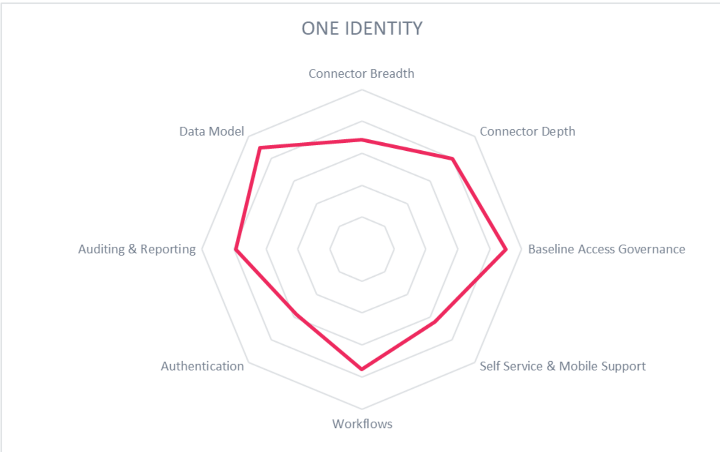
One Identity is a newly founded company, which is part of Quest Software. It owns the IAM portfolio that came from Dell Software. The main product is One Identity Manager, which historically came into the Quest portfolio through the acquisition of the German vendor Völcker Informatik. The product is a central pillar in the One Identity product portfolio. One Identity Manager builds on a sophisticated, consistent concept which allows for rapid customization and manages all dependencies between different objects in a very advanced way. The standard user interfaces of the product are very well constructed. Furthermore, the architecture has been changed over the past years to become more modular and scalable.

Strengths	Challenges
• Innovative, user-friendly interfaces • Well-thought out, sophisticated architecture and concepts • Very good connector support and excellent depth of integration to target systems such as SAP	• Process-driven approach requires some training, but is highly efficient •

Table 39: One Identity major strengths and challenges

The product is designed with some rather uncommon but helpful 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 remain fairly unique. Customization is straightforward, mainly done through configuration or based on creating rules. The concept needs to be well understood given that it is different from typical approaches to Identity Provisioning. However, it is backed by many out-of-the—box processes that just need to be configured via parameters. The flexibility regarding customization and the product architecture have been greatly improved over the past few years.

In addition, One Identity has enhanced the functional capabilities of the product consequently. The number of connectors has grown, even while it is still lower than what some other vendors offer, and there is broad support for Data 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 40: One Identity 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.

5.20 OpenIAM

OpenIAM counts among the less known vendors in the IAM market, taking a different approach than others. They started with an IAM offering deployed in an appliance form factor, which also can be run from the cloud, providing an IDaaS B2E offering. The solution consists of two distinct parts, the OpenIAM Identity Manager delivering Identity Provisioning and auditing features, and the OpenIAM Access Manager, which focuses on Identity Federation, Web Access Management, but also SOA Security.

Strengths	Challenges
• Good Identity Provisioning feature set • Flexible deployment options, including SaaS deployment • Well thought-out, modern architecture • Based on open source	• Good but not leading-edge support for Identity Provisioning features, but strong overall IAM feature set • Relatively small vendor with limited global scale, but growing partner ecosystem

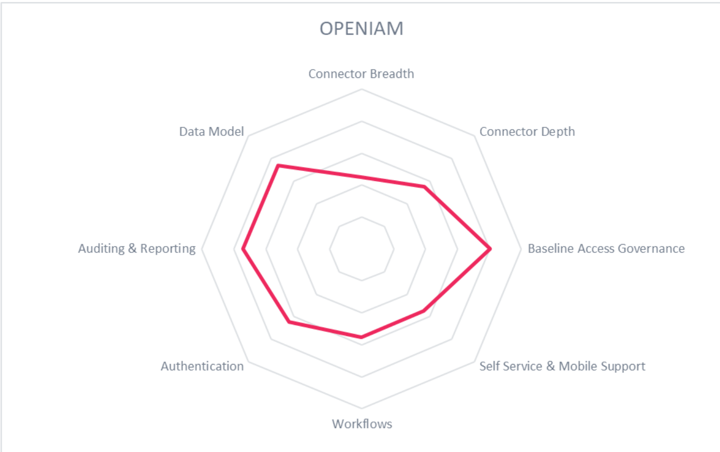
Table 41: OpenIAM major strengths and challenges

When looking at the breadth of feature areas covered, OpenIAM supports a very broad range. Beyond standard capabilities such as Identity Provisioning, delegated administration, and baseline Access Governance capabilities, there is, for example, support for XACML and thus Dynamic Authorization Management or SOA, and API security features.

The service-oriented architecture, based on micro services, makes OpenIAM a flexible offering with a high degree of scalability. It leverages various open source components, which are tightly integrated. The user interfaces are fair, but not leading-edge. However, they deliver support for different devices, from traditional desktops to mobile systems. The same holds true for the self-service interfaces provided out of the box.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 42: OpenIAM rating



In sum, OpenIAM is an interesting alternative for Identity Provisioning deployments when customers are looking for a broad set of capabilities they can run on premises or in the cloud and which they want to adapt to specific requirements. However, there biggest opportunity is in scenarios where customers are looking for comprehensive IAM suites.

5.21 Oracle

Oracle Identity Governance Suite is the on premise offering within Oracle's IAM portfolio. It includes Oracle Identity Manager (OIM), which delivers the Identity Provisioning capabilities. It provides mature capabilities in that area which have again been significantly improved with the 11g R2 release, particularly when it comes to integration and deployment of the various modules. A consequence of the integration 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	Challenges
• Mature, feature-rich product focused on Identity Provisioning • Significant improvements for deployment and customization • Very broad support for different environments and enterprise-level architectures	• Depending on use cases, there exist some dependencies between various components of the Oracle IAM portfolio; however, for Identity Provisioning only when adaptive authentication is required

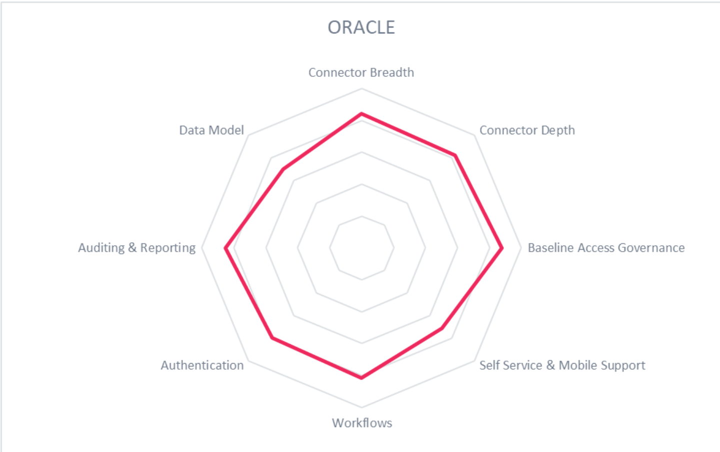
Table 43: Oracle major strengths and challenges

Oracle delivers mature Identity Provisioning capabilities, including a leading-edge set of connectors to a broad variety of on premises systems and business applications as well as to SaaS services. The connectors provide both breadth and depth of support.

Furthermore, in the recent releases we have seen several important changes, including 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	positive
Interoperability	strong positive
Usability	strong positive

Table 44: Oracle 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.

5.22 Pirean

Pirean is a UK-based software company that is not yet well-known outside of their home market, but shows strong potential. Their Access:One offering combines a variety of capabilities, from Identity Provisioning for the workforce to strong user self-service capabilities, support for CIAM (Consumer IAM) use cases, and authentication and SSO support.

Strengths	Challenges
• Well-architected and well-integrated IAM suite • Strong support for use cases beyond the employees • Strong self-service interfaces • Modern UI	• Still relatively small vendor, limited visibility outside of UK, but expanding to APAC and Central Europe • Still small partner ecosystem on global scale • Good but not leading-edge connector framework

Table 45: Pirean major strengths and challenges

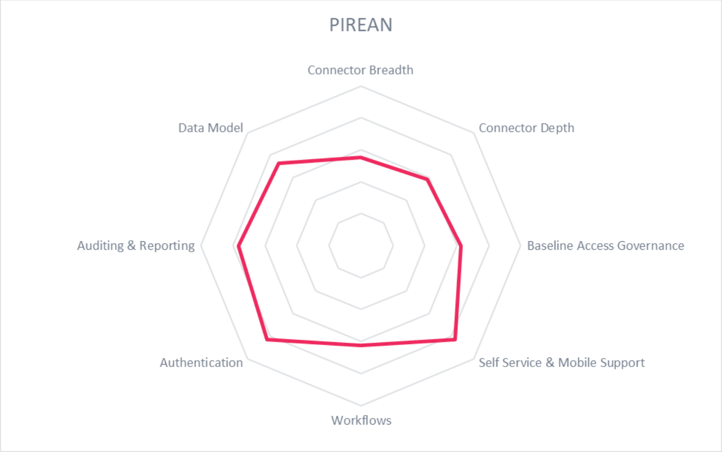
While most Identity Provisioning tools still are primarily focused on employees and contractors, the focus of Pirean Access:One is providing a unified platform across all types of identities, from the employee to the consumer and, in B2G (Business to Government) use cases the citizen. That sets them apart from most other offerings in the market.

From a feature perspective, Pirean Access:One is feature rich, also with respect to the core Identity Provisioning capabilities. It comes with a modern UI including mobile apps, a broad range of self-service interfaces, flexible workflows, and above-baseline support for Access Governance requirements. It also delivers excellent support for administrator and end-user authentication.

The set of connectors is fair, covering the common systems including several SaaS applications, but not leading-edge. Thus, support for the requirements in customer environments must be carefully evaluated to understand challenges and investments of connecting additional systems.

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

Table 46: Pirean rating



With its broad approach, beyond employee lifecycle management, Pirean is an interesting alternative to many of the established players in the Identity Provisioning and overall IAM market.-Their biggest challenge is their lack of visibility outside of the UK and their still limited partner ecosystem. Pirean is investing in growth in both APAC and EMEA. However, due to their specific strengths, we recommend considering Pirean in evaluations.

5.23 Propentus

Propentus, a Finnish software vendor, is one of the IAM vendors entering the market with a comprehensive suite that covers a variety of aspects around IAM, from Identity Provisioning to Privilege Management and Access Management. In some areas, they have opted for concepts that differ significantly from other vendors but might be highly valuable to certain customers.

Strengths	Challenges
• Identity Provisioning delivered as part of comprehensive IAM suite • Innovative approaches to entitlement management, which can be integrated with contract management • Strong business and HR focus of overall solution	• Only baseline authentication support • No support for graphical workflow configuration • Baseline connector support including SAP, but not leading-edge • Small vendor with limited partner ecosystem

Table 47: Propentus major strengths and challenges

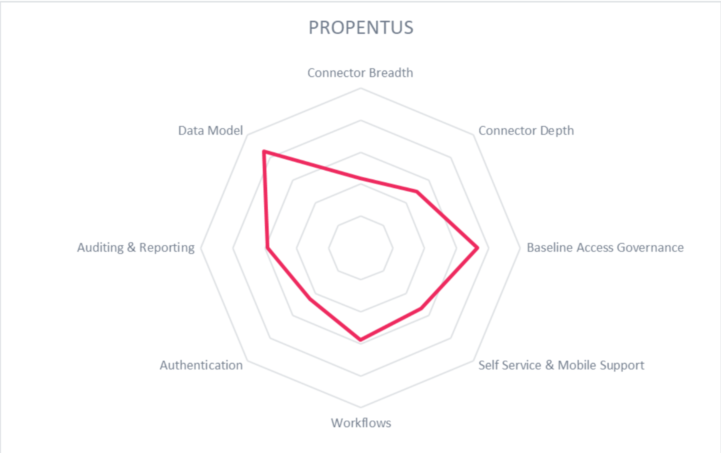
The best example in the context of Identity Provisioning for these specific approaches is their solution for Job Agreement Management, which combines the common Entitlement Management approaches with the management of employee contracts. Based on the information from these contracts, automation of entitlement and overall access management is controlled. That ensures that access is consistent to the job descriptions of the users. However, while that is valuable for some customers, it might interfere with organizational and IT constraints in other organizations. Also, integration to HR systems and Master Data Management (MDM) for identity data count amongst the strength of the solution.

On the other hand, we observe weaknesses in some of the major feature areas we look at when rating Identity Provisioning. This includes the breadth and depth of connectors, where Propentus delivers baseline support for the most common systems and applications including SAP, but lacks e.g. support for many of the established enterprise business services. The workflow capabilities also can only be considered being baseline, with a lack of flexibility when it comes to complex approval schemes and not supporting graphical configuration of workflows yet.

However, the specific, business-focused approaches of Propentus United Identity might anyway make the solution a good fit for certain customers.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 48: Propentus rating



Propentus is yet a very small vendor with a limited number of customers and lacking a global partner ecosystem. They are primarily focused on the Nordics, with expansion plans within Europe. We recommend looking at Propentus United Identity when features such as tight integration into HR and employee contract management are amongst the requirements.

5.24 SailPoint

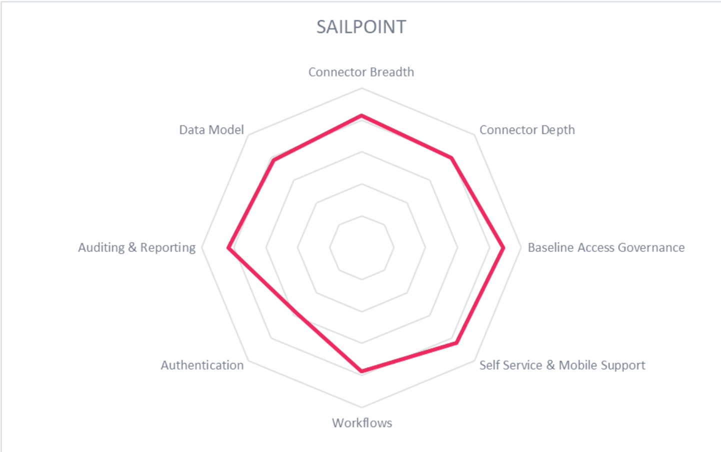
SailPoint originally started as a vendor specialized in Access Governance. However, since 2010 they have made strategic personnel and technology investments in the Identity Provisioning market that have accelerated the capabilities of their flagship product, IdentityIQ.The SailPoint IdentityIQ product now is a solution that integrates Access Governance and Identity Provisioning capabilities into a single product, i.e. a full IGA solution. SailPoint has enhanced its provisioning support massively over the past years.

Strengths	Challenges
• 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 provides separate multi-tenant cloud solution IdentityNow

Table 49: SailPoint major strengths and challenges

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. 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 50: SailPoint 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.

5.25 SAP

SAP has established a considerable IAM portfolio over the past years. It consists of both on premises tools and cloud services. For Identity Provisioning, the product to look at is SAP Identity Management. It is well-integrated with other SAP solutions such as SAP Access Control and SAP Business Suite and provides an overall strong set of capabilities for Identity Provisioning.

Strengths	Challenges
• Excellent integration into SAP environments, including SAP access control • Strong Identity Provisioning feature set • Integrates identity virtualization • Good role management capabilities	• Strong connectors for many systems, but some gaps particularly for non-SAP business applications • Some gaps in baseline Access Governance, but covered by other SAP offerings

Table 51: SAP major strengths and challenges

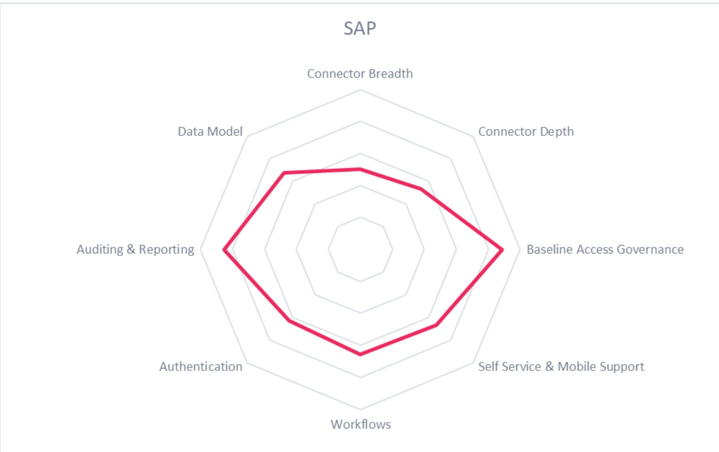
SAP has made significant progress with its SAP Identity Management offering over the past years. A couple of years ago, they have re-architected the program, exposing a comprehensive set of APIs now for simplified customization.

The product comes with the standard capabilities we expect to see, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service interfaces for password reset and management of the user's own identity. It also delivers good reporting and auditing capabilities.

When looking at the challenges we see, one is the relatively small set of connectors, when compared to other offerings in the market. While there is good support for common targets such as LDAP-based directory services, Microsoft Active Directory, SAP's own products and several other systems and applications, including some cloud services, support e.g. for mainframe environments or non-SAP business applications is lacking. Some of these gaps are filled by partners, with all the challenges arising from having a 3rd party providing connectors. Also, the Access Governance capabilities are limited to role management and auditing, while more complex requirements such as SoD controls are served by another SAP product, SAP Access Control.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 52: SAP rating



Despite these shortages we rate SAP as a strong offering in the market, showing significant progress. SAP also executes consequently on a well-thought-out product roadmap. In the current state, SAP Identity Management is an interesting contender in the Identity Provisioning market, particularly for organizations with large SAP infrastructures, but not being limited to these.

5.26 Systancia

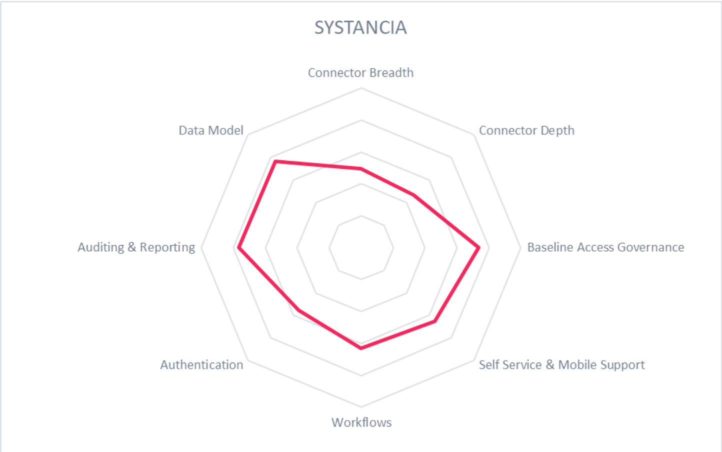
Systancia is a software company that started in the healthcare business. They have merged with French vendor Avencis a while ago. Avencis originally started in the E-SSO (Enterprise Single Sign-On) business. Later, they introduced their Hpliance solution for Identity Provisioning. It delivers Identity Provisioning capabilities, with specific capabilities but not limited to the healthcare market.

Strengths	Challenges
• Tight integration with the the Systancia SSOX product for E-SSO • Well thought-out approach to managing access controls of users • Can simulate forthcoming changes • Specific capabilities for the healthcare market	• Connector set is only average, with specific capabilities in healthcare environments • Limited global reach and still relatively small partner ecosystem

Table 53: Systancia major strengths and challenges

The Hpliance IAM solution has evolved to a considerably mature offering. It supports the standard requirements in Identity Provisioning and has a well-thought-out approach to managing entitlements of users. However, the connector set is only average, lacking breadth compared to other vendors. Given that initial target market has been the healthcare industry, they have strong support for this industry, but the connector support should also work out well for many other organizations. Furthermore, the workflow capabilities have been expanded to meet the common expectations of the market, even while it still lacks support for workflow standards and integration with external workflow tools.

We see a strong potential for the product through its integration with the SSOX solution, allowing customers to manage both authentication and access controls.



Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 54: Systancia rating

Due to the merger with Systancia, there is a global reach now, beyond the healthcare industry. For that market segment, the solution counts amongst the leading services. However, there is also strong potential for deployments in other industries, given the overall good feature set of the product. Systancia has numerous customer references in other industries.

5.27 Tools4ever

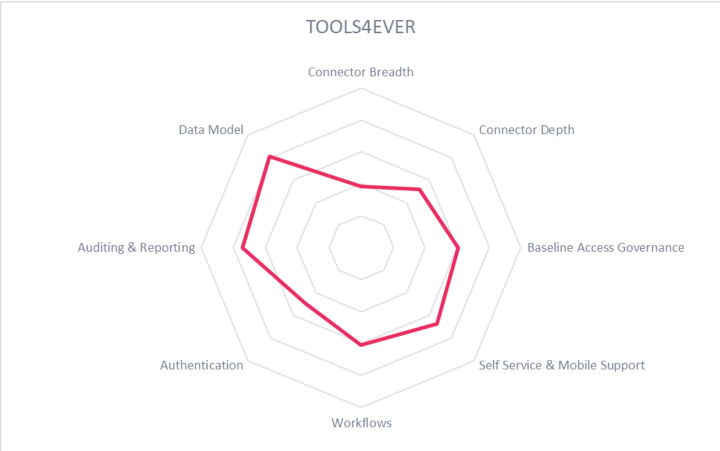
Tools4ever is a Dutch software company that started in the SMB market segment, but has grown its portfolio to a level where it also can serve the IAM requirements of larger organizations. Their main offering for Identity Provisioning is Identity & Access Manager, which covers the major features we expect to see in this market segment.

Strengths	Challenges
• Lean solution for Identity Provisioning • Overall good feature set • Well-thought-out approach for delegating tasks to service desks • Good baseline support for Access Governance	• Small vendor with limited partner ecosystem • Good, but not leading-edge set of connectors, but straightforward customization based on standard connectors

Table 55: Tools4ever major strengths and challenges

Tools4ever provides a solution that covers all major areas of Identity Provisioning, from a good set of connectors, also supporting integration to several HR systems, over password self-services, a good baseline Access Governance functionality to workflow management capabilities. In all these areas, it comes with some good but not yet leading-edge features. A specific strength is their support for delegating tasks to the helpdesk (or other users) in a flexible way. Thus, routine tasks can be distributed efficiently and in a well-managed approach. Furthermore, the solution is lean, compared to some of the more heavy-weight offerings in the market. On-premise and cloud solutions are offered.

While we'd love to see more out-of-the-box connectors, the number and range of connectors provided is overall good. Furthermore, custom connectors can be developed efficiently based on standard connectors for common protocols and interfaces.



Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 56: Tools4ever rating

We see particular potential in large medium-sized organizations and large family-owned businesses, where Tools4ever Identity & Access Manager can be a good fit. Overall, Tools4ever has made significant progress over the past years and moved to the level of a contender for the established players in the Identity Provisioning market. With offices in the U.S., UK, France, Germany, and the Netherlands, they have matured into an interesting alternative.

6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting 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 for these vendors. Notably, several vendors in the broader IDaaS market that are targeting primarily the Identity Provisioning functionality are covered in the KuppingerCole Leadership Compass on Identity Provisioning.

6.1 Atos

Atos has, aside of acquiring Evidian indirectly via their Groupe Bull acquisition, also acquired the former Siemens Business Services, which included the Siemens DirX portfolio. Both the former Evidian and the former Siemens portfolio are now united under the brand Evidian, with the product rated in this Leadership Compass being the new joint offering. However, the traditional DirX products are still available and maintained.

DirX Identity is a proven solution, but Atos has well-managed to modernize the tool and bring it to the level of current standards of IGA tools, with some areas of specific strength. Amongst these areas count the depth of connectors, the underlying support for identity data management based on the meta-directory capabilities, the high availability configurations, and the strong rule-based and role-based capabilities for managing access controls.

From a feature perspective, DirX Identity comes as an offering that delivers a comprehensive set of capabilities, with significant improvements made over the past years regarding the ease of customization and the overall flexibility of the offering. DirX Identity counts amongst the strong IGA offerings in the market.

6.2 Avanpost

Avanpost is a Russian vendor of an IAM solution, covering primarily Identity Provisioning capabilities, but with some limited Access Governance features. Their primary strength however is in supporting a broad range of authentication technologies, including integration with physical access control solutions.

6.3 Caradigm

Caradigm is a software vendor focused on delivering solutions for the Healthcare industry. Amongst other solutions, they deliver an IAM solution covering various areas including Identity Provisioning and Access Governance. Other capabilities include Single Sign-On and Multifactor Authentication.

6.4 Cion Systems

Cion Systems is addressing the market more from the Active Directory management angle. They thus might best be understood as a direct competitor to Microsoft FIM, also providing basic Access Governance capabilities as part of their product offering.

6.5 Deep Identity

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.

6.6 E-Trust

E-Trust is an IAM/IAG vendor headquartered in Brazil that delivers its own IGA solution called Horacius. The platform provides good workflow capabilities and supports features such as self-service access request and recertification. E-Trust is a strong candidate for inclusion in upcoming versions of the KuppingerCole Leadership Compass on Access Governance.

6.7 Identity Automation

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

6.8 Ilantus

Ilantus Technologies is a specialized vendor in the IAM domain. Being primarily a system integrator, it has recently moved to becoming an IDaaS vendor specializing in an enterprise-level solution covering both IDaaS SSO and IDaaS B2E requirements. Their core focus is deploying as-a-service offerings, not on premises solutions.

6.9 ITconcepts

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. This is named go:Identity. While Cognitum itself is attractive as a complementary tool for all IAM deployments, the standard solution is primarily targeted on SMBs.

6.10 ITMC Soft

Danish company ITMC is a software vendor that was founded by several persons with deep backgrounds in IAM system integration. Their product, IDM365, focuses on simplifying both deployment and use of IAM and IAG (identity and Access Management/Governance) infrastructures, particularly by delivering a strong set of out-of-the-box concepts and processes combined with a modern UI, thus reducing the need for long-running and costly implementation projects. With its current feature set, the product fits well into the Identity Provisioning and Access Governance market segments.

6.11 Microsoft

Microsoft's offering in the Identity Provisioning market segment is the Microsoft Identity Manager 2016 (MIM). The product has undergone various name changes in the past. The former Access Governance capabilities, which were based on assets acquired from BHOLD, have been discontinued. On the other hand, Microsoft Identity Manager comes with some specific add-on capabilities such as built-in baseline features for Privileged Account Management and key and certificate management. In sum, MIM follows a relatively technical approach to Identity Provisioning with focus more on synchronization than on workflows.

Microsoft Identity Manager 2016 still relies on the technical foundation of its predecessors. On the other hand, Microsoft has integrated some of the formerly isolated features such as the key and certificate management. Furthermore, the solution is increasingly complemented by Azure-based offerings such as password management in integration with Microsoft Azure Multi Factor Authentication (MFA) and Azure-based reporting capabilities.

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. The set of connectors provided out-of-the-box is good, but not leading-edge. Several partners deliver additional connectors if required.

Microsoft Identity Manager is not part of the rating due to the fact that it is positioned less as a stand-alone Identity Provisioning offering, but the link between existing on premises Active Directory environments and Azure Active Directory infrastructures, but not as the strategic Identity Management offering of Microsoft anymore.

6.12 **Ogitix**

Ogitix is a German company that provides an IAM solution targeted at the SMB market, with focus on the local market. It provides some interesting capabilities, but is not yet at the level of enterprise solutions in the area of Identity Provisioning. However, for SMBs, the Ogitix solutions might be evaluated as a lean alternative to the established players.

6.13 **RSA Security**

RSA Security delivers, as part of their RSA SecurID Suite, its own IAM solution. The product named RSA Identity Governance & Lifecycle is based on the product which came into the RSA portfolio via the Aveksa acquisition. While there is some baseline support for Identity Provisioning, the product is clearly targeted at the Access Governance and IGA market, for customers that start with Access Governance. It also integrates with other Identity Provisioning solutions. The offering is covered in other KuppingerCole Leaderships in that field, including the Leadership Compass Access Governance.

6.14 **SmartAIM**

SmartAIM is a company delivering a number of IGA solutions covering various aspects of this market. They are still small, but might become a vendor that is considered in the next edition of this KuppingerCole Leadership Compass.

6.15 Trustverse

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.

6.16 Usercube

Usercube is a French software company delivering an IAM solution based on the Microsoft technology platform. We consider it a product that might be included in the next edition of this KuppingerCole Leadership Compass, but not yet being mature enough.

6.17 Wise Identity

Wise Identity has acquired the former IAM solution of Netprof. The solution is a specialized Identity Provisioning solution targeting the Education market segment. Thus, their offering is rather specialized, however providing some interesting specific capabilities.

6.18 WSO2

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. It is more an Identity API and development platform, which is targeted at customers integrating IAM and other capabilities into customer solutions. Due to their concept of targeting more towards connecting businesses with partners and customers, their out-of-the-box support for on-premise Identity Provisioning requirements is somewhat limited. However, for customers looking for an Identity API platform, WSO2 is a very interesting option that should be evaluated.

7 Methodology

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

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

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

7.1 Types of Leadership

We look at four types of leaders:

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

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

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

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

7.2 Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

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

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

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

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

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

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

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

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

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

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

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

7.3 Vendor rating

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

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

Market position – measures the position the vendor has in the market or the relevant market segments. This is an average rating 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 considers the vendor's presence in major markets.

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

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

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

7.4 Rating scale for products and vendors

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

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

7.5 Spider graphs

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

Connector Breadth	The number of connectors and the breadth of target systems, including e.g. directory services, business applications, mainframe systems, and others. Also, broad support for common cloud services is rated here.
Connector Depth	Capabilities of connectors, in particular when it comes to connecting to complex target systems such as SAP environments or mainframes. This rating also looks at customization capabilities for connectors through connector toolkits.
Baseline Access Governance	Integrated Access Governance capabilities, including baseline Access Review, Role Management, and SoD (Segregation of Duties) controls.
Self-Service & Mobile Support	User self-service interfaces and support for secure mobile access to selected capabilities.
Workflows	Advanced workflow capabilities, including graphical workflow configuration, for supporting the various requirements of Identity Provisioning.

Authentication	Support for strong and adaptive authentication for both administrators and end users accessing the service.
Auditing & Reporting	Extensive auditing and reporting capabilities, including analytical capabilities for analysing the current state of entitlements.
Data Model	Flexible but centralized data model that allows customization by the customer for its specific need.

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

7.6 Inclusion and exclusion of vendors

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

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

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

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

We provide a quick overview about vendors not covered and their Identity Provisioning offerings in chapter 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.

8 Copyright

The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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