KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | October 2014

Access Governance

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

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

Leadership Compass
Access Governance
By KuppingerCole

KuppingerCole Leadership Compass
Access Governance
Report No.: **70948**

Content

1. **Management Summary** 7
2. **Methodology** 12
3. **Product Rating** 13
4. **Vendor Rating** 15
5. **Vendor Coverage** 16
6. **Market Segment** 17
7. **Specific features analyzed** 21
8. **Market Leaders** 22
9. **Product Leaders** 24
10. **Innovation Leaders** 25
11. **Product/service evaluation** 26

11.1 AlertEnterprise Enterprise Guardian 27
11.2 Atos DirX Identity 28
11.3 Avatier Compliance Auditor 29
11.4 Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager 30
11.5 Brainwave Identity GRC 31
11.6 CA GovernanceMinder 32
11.7 Courion Access Assurance Suite 33
11.8 CrossIdeas IDEAS 34
11.9 Deep Identity IACM / IM / FsGA 35
11.10 Dell One Identity Manager 36
11.11 EmpowerID 37
11.12 Evidian Identity & Access Manager 9 38
11.13 Hitachi ID Identity Manager 39
11.14 IBM Security Identity Manager (“ISIM”) 40
11.15 iSM Secu-Sys bi-Cube® 41
11.16 Microsoft Identity Manager 42
11.17 NetIQ Access Governance Suite 6.2 43
11.18 Omada Identity Suite 44
11.19 Oracle Identity Governance Suite 45
11.20 RSA Identity Management and Governance (IMG) 46
11.21 SailPoint IdentityIQ 47
11.22 SAP Access Control and Identity Analytics 48

11.23 Whitebox Security WhiteOPS™ Intelligent Access Governance Suite ... 49
11.24 WSO2 Identity Server ... 50
12. Products at a glance ... 51
12.1 Ratings at a glance ... 51
12.2 The Market/Product Matrix ... 54
12.3 The Product/Innovation Matrix ... 55
12.4 The Innovation/Market Matrix ... 56
13. Overall Leadership ... 58
14. Vendors and Market Segments to watch ... 59
14.1 Avanpost ... 59
14.2 Bay31 ... 59
14.3 Cion Systems ... 60
14.4 E-Trust ... 60
14.5 Fischer International ... 60
14.6 Indeed-Id ... 60
14.7 OpenIAM ... 60
14.8 SmartAIM ... 60
14.9 Tools4ever ... 60
15. Copyright ... 62

Content Tables

Table 1: AlertEnterprise Enterprise Guardian major strengths and weaknesses. ... 27
Table 2: AlertEnterprise Enterprise Guardian rating. ... 27
Table 3: Atos DirX Identity major strengths and weaknesses. ... 28
Table 4: Atos DirX Identity rating. ... 28
Table 5: Avatier Compliance Auditor major strengths and weaknesses. ... 29
Table 6: Avatier Compliance Auditor rating. ... 29
Table 7: Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager major strengths and weaknesses. ... 30
Table 8: Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager rating. ... 30
Table 9: Brainwave Identity GRC major strengths and weaknesses. ... 31
Table 10: Brainwave Identity GRC rating. ... 31
Table 11: CA GovernanceMinder major strengths and weaknesses. ... 32
Table 12: CA GovernanceMinder rating. ... 32
Table 13: Courion Access Assurance Suite major strengths and weaknesses. ... 33

Table 14: Courion Access Assurance Suite rating. 33
Table 15: CrossIdeas IDEAS major strengths and weaknesses. 34
Table 16: CrossIdeas IDEAS rating. 34
Table 17: Deep Identity IACM / IM / FsGA major strengths and weaknesses. 35
Table 18: Deep Identity IACM / IM / FsGA rating. 35
Table 19: Dell One Identity Manager major strengths and weaknesses. 36
Table 20: Dell One Identity Manager rating. 36
Table 21: EmpowerID major strengths and weaknesses. 37
Table 22: EmpowerID rating. 37
Table 23: Evidian Identity & Access Manager 9 major strengths and weaknesses. 38
Table 24: Evidian Identity & Access Manager 9 rating. 38
Table 25: Hitachi ID Identity Manager major strengths and weaknesses. 39
Table 26: Hitachi ID Identity Manager rating. 39
Table 27: IBM Security Identity Manager (“ISIM”) major strengths and weaknesses. 40
Table 28: IBM Security Identity Manager (“ISIM”) rating. 40
Table 29: iSM Secu-Sys bi-Cube® major strengths and weaknesses. 41
Table 30: iSM Secu-Sys bi-Cube® rating. 41
Table 31: Microsoft Identity Manager major strengths and weaknesses. 42
Table 32: Microsoft Identity Manager rating. 42
Table 33: NetIQ Access Governance Suite 6.2 major strengths and weaknesses. 43
Table 34: NetIQ Access Governance Suite 6.2 rating. 43
Table 35: Omada Identity Suite major strengths and weaknesses. 44
Table 36: Omada Identity Suite rating. 44
Table 37: Oracle Identity Governance Suite major strengths and weaknesses. 45
Table 38: Oracle Identity Governance Suite rating. 45
Table 39: RSA Identity Management and Governance (IMG) major strengths and weaknesses. 46
Table 40: RSA Identity Management and Governance (IMG) rating. 46
Table 41: SailPoint IdentityIQ major strengths and weaknesses. 47
Table 42: SailPoint IdentityIQ rating. 47
Table 43: SAP Access Control and Identity Analytics major strengths and weaknesses. 48
Table 44: SAP Access Control and Identity Analytics rating. 48
Table 45: Whitebox Security WhiteOPS™ Intelligent Access Governance Suite major strengths and weaknesses. 49
Table 46: Whitebox Security WhiteOPS™ Intelligent Access Governance Suite rating. 49
Table 47: WSO2 Identity Server major strengths and weaknesses. 50
Table 48: WSO2 Identity Server rating. 50

Table 49: Comparative overview of the ratings for the product capabilities. 52

Table 50: Comparative overview of the ratings for vendors. 53

Table of Figures

Fig. 1: Overall Leaders in the Access Governance market segment 8

Fig. 2: Product Leaders in the Access Governance market segment 9

Fig. 3: Market Leaders in the Access Governance market segment. 10

Fig. 4: Innovation Leaders in the Access Governance market segment 11

Fig. 5: The status and expected evolution of Access Governance 20

Fig. 6: Market leaders in the Access Governance market segment. 22

Fig. 7: Product leaders the Access Governance market segment. 24

Fig. 8: Innovation leaders in the Access Governance market segment. 25

Fig. 9: The Market/Product Matrix. 54

Fig. 10: The Product/Innovation Matrix. 55

Fig. 11: The Innovation/Market Matrix. 56

Fig. 12: The Overall Leadership rating for the Access Governance market segment. 58

Related Research

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

Advisory Note: Access Governance Architectures - 71039

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

Executive View: Beta Systems SAM Enterprise Identity Manager - 70907

Executive View: Brainwave Identity GRC - 70985

Executive View: EmpowerID 2013 - 70005

Executive View: IBM Security QRadar® - 70980

Executive View: NetIQ Identity Manager - 70901

Executive View: Omada Identity Suite - 70828

Executive View: RSA Aveksa Identity Management & Governance - 70873

Executive View: SailPoint IdentityNow - 70826

Leadership Compass: Cloud User and Access Management - 70969

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Dynamic Authorization Management - 70966

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: EmpowerID - 71115

Product Report: CrossIdeas IDEAS - 70897

Product Report: CA IdentityMinder™ - 70914

Product Report: CA GovernanceMinder™ - 70837

Product Report: SAP GRC Access Control 10 - 70737

Product Report: SailPoint IdentityIQ 5.2 - 70287

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

Scenario: Understanding Cloud Security - 70321

Scenario: Understanding Cloud Computing - 70157

Scenario: Understanding Identity and Access Management - 70129

Vendor Report: Dell IAM - 70812

Vendor Report: Courion Corporation - 70920

Vendor Report: Avatier - 70144

Vendor Report: Atos DirX - 70741

Vendor Report: NetIQ – the complete portfolio - 70624

1. Management Summary

Access Governance remains one of the fastest growing market segments in the broader IAM/IAG (Identity and Access Management/Governance) market. Over the past few years, this segment has evolved significantly. Access Intelligence, providing advanced analytical capabilities for identifying access risks and analyzing the current status of entitlements is one of these additions. Improved capabilities in managing access risks are another. Some vendor have also added user activity monitoring to their products.

However, features such as access recertification, access request management, role management and SoD (Segregation of Duties) management remain at the center of the capabilities within this market segment. Most vendors also have some functionality for connecting back to the target systems, i.e. some included Identity Provisioning capabilities. However, there are still vendors in the market that focus only on the Access Governance portion, while others support both deployment on top of an existing Identity Provisioning solution and integrated deployments. Depending on the current existing IAM infrastructure and the customer requirements, an integrated solution or a separate one might be the better choice.

A few years ago, there were only a handful of vendors in the Access Governance market. While the large players in the overall IAM/IAG market made acquisitions, new players entered the market, and some of the Identity Provisioning vendors developed Access Governance capabilities by themselves. In contrast to the 2013 edition, the number of vendors has now grown to more than 20 vendors included in this analysis.

This Leadership Compass provides an overview and analysis of the Access Governance market segment. Access Governance nowadays goes well beyond access recertification, role management and analytics. Strong capabilities for access request management, access analytics, and advanced direct or indirect capabilities of provisioning changes back are mandatory features. In addition, access risk management, enhanced data governance for non-structured data, or improved integration with, for instance, Privilege Management tools or User Activity Monitoring solutions are increasingly common. The Access Governance market is changing and our rating not only focuses on the traditional capabilities but also takes into account what we expect to become the new key features.

The analysis shows that there are several established vendors with mature solutions, but also some very interesting smaller or regional vendors with a good potential for growth and for delivering what customers require. Furthermore, there are some specialized players providing specific point solutions for role and risk analytics or just taking another approach on the overall IAM/IAG market. While not being leaders in a standardized comparison of a market segment, these might be excellent fits for some customers.

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

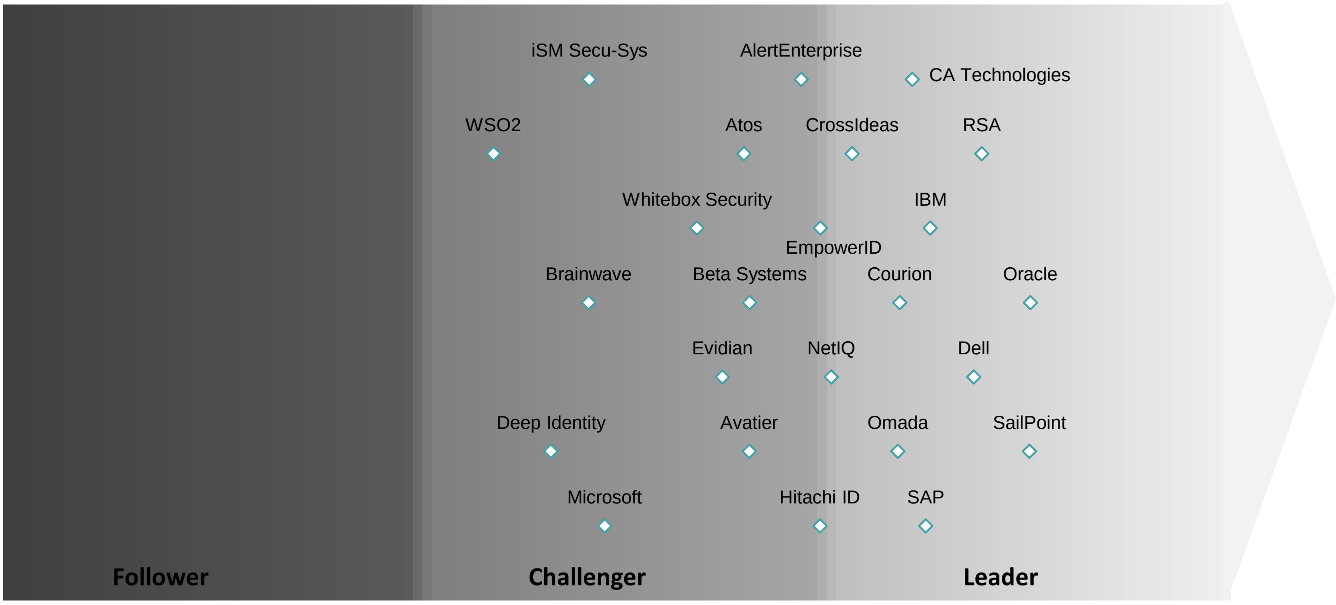

Fig. 1: Overall Leaders in the Access Governance market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at the Overall Leadership, we see a number of vendors in the Leaders segment. Oracle and SailPoint are leading, closely followed by Dell and RSA, who acquired Aveksa in 2013.

Following these, we see some other big names out of the software industry. CA Technologies, IBM, SAP, and NetIQ all score well in the Overall Leadership rating. This is certainly caused by their strong market position, but is also based on product capabilities and their ability to consequently innovate based on their roadmaps.

We also see Omada and Courion among the leaders in this market segment. Both are quite innovative, with Courion being among the first ones delivering advanced Access Intelligence capabilities as part of their offering and Omada with their new governance workbench. Finally, there is CrossIdeas, an IBM Company, in the Leader segment, which - after their recent acquisition by IBM - now have a stronger financial background, in addition to their long-standing strength in product capabilities and innovation.

There are a number of vendors in the Challenger segment that are very close to moving into the Leader segment. EmpowerID, Hitachi ID, AlertEnterprise, and NetIQ all are candidates for becoming Leaders in the next edition of this Leadership Compass. Besides them, several other vendors are placed in good positions in this rating.

Only a few vendors fall somewhat behind. However, all of them have their particular strengths. While Deep Identity is innovative, they have still a very limited market presence. WSO2 takes a fundamentally different approach to IAM/IAG, based on a business process integration platform. As of now, the built-in feature set is somewhat limited, but flexibility for customization and scalability are strong, which makes them an interesting pick for specific use cases.

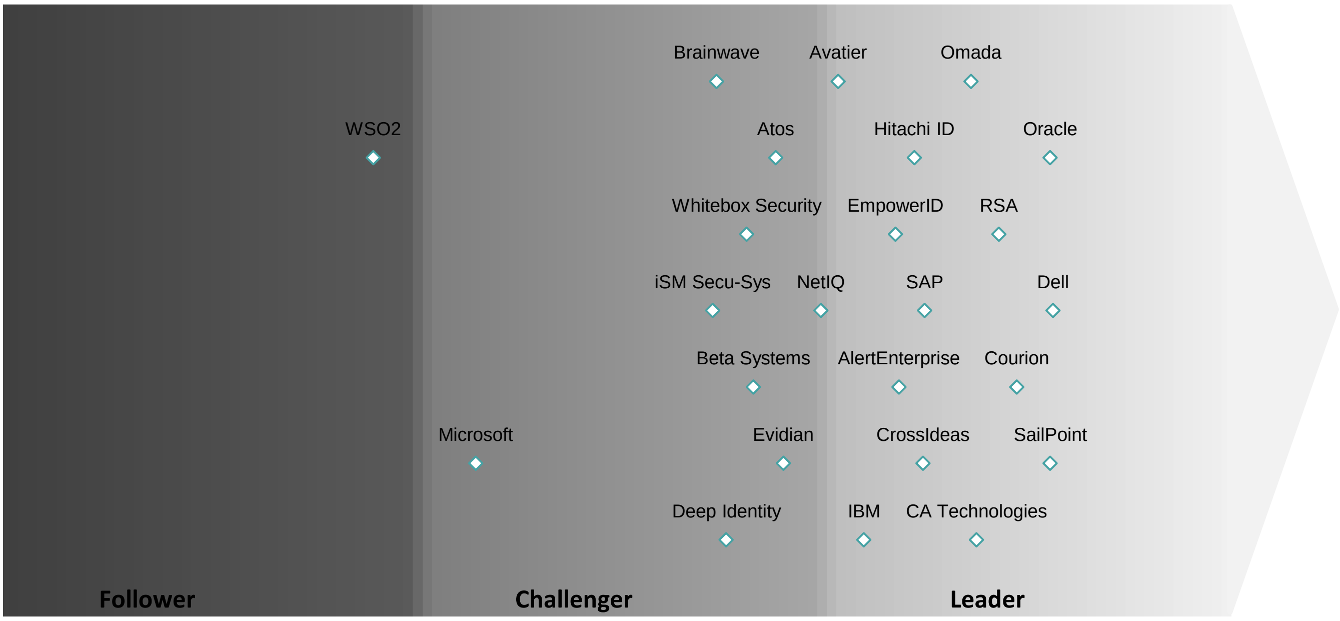

Fig. 2: Product Leaders in the Access Governance market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at Product Leadership, we again see some of the large vendors in front. Dell, Oracle, and SailPoint are leading, followed by Courion, RSA, CA Technologies, and Omada. SAP is also placed well, taking a different approach to Access Governance. However, with their integration into solutions other than SAP Risk Management they have a strong offering, and not only for SAP environments.

There are a number of other vendors in the Leader segment, including CrossIdeas, an IBM Company, AlertEnterprise, and others. The number of leaders proves that overall maturity of the Access Governance segment has increased significantly over the past 18 months, since we last did this analysis.

We also see a number of challengers that are in good positions. These include NetIQ, being very close to a leader position with both their integrated capabilities in the NetIQ Identity Manager including their Access Review offering, and their Access Governance Suite, and a number of other vendors. Again, there are a few vendors that are not in a leading position. Microsoft is among these, showing limited innovation in their offering and limited integration. However, for customers of Microsoft FIM, this might be a sufficient solution anyway.

Furthermore, there is WSO2 in the Follower section. As mentioned above, they take a somewhat different approach to Access Governance. They are a great fit for some customer scenarios anyway, but do not cover all standard requirements in the Access Governance market.

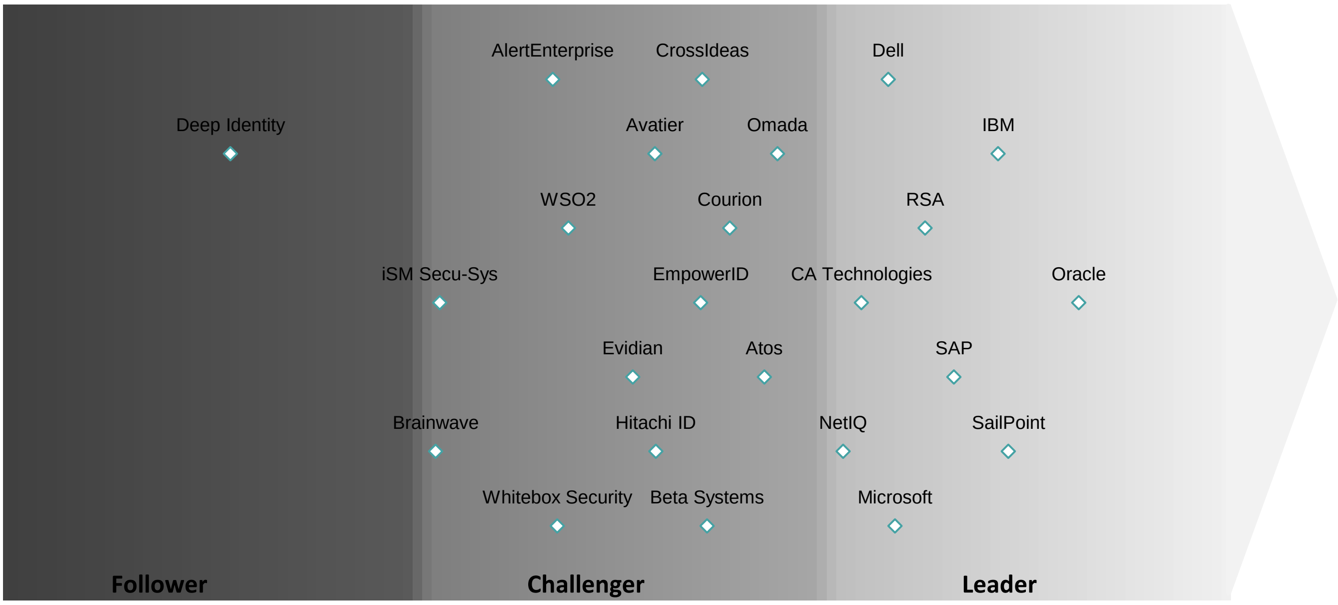

Fig. 3: Market Leaders in the Access Governance market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at the market leaders, it is no surprise that the big names are among at the top. Oracle, IBM, SAP, SailPoint, RSA, and also Microsoft take a strong position, followed by Dell, CA Technologies, and NetIQ that are also placed in the Leader segment.

We also see a large number of Challengers, with some being close to the Leader segment such as Omada and Atos, indicating a quite strong position in the market, while others are placed more to the left, indicating a smaller customer base and, in most cases, also a regional presence.

In the Follower section, we find Deep Identity, which yet have a small customer base and partner ecosystem.

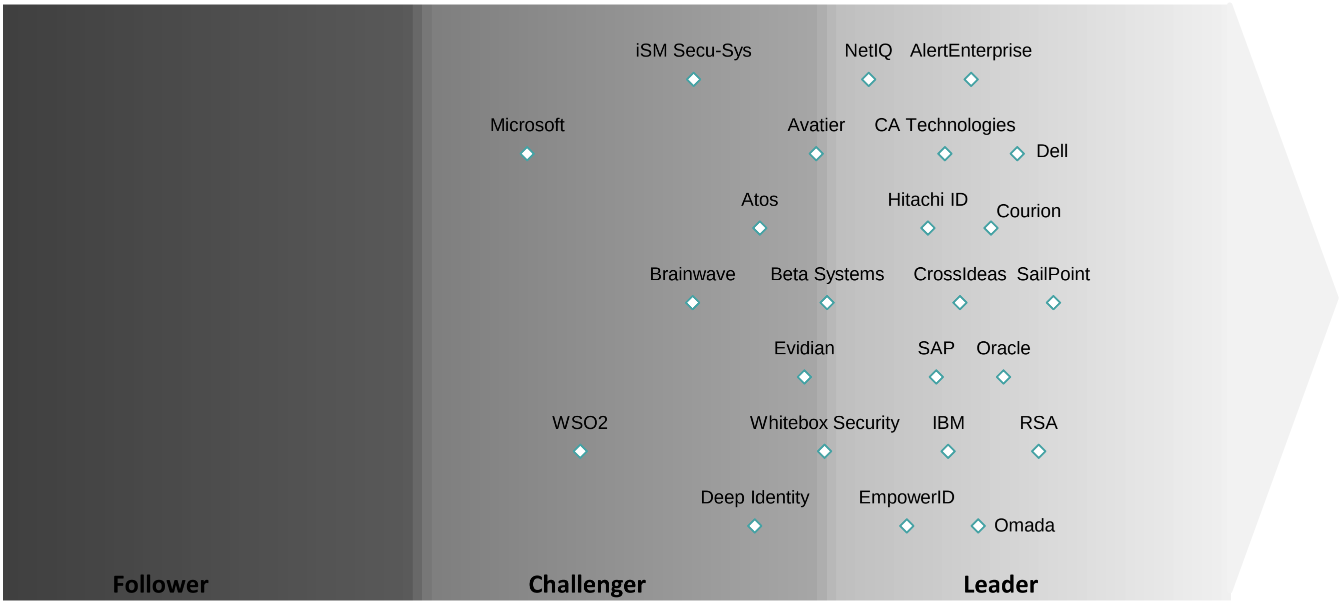

Fig. 4: Innovation Leaders in the Access Governance market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

When looking at leadership in innovation, we find SailPoint slightly in front. The company has invested heavily into its technology in the past 18 months and executes well on its roadmap.

Besides the large vendors, some others are of specific interest. AlertEnterprise focuses on managing not only standard IT environments but also ICS (Industrial Control Systems) and physical access control solutions, providing a broader approach to Access Governance. Whitebox Security supports a well thought-out approach on real time access risk and threat analytics. Beta Systems is among the innovators in the field of Access Intelligence.

We also see a number of vendors in the Challenger section that are close to becoming a Leader. Avatier shows particular strength in its user interfaces and might be a good complement to existing IAM infrastructures, when smooth interfaces are required. Evidian has its strengths in the integration of a number of capabilities.

From the vendors more to the left, WSO2– as mentioned for the other leadership ratings – takes a different approach but might be a good fit for various use cases. In the case of Microsoft, the rating is caused among other reasons by a lack of some integration capabilities we look for when rating innovation and the fact that the current release mainly was focused on integration of the recently acquired BHOLD assets into the Microsoft FIM product. We expected Microsoft to become more innovative over the next 18 months, but have seen little evolution in their Access Governance capabilities.

2. Methodology

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

We look at four types of leaders:

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

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

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag behind in some areas, such as 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.

In addition, we have defined a series of matrices which

- Compare, for instance, the rating for innovation with the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path than established vendors, but also established vendors which no longer lead in innovation. These additional matrices provide additional viewpoints on the vendors and should be considered when picking vendors for RfIs (Request for Information), long lists, etc. in the vendor/product selection process.
- Add additional views by comparing the product rating to other feature areas. This is important because not all customers need the same product, depending on their current situation and specific requirements. Based on these additional matrices, customers can evaluate which vendor fits best to their current needs but also is promising regarding its overall capabilities. The latter is important given that a product typically not only should address a pressing challenge but become a sustainable solution. It is a question of helping now, but also being good enough for the next steps and future requirements. Here these additional matrices come into play.

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

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, a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

3. Product Rating

KuppingerCole as an analyst company regularly does evaluations of products,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

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

weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

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

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

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 increase costs, but inevitably lead to mistakes and breakdowns. This will create openings for attack and failure.

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

4. Vendor Rating

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

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

5. Vendor Coverage

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

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

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

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

For this Leadership Compass document, some vendors decided not to participate due to a specific focus of their products or other reasons. Various vendors are covered briefly at the end of this document. Of the larger players in the IAM/IAG market, Fischer did not return our questionnaire. However, the vendor might also be worth evaluating, given that it has a long history in the field and a platform that provides well thought-out customization capabilities.

6. Market Segment

Access Governance concerns the mechanisms, processes relations and management of access controls in IT systems and thus is about mitigating access-related risks. These risks include the theft of information, fraud through changes to information, and the subversion of IT systems - for example in banking - to facilitate illegal actions, to name just a few. The large number of prominent incidents within the last few years proves the need to address these issues – in all industries. The loss of privacy-related customer data or industrial espionage is a problem in virtually every industry, besides industry-specific issues such as the illegal actions of stock dealers.

Simply said, Access Governance focuses on providing answers to three key questions:

- Who has access to what?
- Who has accessed what?
- Who has granted that access?

That is done via a set of functionalities, which include the following features:

- Access „Warehouses“: Collecting current and historic access controls from different systems. The collection can be done either via Provisioning tools or by the Access Governance systems’ own connectors. Frequently the collection is based on imports of flat files.
- Access Recertification: Requiring the responsible persons (such as departmental managers or system and information owners) to do scheduled or ad-hoc periodic reviews of the current status of access controls and request changes if required.
- Access Analytics and Intelligence: Analytical capabilities to facilitate understanding the current status of access controls, sometimes complemented by adding real-time monitoring information about information access.
- Access Risk Management: Defining risks for systems or (better) information and allowing actions and analysis based on these risks.
- Access Request Management: Providing interfaces to request access to specific information or systems.
- SoD controls and enforcement: Definition and enforcement of business rules to control Segregation of Duties.
- Enterprise Role Management: A complementary technology given that roles are the typical method used to manage access. Thus Enterprise Role Management, including the capability of analysing and defining roles, is mandatory.

Access Governance is one of the core areas to cover for any organization due to the potential massive impact of incidents. Access risks might have severe operational impact and might even relate to strategic risks – the Barings Bank incident and the Société Générale scandal being two of many prominent examples. However, there are many other issues which might also affect the business: The loss of blueprints to competitors, fraud in ERP systems including illegal financial transactions, reputation problems due to the loss of privacy-related data, secret documents being unveiled to the press, and many more.

Access Governance products focus on implementing controls for access management. That includes manual controls based on attestation and recertification processes as well as auditing capabilities which include automated controls for detecting changes which don't comply with policies. And that, in turn, includes active management for preventive controls to mitigate the risks. Additional aspects are role management capabilities as part of the management processes.

These features are currently mainly provided by two distinct groups of products. One is the pure play Access Governance solutions market segment, the other is the Identity Provisioning tools market segment. Some support is also found in IT GRC tools which offer at least recertification support as a feature but usually lack other standard features of Access Governance tools such as Access Request Management. Besides these there are some solutions for specific environments, especially SAP, which provide some Access Governance functionality with a focus mainly on the SAP environments.

During the last few years, several start-ups have appeared in the market with specific solutions for Access Governance only. On the other hand, many of the Provisioning tools vendors have started adding capabilities for access governance to their existing solutions, especially for attestation and recertification. Interestingly, virtually all of the pure-play Access Governance vendors have recently started to add provisioning functionalities to their products. Thus, the market today is mostly divided into products which started with Access Governance and are in many cases not as strong in provisioning, and others which started in provisioning and added Access Governance. It comes as no surprise that many of these solutions are not as strong in Access Governance – yet. But clearly, the segmentation between these categories is diminishing over time.

There are strengths with both approaches. Separate Access Governance tools can address all systems and they can integrate multiple provisioning tools. Using Provisioning tools, however, reduces the need to interface with systems twice and provides a direct integration for implementing preventive controls. The decision between these categories depends on several factors, including the existing infrastructure, the systems to be covered, the workflow capabilities of the chosen provisioning tool, and many more.

Overall, we observe two distinct trends. The first is a trend towards using specific, additional Access Governance tools to cover the full breadth of existing systems beyond the ones which are automatically managed by Identity Provisioning tools – the latter frequently being limited to (configured) connections to just a few systems. While Identity Provisioning tools theoretically can support virtually any target system, most customers in practice use only a few connectors to a set of selected systems, due to the organizational and sometimes technical complexity of connecting systems. There are even several Access Governance vendors which have OEM agreements with Provisioning vendors to provide a complete solution. There are also Access Governance vendors providing some Identity Provisioning capabilities while also providing integrations with other Identity Provisioning products. This is about keeping a modular approach – a concept that is driven both by some of the vendors and by various customers.

The second trend we observe is towards unified solutions, integrating Access Governance and Identity Provisioning into a single solution. Again, some customers favor that approach and some vendors follow that strategy.

Obviously, there is no single right system of Access Governance. It depends on the customer requirements, whether unified solutions or modular systems are the better choice.

From the KuppingerCole perspective, a complete Access Governance approach has to go beyond the "standard users" and to cover privileged access as well, e.g. administrative access, technical users, system-level accounts, and other types of privileged (and frequently shared) accounts. However, we don't see many vendors in the market right now which have a well thought-out, deep integration of Privilege Management with the standard Access Governance features. There are some few players in the market already delivering on that, but the mass lacks this integration. While privileged users are pretty much the same as "standard" users from an Access Governance perspective, Privilege Management tools add features such as restricting elevation of rights at run-time and managing shared account passwords. Complete solutions would require tight integration between both groups of capabilities, to not only identify the risk in Access Governance but mitigate it by using specific Privilege Management capabilities.

We also see the need for looking at advanced, integrated capabilities of managing access controls within the target systems such as SAP environments or Microsoft Windows File Server/Active Directory environments. Some vendors are moving in the direction of Entitlements and Access Governance (EAG)[3].

From a KuppingerCole view there is a need for specific tools for specific sets of controls which provide in-depth governance and management functionality below the integrating layer of CCM (Continuous Controls Monitoring) or IT GRC. We don't expect that higher-level GRC tools can successfully replace specific Access Governance solutions but understand the need for a tight integration with such tools out-of-the-box.

Summarized, these are the features we understand as core elements of Access Governance solutions:

- Policy and Role Management to define the roles, business rules, and SoD policies in place within an organization.
- Attestation and Recertification as detective, manual controls which allow organizations to analyze the status of access controls in a structured way.
- Auditing and Analysis features which support an after the fact view to access-related events.
- Access Request Management as the preventive, at least partially automated, process including automated reconciliation.
- Integrated (!) Privilege Management features for extending these controls to privileged users, which today aren't typically covered by the standard access governance tools.
- Support for EAG (Entitlement and Access Governance).

Over time a deep integration with Dynamic Authorization Management Systems which are used to centrally define policies for application and system security is required as well. However, there are still few solutions in the market providing even minimal integration.

[3] **http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214**

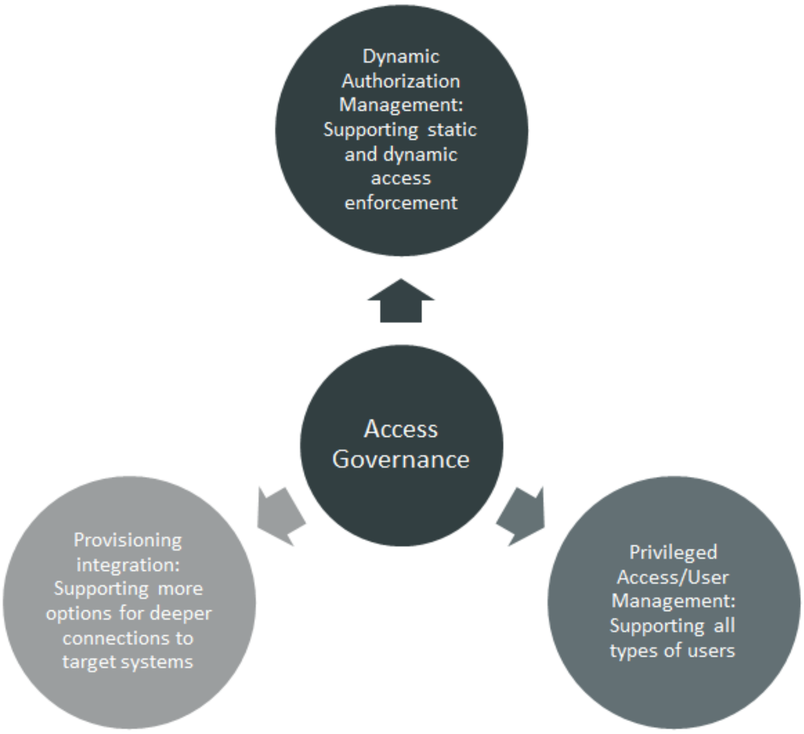
Dynamic Authorization Management: Supporting static and dynamic access enforcement
Access Governance
Provisioning integration: Supporting more options for deeper connections to target systems
Privileged Access/User Management: Supporting all types of users

Fig. 5: The status and expected evolution of Access Governance

To achieve this, features for role management, policy management, rule definition and analysis, workflows as well as additional functionality are required. Dashboards for executives and extended auditing and reporting capabilities are a part of these tools. Risk management features are recommended but not yet a standard feature of all products in the market.

To connect with target systems, Access Governance tools should support different types of interfaces:

- Connectors to extract access control status information out of target systems, frequently using flat file exports;
- Interfaces to provisioning systems to use their access management features for active management and, in some cases, to extract access control status information;
- Direct connectors to target systems for changing access control information in these systems;
- Interfaces to Service Request Management (SRM) tools which are used to manually provide information to target systems;
- Workflows providing manual tasks to operators. The execution of these tasks should be automatically tracked by the analysis features of the product.

An increasing number of tools support all these features at least to some extent. An in-depth analysis of architectural options for Access Governance is provided in the KuppingerCole Advisory Note #71,039 “Access Governance Architectures”[4].

[4] **http://www.kuppingercole.com/report/adnote_accessgov_7103914314**

7. Specific features analyzed

When evaluating the products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- core features of Access Governance 6

we also considered several specific features. These include:

Connectivity
The ability to connect to various sources of target systems, including direct connections, integration with existing Identity Provisioning tools from various vendors, and integration to SRM (Service Request Management) solutions. In general we expect Access Governance solutions of today to not only read data from target systems but provide changes back.

Flexibility
This is about the possibility to use the solution on top of existing Identity Provisioning implementations as well as in “full stack” implementations. Having the ability to support all types of architectures is an important feature.

Standards
Support for standards, particularly SPML (legacy) and SCIM, is considered important as well for simplified integration to Identity Provisioning tools as well as target systems.

Deployment models
In today’s IT environments, flexibility in deployment models is of high importance. We looked at support for soft appliance, hard appliance, and Cloud/MSP deployment models.

Customization
The less you need to code and the more you can configure, the better – that’s the simple equation we took into account around customization. However, we also looked for features like a transport system to segregate development, test, and production environments. Notably, copying configuration files does not count for a transport system.

Analytical capabilities
Advanced analytical capabilities beyond reporting, using standard BI (Business Intelligence) technology or other advanced approaches are becoming increasingly important.

Role and risk models
Especially in Access Governance, what counts is the quality and flexibility of role and risk models. These models not only need to look nice, there needs to be a strong conceptual background and sufficient flexibility to adapt to the customer’s need. Unfortunately not every tool that looks nice at first glance is sophisticated enough to cover all needs of customers. But it is not the customer adapting to the tool, it should be the tool adapting to the customer.

EAG[5] Support for Entitlement and Access Governance (EAG), i.e. the ability to also analyze entitlements at the level of underlying systems such as SAP, Windows file servers, etc.

Multi tenancy Given the increasing number of cloud deployments, but also specific requirements in multi-national and large organizations ("chinese walls"), support for multi-tenancy is highly recommended.

Role/SoD concept Provisioning should be feasible based on role concepts and with support for the definition of SoD rules (Segregation of Duties), despite the fact that Access Governance tools are increasingly used on top of Identity Provisioning.

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

8. Market Leaders

Based on our evaluation of the products, we've identified (as mentioned above) different types of leaders in the Access Governance market segment. The market leaders are shown in figure 6.

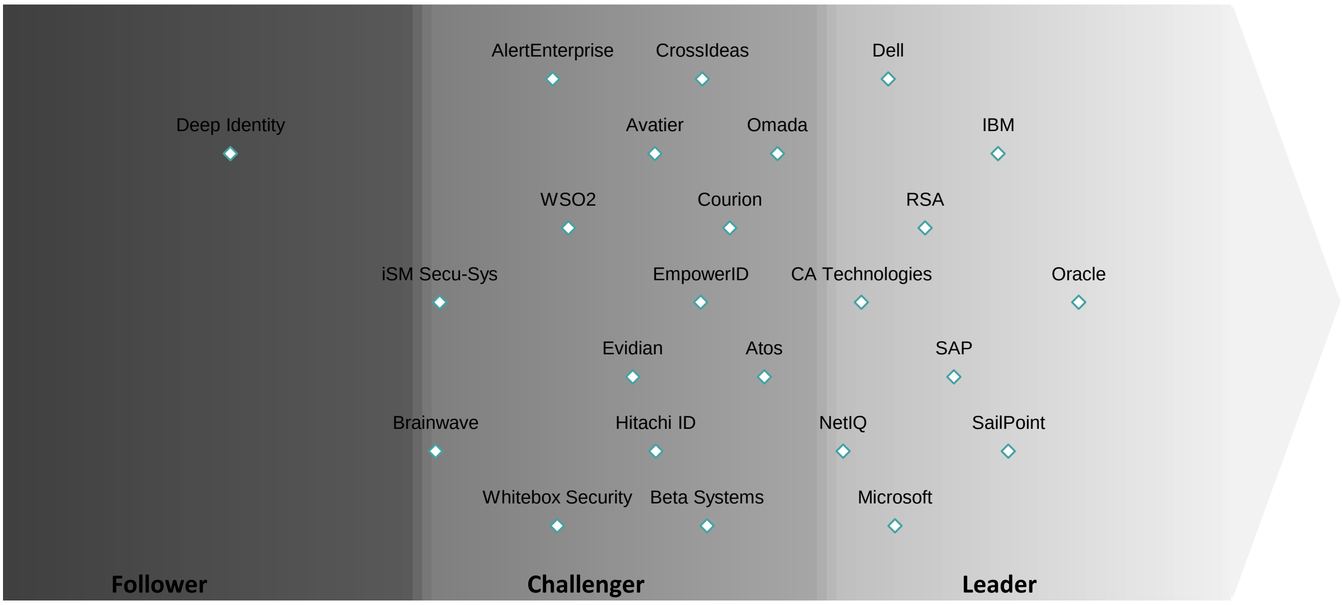

Fig. 6: Market leaders in the Access Governance market segment.

The market is affected by a situation where several very large software vendors compete with a large number of smaller vendors, which, frequently, are only acting regionally. Market leadership is mainly a hint at the overall position of the vendor regarding the number and size of customers, its strength in sales, and its partner ecosystem.

[5] http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214

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

Market Leadership is an indicator for the ability of vendors to execute on projects. However this depends on other factors as well. Small vendors might be well able to execute in their "home base". Small vendors sometimes are more involved directly in projects, which can be positive or negative – the latter, if it leads to branches in product development which aren't managed well. Besides that, the success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with a good ecosystem might fail in projects.

When looking at the market leaders, it is no surprise that the big names are among the leaders. Oracle, IBM, SAP, SailPoint, RSA, and Microsoft take a strong position, followed by Dell, CA Technologies, and NetIQ that are also placed in the Leader segment.

We also see a large number of Challengers, with some being close to the Leader segment such as Omada and Atos, indicating a quite strong position in the market, while others are placed more to the left, indicating a smaller customer base and, in most cases, also a regional presence.

In the Follower section, we find Deep Identity, which yet have a small customer base and partner ecosystem.

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

Market Leaders (in alphabetical order):

- CA Technologies
- Dell
- IBM
- Microsoft
- NetIQ
- Oracle
- RSA
- SailPoint
- SAP

9. Product Leaders

The second view we provide concerns Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

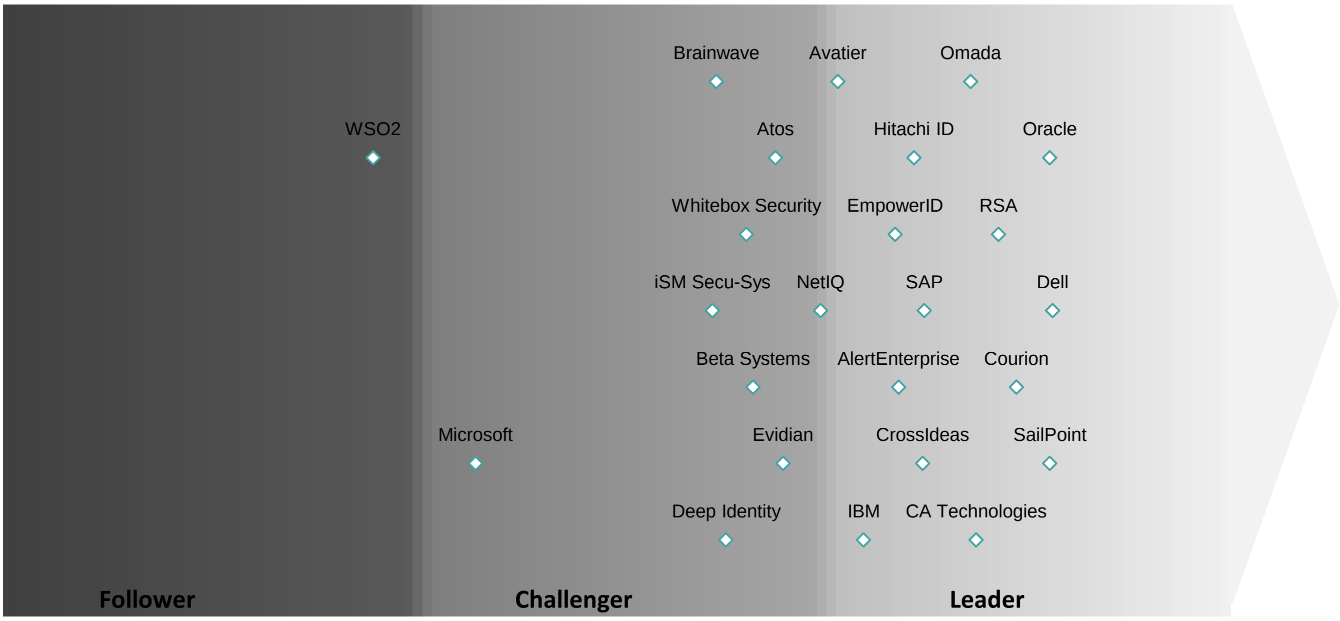

Fig. 7: Product leaders the Access Governance market segment.

When looking at Product Leadership, we again see some of the large vendors in front. Dell, Oracle, and SailPoint are leading, followed by Courion, RSA, CA Technologies, and Omada. SAP is also placed well, even while taking a different approach to Access Governance. However, with their integration into SAP Risk Management and other solutions, they have a strong offering, and not only for SAP environments.

There are a number of other vendors in that Leader segment, including CrossIdeas, an IBM Company, AlertEnterprise, and others. The number of leaders proves that the overall maturity of the Access Governance segment has increased significantly over the past 18 months, since we last did this analysis.

We also see a number of challengers that are in good positions. These include NetIQ, being very close to a leader position with both their integrated capabilities in the NetIQ Identity Manager including their Access Review offering, and their Access Governance Suite, and a number of other vendors. Again, there are a few vendors that are not in a leading position. Microsoft is among these, showing limited innovation in their offering and limited integration. However, for customers of Microsoft FIM, this might be a sufficient solution anyway.

Furthermore, there is WSO2 in the Follower section. As mentioned above, they take a somewhat different approach to Access Governance. They are a great fit for some customer scenarios anyway, but do not cover all standard requirements in the Access Governance market.

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

Product Leaders (in alphabetical order):

- AlertEnterprise
- Avatier
- CA Technologies
- Courion
- CrossIdeas, an IBM Company
- Dell
- EmpowerID
- Hitachi ID
- IBM
- Omada
- Oracle
- RSA
- SailPoint
- SAP

10. Innovation Leaders

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

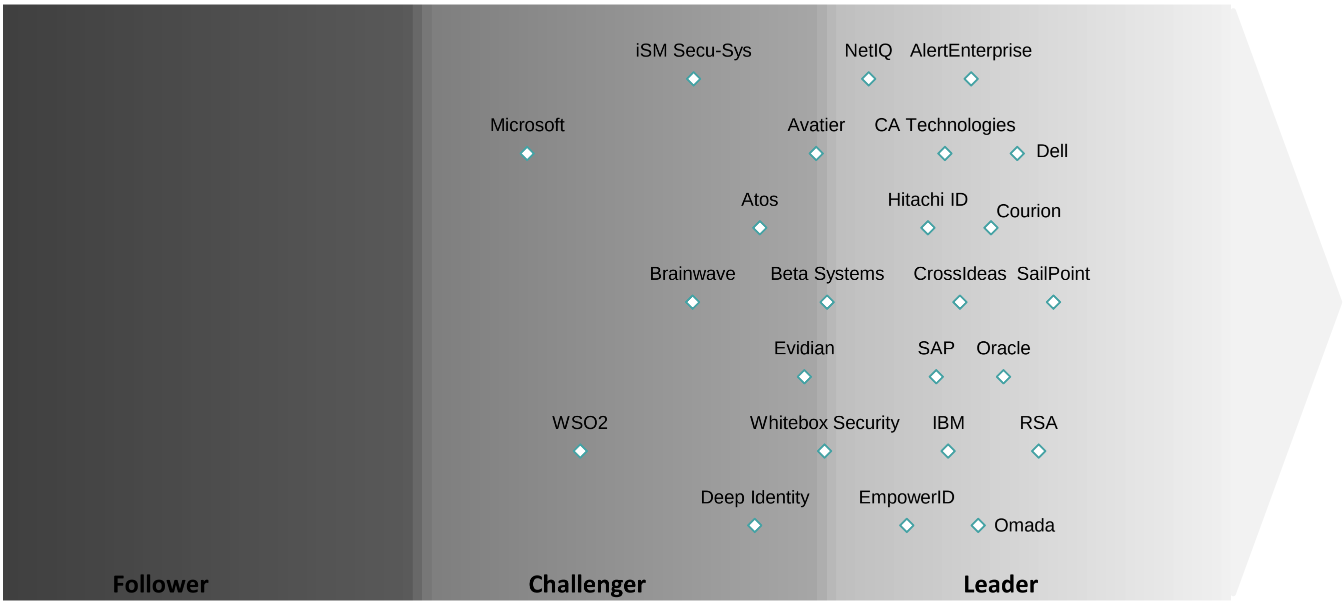

Fig. 8: Innovation leaders in the Access Governance market segment.

When looking at leadership in innovation, we find SailPoint slightly in front. The company has invested heavily into its technology in the past 18 months and executes on its roadmap.

Aside from the large vendors, some other vendors are of specific interest. AlertEnterprise focuses on managing not only standard IT environments but also ICS (Industrial Control Systems) and physical access control solutions, providing a broader approach on Access Governance. Whitebox Security supports a well thought-out approach to real time access risk and threat analytics. Beta Systems is among the innovators in the field of Access Intelligence.

We also see a number of vendors in the Challenger section that are close to becoming a Leader. Avatier shows particular strength in its user interfaces and might be a good complement to existing IAM infrastructures, when smooth interfaces are required. Evidian has its strengths in the integration of a number of capabilities.

From the vendors more to the left, WSO2– as mentioned for the other leadership ratings – takes a different approach but might be a good fit for some use cases. In the case of Microsoft, the rating is caused among other reasons by a lack of some integration capabilities we look for when rating innovation and the fact that the current release mainly was focused on integration of the recently acquired BHOLD assets into the Microsoft FIM product. We expected Microsoft to become more innovative over the next 18 months, but have seen little evolution in their Access Governance capabilities.

Innovation Leaders (in alphabetical order):

- AlertEnterprise
- Beta Systems
- CA Technologies
- Courion
- CrossIdeas, an IBM Company
- Dell
- EmpowerID
- Hitachi ID
- IBM
- NetIQ
- Omada
- Oracle
- RSA
- SailPoint
- SAP
- Whitebox Security

11. 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.

11.1 AlertEnterprise Enterprise Guardian

AlertEnterprise is a relatively young player in the Access Governance market. Executives mainly of Virsa, a company that had been acquired by SAP some years ago, were its founders. It is backed by venture capital. AlertEnterprise takes a somewhat different approach to IAM/IAG with focus on integrating physical, IT, and ICS (Industrial Control System) security.

Strengths/Opportunities	Weaknesses/Threats
● Integration of ICS into IAG approaches. ● Strong focus on enterprise systems and requirements. ● Leading-edge risk management features.	● Still small footprint in the market. ● Small but focused partner ecosystem. ● No support for multi-tenancy.

Table 1: AlertEnterprise Enterprise Guardian major strengths and weaknesses.

AlertEnterprise Guardian consists of a number of different modules, which promise to cover virtually every facet of Identity and Access Management and Governance. Additional modules allow for integration and management into physical security solutions and SCADA environments. The latter is an important feature in times where attacks on such environments are becoming a frequent reality.

In contrast to other products, AlertEnterprise Guardian also moves up the stack towards more advanced risk management and auditing functions, beyond pure access management. It is built on a core platform that provides key features like a policy and rules engine. Overall, the product and its components appear to be well architected, despite the lack of multi-tenancy support that is, from our perspective, a mandatory feature for products newly built from scratch.

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

Table 2: AlertEnterprise Enterprise Guardian rating.

AlertEnterprise, with its integrated approach to the entire breadth of IAM/IAG and beyond, is worth taking into account in product decisions as an alternative to established products. However, maturity of features needs to be carefully reviewed. The small partner ecosystem might become an inhibiting factor in implementing the AlertEnterprise Guardian. However, AlertEnterprise has well selected partners such as SAP.

11.2 Atos DirX Identity

Atos quite a while ago acquired the former Siemens SIS, including the DirX product unit. Atos now provides the DirX products. The core product is DirX Identity, which provides traditional Identity Provisioning but also more advanced and tightly integrated Access Governance capabilities. DirX Audit adds advanced analytical capabilities

Strengths/Opportunities	Weaknesses/Threats
● Very mature offering with strong role management capabilities. ● Long experience in complex and large-scale use cases. ● Provides own managed services.	● Tightly integrated, not well suited for a separate Access Governance layer. ● Requires DirX Audit for advanced analytics. ● Small partner ecosystem besides Atos itself.

Table 3: Atos DirX Identity major strengths and weaknesses.

DirX Identity has a long history of support for Enterprise Role Management as one of the core capabilities of Access Governance. Over time, an increasing number of features for Access Governance have been added. Some of the features for more advanced analytics and auditing are only available through DirX Audit which, however, is tightly integrated.

Atos also has a long experience in large-scale projects and projects in complex environments. Thus, it is well suited for environments that require a mature, sophisticated, and integrated IAM/IAG infrastructure.

Atos, as one of the leading system integrators worldwide provide a strong ecosystem themselves. However, there are few partnerships with system integrators. However, Atos shall be well able to deliver projects on any scale and in virtually any location globally.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 4: Atos DirX Identity rating.

Due to the integrated approach of the product, DirX Identity clearly is targeted at customers who are looking for a “full stack solution” covering both Identity Provisioning and Access Governance. For these environments, the product is of high interest, especially when it comes to large or complex installations.

11.3 Avatier Compliance Auditor

Avatier is one of the vendors in the Access Governance market taking a somewhat different approach in what they call "Assignment Management". This approach goes beyond managing access and focuses on request and management of all types of assets an employee might need, through a simple, intuitive user interface following state-of-the-art user interface paradigms.

Strengths/Opportunities	Weaknesses/Threats
● Simple, intuitive user interfaces. ● Approach of "assignment management" goes beyond access to include assets and service requests as well. ● Integrated platform, providing both Identity Provisioning and Governance features.	● Small but growing partner ecosystem. ● Limited global reach and small customer base outside the U.S. as of now, but growing global partner ecosystem. ● No multi-tenancy.

Table 5: Avatier Compliance Auditor major strengths and weaknesses.

Avatier Compliance Auditor is part of the overall Avatier product suite that focuses on simplifying IAM/IAG. It provides a fair level of functionality designed for on-premise installations, but multi-tenancy support still lacks. When looking at the feature set, the product delivers a good level while not being leading edge from the pure Access Governance and auditor perspective. However, it might well provide what companies really need when it comes to successfully deploying and simplifying Access Governance since its ease-of-use and ease-of-administration are key strong points. Furthermore, it includes user activity monitoring capabilities.

A clear shortcoming of Avatier is the still small but growing partner ecosystem and, therefore, the lack of global reach. This has to be taken into account because it might affect the capability for successfully delivering projects. However, Avatier is working intensively on changing that situation.

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

Table 6: Avatier Compliance Auditor rating.

Avatier Compliance Auditor and the entire Avatier product portfolio are definitely worth a look when deciding about Access Governance, due to the different approach they take. Despite not being the vendor which leads from a pure feature perspective, their offering will be a better fit for some customers due to the pragmatic approach chosen by Avatier. The product might also well complement other vendor's offerings when looking for an intuitive end-user interface.

11.4 Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager

Beta Systems, a German vendor, is among the pioneers in the Identity Provisioning market, including Enterprise Role Management. They provide a good level of integrated Access Governance capabilities in their SAM Enterprise Identity Management Suite and more advanced Identity and Access Intelligence features in their new Garancy Access Intelligence Manager, which is based on standard BI (Business Intelligence) technology.

Strengths/Opportunities	Weaknesses/Threats
• Strong Enterprise Role Management capabilities. • Mature offering with good workflow support. • Innovative approach to Access Intelligence.	• Modules not fully integrated as of now, but integration gradually moving forward. • Small partner ecosystem.

Table 7: Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager major strengths and weaknesses.

Beta Systems has put a lot of effort into moving forward with its established offering, SAM Enterprise Identity Management Suite. Beyond the mature and proven Enterprise Role Management capabilities, Beta Systems has added good workflow functionalities, allowing, for instance, managing recertification campaigns.

They also deliver an additional Access Intelligence product that supports advanced analytics of access risks. The latter product is based on Microsoft SQL Server/BI technology. Even while the two products are not fully integrated yet, they deliver in combination a strong solution for Access Governance. Beta Systems is executing well on further integration, for instance, with significant progress in security management for Garancy Access Intelligence Manager.

For environments which look for integrated solutions providing both Identity Provisioning and Access Governance, the product offerings provide good capabilities, with good support for Access Governance features plus strong features in classical Identity Provisioning and Enterprise Role Management. These are complemented by the additional Access Intelligence capabilities.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 8: Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager rating.

Beta Systems, from our perspective, has to further focus on integration of the different modules. On the other hand, they show quite a bit of innovation. The products are an interesting pick for companies looking for a solution with integrated Identity Provisioning capabilities and which need additional advanced Access Intelligence capabilities.

11.5 Brainwave Identity GRC

Brainwave is a French vendor focusing on a specialized solution for what they call Identity GRC. The product is focused on the advanced analysis of access-related data. Brainwave has partnerships with Identity Provisioning vendors such as ForgeRock to provide comprehensive IAM/IAG solutions.

Strengths/Opportunities	Weaknesses/Threats
• Strong approach to integration of access information from target systems, including cleansing and transformation. • Strong Identity Analytics features with well-thought-out controls and metrics. • Large number of standard reports.	• No support for reconciliation through either integrated provisioning or out-of-the-box integration with provisioning tools. • Relatively small vendor, but some strong partnerships.

Table 9: Brainwave Identity GRC major strengths and weaknesses.

The approach Brainwave has chosen is not uncommon for vendors that are entering the Access Governance market. Brainwave has focused on the collection of access rights and the analytics. They provide very strong capabilities in these areas, allowing customers to efficiently and quickly analyze the status of access rights within the enterprise. This includes the definition of roles and SoD controls.

Brainwave has added workflow capabilities, including support for standard recertification workflows, and is consequently extending the feature set in this area, while continuing to concentrate on the pure-play Access Governance capabilities. Reconciliation and fulfillment is done by integrations to Identity Provisioning solutions, including ForgeRock. Additionally, there are also (custom) integrations to Service Desks/Incident Management systems.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 10: Brainwave Identity GRC rating.

The Brainwave solution has matured significantly over the past few years, while maintaining its strength in Identity and Access Analytics. In this area, the product is very strong. Further functional improvements are planned. Brainwave Identity GRC should be considered by customers looking for an analytics solution which is rapid to deploy and feature-rich, in combination with other vendor’s Identity Provisioning tools.

11.6 CA GovernanceMinder

CA Technologies started into Access Governance with a focus on strong role mining capabilities. Today, CA GovernanceMinder is a comprehensive Access Governance solution. The product is tightly integrated with CA IdentityMinder, the Identity Provisioning product provided by CA Technologies, and follows the same architectural and user interface paradigms. However, it supports other Identity Provisioning products as well.

Strengths/Opportunities	Weaknesses/Threats
• Overall strong feature set with outstanding role mining capabilities. • Direct provisioning capabilities for standalone implementations. • Strong integration with Service Management infrastructures. • Support for User Activity Monitoring and Privilege Management.	• Historically associated with role mining, even though the product has broad capabilities beyond that as of now. • Core focus on integration with CA IdentityMinder, but also support for other Identity Provisioning products.

Table 11: CA GovernanceMinder major strengths and weaknesses.

Based on role mining and analytics technology, CA Technologies has created a product that is tightly integrated with the other CA Technologies offerings in the area of IAM/IAG, both from an architectural and from a user interface perspective. Features are increasingly also supported by the CA SecureCloud offering for cloud-based delivery models. Role mining is still a major strength of the product. However, GovernanceMinder also provides strong support for other requirements in Access Governance.

Among the outstanding features is, for example, the integrated support for user activity monitoring, adding a dynamic view to the static management of access. Also important is the new integration with the Privilege Management products of CA Technologies. Yet another important feature is the tight integration with Service Management tools, especially the ones from CA Technologies itself. While being tightly integrated with CA IdentityMinder, standalone deployments are supported as well.

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

Table 12: CA GovernanceMinder rating.

CA GovernanceMinder is a tool that is definitely worth evaluating, based on its strong feature set and the tight integration with other products from CA Technologies. However, it might also act as a standalone solution on top of existing Identity Provisioning tools. We strongly recommend evaluating the product, focusing especially on the features other than those connected with role mining.

11.7 Courion Access Assurance Suite

Courion has, over the years, become a leader in the IAM/IAG market, consequently enhancing its existing product portfolio and moving up the stack by first adding Access Governance and nowadays Access Intelligence and Access Risk Management features, while still providing a tightly integrated offering.

Strengths/Opportunities	Weaknesses/Threats
• Leading-edge Access Intelligence capabilities. • Well-integrated product portfolio. • Broad support for existing Identity Provisioning solutions.	• Small footprint outside of the North American market. • Consistent approach might not suit all customers' requirements.

Table 13: Courion Access Assurance Suite major strengths and weaknesses.

Courion Access Assurance Suite is a complete offering of capabilities ranging from advanced Access Risk Management and Access Intelligence down to strong integration support with target systems. However, based on the well-integrated but still modular approach, other Identity Provisioning systems can be integrated as well.

From a feature perspective, Courion provides a very strong offering that covers virtually all current standard requirements. However, as with all feature-rich and tightly integrated products, there might be customer situations where this approach does not fully suit the customer's needs, given that customers are looking for more lightweight solutions.

Courion's biggest shortcoming from our perspective is the relatively small partner ecosystem outside the North American market, which limits their ability for successfully delivering projects on a global scale.

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

Table 14: Courion Access Assurance Suite rating.

Courion is among the vendors that should be taken into account when looking for an Access Governance solution. They show innovativeness and provide a feature-rich, established, and well-integrated platform. For customers outside of North America, the support of Courion and its partners in implementation projects need to be carefully reviewed.

11.8 CrossIdeas IDEAS

The Italian vendor CrossIdeas, an IBM Company was recently acquired by IBM. CrossIdeas, an IBM Company has a strong background in role mining and a well-thought-out approach to business-centric Access Governance and Access Risk Management, with tight integration to the business organization and business processes. CrossIdeas, an IBM Company calls this “activity-based modeling”.

Strengths/Opportunities	Weaknesses/Threats
● Sophisticated, business-centric approach to Access Governance. ● Innovative, well-thought-out approach to Access Risk Management. ● Track record of large scale and fast deployments.	● IBM will need to perform full integration into its IBM Security product portfolio.

Table 15: CrossIdeas IDEAS major strengths and weaknesses.

From a conceptual perspective, CrossIdeas, an IBM Company probably is the vendor that has the most sophisticated approach to Access Governance. The concept of activity-based modeling allows building on existing business processes and functions or activities within these for creating a consistent, business-focused access management model. The approach of CrossIdeas, an IBM Company is sustainable to changes in the business organization due to its process focus.

CrossIdeas, an IBM Company also has strong support for SAP environments, for role mining, and for Access Risk Management and innovative analytical capabilities. Its user interfaces are targeted at efficiency in daily use. The company has a small but proven track record for deploying both large scale projects as well as projects with tight deadlines. Being now part of IBM, they have a far better position in the market. However, integration between IDEAS and the IBM Security products has yet to be done, even while IDEAS already provides out-of-the-box integration into IBM Security Identity Manager.

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

Table 16: CrossIdeas IDEAS rating.

Being innovative and based on their conceptual strength, now combined with being part of IBM as a large vendor with a strong ability to execute, we strongly recommend looking at CrossIdeas, an IBM Company in the segment of Access Governance. For a business-centric approach on Access Governance, CrossIdeas, an IBM Company definitely is one of the best picks in the market.

11.9 Deep Identity IACM / IM / FsGA

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

Strengths/Opportunities	Weaknesses/Threats
• Strong capabilities in Access Governance, with a layered approach for Identity Provisioning. • Comprehensive set of compliance features for heterogeneous environments • Strong support for SAP environments.	• Small vendor with limited number of customers. • Certain features such as shopping cart or standard IAM processes can be further improved. • No established partner ecosystem as of now.

Table 17: Deep Identity IACM / IM / FsGA major strengths and weaknesses.

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

On the other hand, we still see a lack of maturity in certain common features. While there are a shopping cart approach and some pre-configured processes, there is still room for optimization. The product also lacks a comprehensive set of APIs, exposing all functions of the products. On the other hand, they have strong support for basic Access Governance capabilities, including strong support for SAP environments.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 18: Deep Identity IACM / IM / FsGA rating.

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

11.10 Dell One Identity Manager

Dell Software has established itself as a leading vendor in the IAM/IAG market place with the Dell One Identity offerings. Dell One Identity Manager and the additional Data Governance edition deliver not only strong Identity Provisioning capabilities but also excel in Access Governance and Data Governance.

Strengths/Opportunities	Weaknesses/Threats
● Leading-edge functionality for Access Governance, including several innovative features. ● Excellent integration within the platform, based on a strong conceptual approach. ● Support for Data Governance, focusing on additional environments like Microsoft SharePoint.	● Limited integration with other Identity Provisioning tools. ● No deployment as virtual appliance. ●

Table 19: Dell One Identity Manager major strengths and weaknesses.

Dell One Identity Manager, including the complementary Data Governance Edition, is among the leading-edge products in the Access Governance market. It provides easy-to-use capabilities for access request management, strong role management capabilities, and other standard features for Access Governance.

Beyond these basic capabilities, there are some interesting features that are unique or, at least, seldom found. The capabilities of not only collecting audit data but also allowing rollbacks to earlier points in time, the simulation features, and the Data Governance capabilities are among these unique features. Another important feature is the integration with Dell Privileged Password Manager that allows request, provision, and recertification of privileged access within the same console.

Dell also has managed to combine a consistent conceptual and architectural approach with sufficient flexibility for customization and interoperability with other existing building blocks of the IT infrastructure.

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

Table 20: Dell One Identity Manager rating.

Dell One Identity Manager should be included when evaluating Access Governance products. It provides a strong feature set, a high degree of flexibility, and it is fairly easy to customize. It is somewhat specific conceptual approach might require some more investigation but is the foundation for some of the rather unique features.

11.11 EmpowerID

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

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

Table 21: EmpowerID major strengths and weaknesses.

Customization of EmpowerID is very flexible, based on the approach chosen by the company. The product is built on a base of Microsoft's .NET platform. It delivers a very broad feature set for Identity and Access Management, going well beyond Access Governance but with tight integration to these core features that includes Dynamic Authorization Management capabilities and integrated Identity Federation features. Overall, support for new technologies and standards like OAuth, OpenID, RESTful APIs, or integrated STS (Secure Token Service) is broad.

However, the product also delivers a broad functionality for basic Access Governance 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	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 22: EmpowerID rating.

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

11.12 Evidian Identity & Access Manager 9

The French vendor Evidian is part of Groupe Bull, one of the leading European IT companies. Evidian has been in the IAM business for many years. Their product, Identity & Access Manager, has been developed over a number of years and provides a good baseline set of features in Access Governance. Evidian focuses on an integrated solution with all major required features. This allows customers implementing an integrated approach to acquire the core IAM requirements.

Strengths/Opportunities	Weaknesses/Threats
● Established product with good feature set in core functionality. ● Excellent integration to Evidian SSO/Access Management solutions. ● Integrated offering with a consistent concept for managing identities and access. ● Integrated support for Dynamic Authorization Management.	● Limited deployment models. ● 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 23: Evidian Identity & Access Manager 9 major strengths and weaknesses.

Evidian has developed a tightly integrated product which covers major aspects of Access Governance. It is focused on providing a consistent set of processes for users. Besides these capabilities, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian. This allows for a broader view of Access Governance than with other solutions.

There is a lack of advanced integration, such as support for ESB (Enterprise Service Bus) concepts or SRM (Service Request Management) integration out-of-the-box. On the other hand the product can use existing external workflow systems. The product allows a quick start for many scenarios, especially in medium-sized businesses. However it might not be the perfect fit for some customer scenarios due to its tight integration of various capabilities.

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

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 24: Evidian Identity & Access Manager 9 rating.

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

11.13 Hitachi ID Identity Manager

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

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

Table 25: Hitachi ID Identity Manager major strengths and weaknesses.

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

The SoD approach implemented ensures that SoD violations and the impact of changes are handled correctly at all layers in a multi-layered role/entitlement model which is not the case with all products in the market. Some specific strengths are the integration with Microsoft SharePoint and Windows Explorer, allowing users to directly request access to resources from these environments. The product also supports managing Active Directory groups. Another important capability is the integration between their Privilege Management and Access Governance capabilities, relying both on the same platform and architecture.

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

Table 26: Hitachi ID Identity Manager rating.

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

11.14 IBM Security Identity Manager ("ISIM")

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

Strengths/Opportunities	Weaknesses/Threats
• Mature product with significant recent enhancements. • Embedded basic Access Governance capabilities. • Significantly improved user interface.	• Multi-tenancy requires significant additional configuration, but partners provide fully multi-tenant implementations. • No support for Access Risk Management.

Table 27: IBM Security Identity Manager ("ISIM") major strengths and weaknesses.

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

However, despite recent enhancements to the Access Governance capabilities, IBM Security Identity Manager is at its core an Identity Provisioning solution with added Access Governance capabilities. However, with the recent acquisition of CrossIdeas, an IBM Company, who are discussed separately in this document, IBM enters an overall leading position in this market segment. Notably, there already is tight integration between IBM Security Identity Manager and CrossIdeas IDEAS.

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

Table 28: IBM Security Identity Manager ("ISIM") rating.

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

11.15 iSM Secu-Sys bi-Cube®

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

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

Table 29: iSM Secu-Sys bi-Cube® major strengths and weaknesses.

A positive aspect of the product clearly is that it delivers a broad set of functionality based on a well-thought-out conceptual approach and methodology. Specific strengths are the role model and, as mentioned above, the standard processes provided. This includes features such as Role Lifecycle processes which still are rarely found in Access Governance solutions.

The product also provides integrated Single Sign-On capabilities and support for strong authentication. On the other hand there is a lack of integration partners and of visibility outside of the local markets.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 30: iSM Secu-Sys bi-Cube® rating.

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

11.16 Microsoft Identity Manager

With the acquisition of the assets of the Dutch vendor BHOLD some time ago, Microsoft made its entry into the Access Governance market. The BHOLD product right now is available as part of the Forefront Identity Manager (FIM) 2010 R2 SP1 offering, combined into a bundle. Microsoft Identity Manager currently is branded Forefront Identity Manager, while the upcoming new release will be formally named Microsoft Identity Manager.

Strengths/Opportunities	Weaknesses/Threats
• Strong footprint of Microsoft FIM in the market. • Advanced Access Governance approach for core features.	• Still a bundle, not a fully integrated product offering. • No support for Access Risk Management and advanced analytics. • No out-of-the-box support for existing Identity Provisioning solutions.

Table 31: Microsoft Identity Manager major strengths and weaknesses.

Microsoft has a distinct position in the IAM market with its FIM product, especially with regard to integration with Active Directory. With the BHOLD product, Microsoft has added capabilities it previously lacked in the area of Access Governance. BHOLD's strengths are in a business-centric approach of modeling roles and managing access based on them, including recertification capabilities.

However, the offering is still more of a bundle of offerings rather than a fully integrated product. Besides that, more advanced features such as Access Risk Management and advanced analytical capabilities are lacking. In contrast to the former BHOLD offering, Microsoft concentrates almost solely on integration with the FIM product. This is, from our perspective, a shortcoming.

A clear strength of Microsoft is its large established customer base for Microsoft FIM and the large partner ecosystem on a global scale.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	neutral

Table 32: Microsoft Identity Manager rating.

The current release of this product suite is mainly interesting to existing customers of Microsoft FIM where it adds Access Governance capabilities. However, it lacks innovative features and is not open to supporting other existing Identity Provisioning solutions. For full stack approaches including Identity Provisioning capabilities, the offering is worth being evaluated, even while Microsoft as of now does not deliver on the potential they show in the Identity and Access Management space.

11.17 NetIQ Access Governance Suite 6.2

NetIQ, being part of The Attachmate Group, is where the IAM-related assets of the former Novell have been integrated. A core product of NetIQ today is the NetIQ Access Governance Suite 6.2 which is based on Access Governance capabilities of SailPoint IdentityIQ, integrated with underlying NetIQ technology. Additionally, NetIQ offers basic Access Governance features as part of its NetIQ Identity Manager And in the Access Review product.

Strengths/Opportunities	Weaknesses/Threats
● Overall strong Access Governance capabilities. ● Out-of-the-box integration with NetIQ Identity Manager. ● Large partner ecosystem on global scale.	● OEM offering, based on the SailPoint IdentityIQ product. ● NetIQ Identity Manager offers only baseline Access Governance capabilities by itself.

Table 33: NetIQ Access Governance Suite 6.2 major strengths and weaknesses.

The NetIQ Access Governance Suite is among the market-leading offerings in that market, providing a rich set of features. The challenge of such an integrated solution always is that it relies on release plans of other vendors, with increasing overlap in functionality. In sum, it provides strong Access Governance capabilities with acceptable integration.

NetIQ has recently added Access Review to their Identity Manager Portfolio to enable organizations to review and certify user access to applications and systems across the enterprise, including those managed by NetIQ Identity Manager as well as those that are not.

Access Review will be the nucleus of future innovations around more intelligent access certifications. Leveraging Access Review, NetIQ plans to utilize several components throughout their product portfolio to deliver intelligent and comprehensive reviews focused on data governance, privileged Identity Management (i.e. Active Directory, Linux/Unix, Mid-range/mainframe, etc.) and access management (cloud, device and traditional access management use cases) review.

NetIQ also provides the ability to deliver access review and authorization to managers using mobile devices. All of these interfaces are designed to make it easier to use on touch-screen mobile devices.

A clear strength of NetIQ is their large partner ecosystem on a global scale and the tight integration of the Access Governance Suite with Novell Sentinel, a SIEM solution.

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

Table 34: NetIQ Access Governance Suite 6.2 rating.

NetIQ Access Governance Suite is a logical pick for existing customers using NetIQ Identity Manager. From a feature perspective, the product is strong. As an alternative, NetIQ delivers their Identity Manager in combination with Access Review as an approach that serves well for many customers..

11.18 Omada Identity Suite

Omada, a Danish vendor, provides the Omada Identity Suite. Omada focuses on adaptable business-centric and collaborative features such as workflows, attestation and advanced access analysis, role management, reporting, governance and compliance and application management. This product is built on a Microsoft platform and offers an out-of-the-box integration with Microsoft Forefront Identity Manager Server (FIM Synchronization Server) for provisioning with backend systems as the common deployment model, but also can rely on ESB (Enterprise Service Bus) integrations, IT Service Management solutions, or other provisioning systems. Furthermore, for extracting information from target systems for Access Governance requirements, the product relies on Microsoft SQL Server Integration Services (SSIS) and packaged collector frameworks for systems such as SAP.

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

Table 35: Omada Identity Suite major strengths and weaknesses.

In the common deployment model, Omada offers a modularized solution, fully based on the Omada web portal that supports the core features. Opting for Omada Identity Suite commonly, but not necessarily, implies opting for Microsoft FIM Sync Server, requiring licensing of both products (but no FIM CALs). However, pure play Access Governance or integration with other Identity Provisioning solutions only require Omada licenses.

The strong support for SAP environments and the added features for workflows, role management, Access Governance such as their “Access Governance Workbench”, and other business-centric functions is a strength. Another interesting option is the ability of Omada to quickly onboard new applications in a structured process.

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

Table 36: Omada Identity Suite rating.

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

11.19 Oracle Identity Governance Suite

Oracle, as part of the 11g R2 release, has put together an Identity Governance Suite that combines existing products, mainly OIM (Oracle Identity Manager) and OIA (Oracle Identity Analytics). As part of 11g R2 Oracle has made massive progress in further integrating these products, both regarding architecture as well as the underlying data models and user interfaces.

Strengths/Opportunities	Weaknesses/Threats
● Market-leading vendor. ● Overall strong feature set in IAG. ● Strong integration with overall Oracle product suite, beyond IAM/IAG – up to the Line-of-Business products.	● Some inflexibility in the role model. ● Tight integration between different modules of the suite.

Table 37: Oracle Identity Governance Suite major strengths and weaknesses.

Oracle 11g R2, despite its name, is in fact a major release for the Oracle IAM/IAG offerings. Oracle has delivered on its roadmap for further integration of different products derived via several acquisitions. As of now, Oracle can claim having a really integrated suite of products, beyond just combining some packages. One of the strengths is integration with the new OPAM product (Oracle Privileged Access Manager). Furthermore Oracle is driving integration with its Line-of-Business products and clearly leads innovation in that space.

For Access Governance, the Oracle Identity Governance Suite is the product of choice. Oracle focuses on an offering targeted on a "full stack approach", combining both Identity Provisioning and Access Governance features. Further integration of the formerly separate offerings is on the roadmap. That leaves little room for more flexible architectures with multiple Identity Provisioning products in place.

When looking at the Oracle offering, this strategy has to be taken into account – there are clear advantages of that tight integration, but also some disadvantages regarding architectural flexibility. Another shortcoming is the somewhat inflexible use of role models which might lead to limitations when trying to implement well-defined, business-driven policies and role models.

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

Table 38: Oracle Identity Governance Suite rating.

Overall, Oracle Identity Governance Suite is one of the market-leading offerings that should be taken into account when looking for an Access Governance solution. It provides an overall strong feature set based on a well-thought-out architecture and a massively improved data model and approach on customization. Besides that, Oracle sparkles with its large partner ecosystem.

11.20 RSA Identity Management and Governance (IMG)

RSA acquired Aveksa, which has commonly been seen as one of the “inventors” and leaders in the Access Governance market, in 2013. This gives them a much stronger position in the market. Beyond pure-play Access Governance, RSA increasingly adds Identity Provisioning capabilities. Furthermore, the product supports EAG (Entitlement and Access Governance) with fine-grained control of target systems.

Strengths/Opportunities	Weaknesses/Threats
• Recognized leader in the Access Governance market. • Innovative features like ESB-based integration to target systems and a highly flexible data model. • Overall strong core Access Governance capabilities.	• Innovative but still relatively new capabilities for Entitlement and Access Governance (EAG). • Lack of advanced analytical capabilities.

Table 39: RSA Identity Management and Governance (IMG) major strengths and weaknesses.

Based on the Aveksa history, the company has a fair number of references and a long history in this market segment. It has a well-established partner ecosystem on a global scale. The product is constantly extended, with new features such as EAG support and role lifecycles being added.

Some features such as advanced analytical capabilities based on standard BI technology are still lacking. We also recommend thoroughly analyzing the usability that might not suit every customer’s requirements for efficient daily use.

Beyond providing the standard features at an overall high level, RSA Aveksa has put emphasis on innovating Access Governance. This especially includes the capability to connect back to the target systems using ESB (Enterprise Service Bus) technology. This allows for reliable, scalable communication.

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

Table 40: RSA Identity Management and Governance (IMG) rating.

Overall, RSA is a clear choice for a vendor to look at in shortlists, given the maturity of their product. However, as with all vendors, there are some areas that might be lacking from the customer’s perspective, thus a thorough analysis and mapping to the specific customer requirements is recommended. On the other hand, RSA is one of the first vendors who massively focuses on EAG for less structured environments like file systems, beyond traditional Access Governance.

11.21 SailPoint IdentityIQ

SailPoint started as a pure-play Access Governance vendor. Over time, SailPoint moved forward towards becoming a vendor of a full IAM/IAG stack. The current SailPoint IdentityIQ product supports both Identity Provisioning and Access Governance. However, it might be used as a standalone Access Governance offering as well.

Strengths/Opportunities	Weaknesses/Threats
● Overall strong Access Governance capabilities. ● Integrated support for Identity Provisioning plus support of existing Identity Provisioning solutions. ● Flexible customization trough configuration.	● Out-of-the box configuration is focused on rapid deployments but can be adopted to more complex, sophisticated requirements in the area of role management and risk management. ● No support for multi-tenancy.

Table 41: SailPoint IdentityIQ major strengths and weaknesses.

SailPoint Identity IQ provides a strong set of Access Governance features plus full-featured Identity Provisioning capabilities. It can be run both as a full, standalone IAM/IAG stack and in combination with existing Identity Provisioning products of other vendors. Other leading-edge features include the support integration with MDM (Mobile Device Management) tools and for Cloud environments.

SailPoint has significantly matured the product and is balancing between easy-to-use standard configurations and the ability to support more complex requirements. Nevertheless, customers with complex environments should carefully review the product capabilities, including depth of connectors to target systems, applicability of the risk management approach, and other features. However, in sum SailPoint clearly is among the leaders in the Access Governance market segment.

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

Table 42: SailPoint IdentityIQ rating.

Without doubt, SailPoint IdentityIQ is among the products that should be included in shortlists and evaluations. The product provides a strong feature set. As with any other product, the features still need review by the customers to analyze whether they fit well to the concepts, the guidelines, and the policies of the customer. However, based on the strong configuration capabilities and the good partner ecosystem, adoption to specific customer needs usually are pretty straightforward.

11.22 SAP Access Control and Identity Analytics

SAP Access Control and the new SAP Identity Analytics are somewhat exotic products in this KuppingerCole Leadership Compass. The products are targeted at providing Access Governance for SAP environments specifically and have their strength in these environments. However, support for heterogeneous environments is better than commonly assumed, in particular when combined with SAP Identity Management.

Strengths/Opportunities	Weaknesses/Threats
• Excellent Access Governance capabilities for SAP environments. • Pre-configured SoD controls for SAP environments. • Tight integration with other products within the SAP GRC portfolio.	• Basic support for heterogeneous environments, extended capabilities in combination with SAP Identity Management. • Product runs on SAP infrastructures, which might be challenging for managing heterogeneous infrastructures.

Table 43: SAP Access Control and Identity Analytics major strengths and weaknesses.

Heterogeneous environments are supported either via some direct connectivity, using the offerings of Greenlight (a SAP partner which extends the reach of SAP GRC to other enterprise systems), or via the web service interfaces which allow interaction with other products in the market, including SAP Identity Management and other products. Overall, support is better than commonly assumed, even while it requires thorough planning.

On the other hand, SAP GRC has outstanding capabilities for managing access in SAP environments, including pre-configured SoD controls and a tight overall integration into SAP environments. Thus, it provides a quick-start especially to customers using SAP mainly in standard configurations. The Identity Analytics product delivers additional capabilities for in-depth analysis and role mining, covering both SAP and heterogeneous environments.

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

Table 44: SAP Access Control and Identity Analytics rating.

From the KuppingerCole perspective, SAP Access Control is a logical choice when it comes to Access Governance for SAP environments. It can serve as a central component also for managing heterogeneous environments, but commonly will require additional components then. Beyond that, the fact that it runs on SAP infrastructures might impose organizational challenges when it comes to managing heterogeneous environments. Nevertheless it is worth evaluating these offerings, particularly in organizations with large SAP infrastructures.

11.23 Whitebox Security WhiteOPS™ Intelligent Access Governance Suite

Whitebox Security is an Israeli vendor that takes a different approach on Access Governance than other vendors. With their WhiteOPS Intelligent Access Governance Suite, Whitebox Security focuses on real-time monitoring and detection of issues in Access Management. Thus, the tool might also complement existing Identity Provisioning and Access Governance offerings.

Strengths/Opportunities	Weaknesses/Threats
● Real-time monitoring of access. ● Strong Entitlement and Access Governance capabilities, providing deep insight into target systems such as Windows file servers. ● Innovative analytical capabilities.	● Somewhat technical user interfaces, not ideally suited for business users. ● Relatively small vendor with limited partner ecosystem.

Table 45: Whitebox Security WhiteOPS™ Intelligent Access Governance Suite major strengths and weaknesses.

Based on pattern-based analytical capabilities, WhiteOPS can provide deep insight into the entitlement structures and current access to systems. This is not only done at the abstract level of business roles, but down to the detailed entitlements in a number of platforms, thus supporting the upcoming Entitlement and Access Governance (EAG) market – sometimes referred to as Data Governance – segment as well.

WhiteOPS allows enforcing SoD policies and real-time detection of violations in a sophisticated way. This requires that customers investi some time in evaluating the product and its specific capabilities.

When comparing WhiteOPS with other Access Governance solutions, the user interfaces appear to be somewhat more technical and not ideally suited to business users, for instance doing access requests or recertification. On the other hand, WhiteOPS with its specific capabilities also might complement existing Access Governance offerings, particularly due to their real-time capabilities and their in-depth features in Entitlement and Access Governance.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 46: Whitebox Security WhiteOPS™ Intelligent Access Governance Suite rating.

WhiteOPS is one of the tools that are worth detailed evaluation, due to the specific approach taken. It provides good baseline support for common Access Governance requirements, but adds a number of other features. The partner ecosystem of Whitebox Security is still quite small, which might cause issues in large scale deployment projects.

11.24 WSO2 Identity Server

WSO2 is a company based in Palo Alto, CA. They provide a platform for connecting businesses, based on SOA (Service Oriented Architecture) concepts. The approach differs from common approaches by not focusing only on IAM/IAG. They deliver a product called Identity Server that provides IAM capabilities, including basic Access Governance features. Due to their concept of targeting more towards connecting businesses with partners and customers, their support for on-premise Access Governance requirements is somewhat limited. However, it might be an interesting choice for customers looking more towards a highly customizable, integrated Access Governance approach for their business process platform.

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

Table 47: WSO2 Identity Server major strengths and weaknesses.

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

However, when looking at core Access Governance capabilities, support is quite low. Most features need to be customized. There are no standard processes deployed. There is no built-in role management capability. A shopping cart for access request management is missing. The WSO2 Identity Server provides a foundation and we find several of these features on the roadmap, but as of now there are various gaps. Customers looking for a strong out-of-the-box feature set will miss a number of features.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 48: WSO2 Identity Server rating.

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

12. Products at a glance

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

12.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 49.

Product	Security	Functionality	Integration	Interoperability	Usability
AlertEnterprise Enterprise Guardian	positive	positive	strong positive	positive	strong positive
Atos DirX Identity	positive	positive	positive	positive	positive
Avatier Compliance Auditor	strong positive	positive	positive	positive	strong positive
Beta Systems SAM Enterprise Identity Management Suite/Garancy Access Intelligence Manager	positive	positive	neutral	positive	positive
Brainwave Identity GRC	positive	positive	positive	neutral	positive
CA GovernanceMinder	strong positive	strong positive	strong positive	positive	strong positive
Courion Access Assurance Suite	strong positive	strong positive	strong positive	positive	strong positive
CrossIdeas IDEAS	strong positive	strong positive	positive	positive	strong positive
Deep Identity IACM / IM / FsGA	positive	positive	positive	positive	positive
Dell One Identity Manager	strong positive	strong positive	strong positive	strong positive	strong positive
EmpowerID	strong positive	positive	positive	positive	strong positive
Evidian Identity & Access Manager 9	strong positive	positive	positive	positive	positive
Hitachi ID Identity Manager	strong positive	strong positive	strong positive	positive	strong positive
IBM Security Identity Manager (“ISIM”)	strong positive	positive	positive	strong positive	positive
iSM Secu-Sys bi-Cube®	strong positive	positive	positive	neutral	positive
Microsoft Identity Manager	positive	positive	neutral	positive	neutral

Product	Security	Functionality	Integration	Interoperability	Usability
NetIQ Access Governance Suite 6.2	strong positive	positive	positive	strong positive	positive
Omada Identity Suite	strong positive	strong positive	strong positive	positive	strong positive
Oracle Identity Governance Suite	strong positive	strong positive	strong positive	strong positive	strong positive
RSA Identity Management and Governance (IMG)	strong positive	strong positive	strong positive	strong positive	strong positive
SailPoint IdentityIQ	strong positive	strong positive	strong positive	strong positive	strong positive
SAP Access Control and Identity Analytics	strong positive	strong positive	strong positive	positive	strong positive
Whitebox Security WhiteOPS™ Intelligent Access Governance Suite	strong positive	positive	positive	positive	positive
WSO2 Identity Server	positive	neutral	neutral	neutral	neutral

Table 49: Comparative overview of the ratings for the product capabilities.

In addition we provide in table 50 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
AlertEnterprise	strong positive	weak	neutral	neutral
Atos	positive	positive	strong positive	neutral
Avatier	positive	neutral	neutral	neutral
Beta Systems	positive	positive	positive	neutral
Brainwave	neutral	weak	neutral	neutral
CA Technologies	positive	positive	strong positive	neutral
Courion	strong positive	neutral	positive	neutral
CrossIdeas, an IBM Company	strong positive	neutral	positive	positive
Deep Identity	positive	critical	weak	weak
Dell	strong positive	positive	positive	positive
EmpowerID	positive	neutral	neutral	neutral

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Evidian	positive	neutral	positive	neutral
Hitachi ID	positive	neutral	positive	neutral
IBM Security	strong positive	strong positive	strong positive	positive
iSM Secu-Sys	positive	weak	neutral	weak
Microsoft	neutral	positive	positive	positive
NetIQ	positive	positive	positive	positive
Omada	strong positive	neutral	positive	positive
Oracle	strong positive	strong positive	strong positive	strong positive
RSA	strong positive	positive	strong positive	positive
SailPoint	strong positive	positive	positive	strong positive
SAP	positive	positive	strong positive	positive
Whitebox	positive	neutral	neutral	neutral
WSO2	neutral	neutral	neutral	positive

Table 50: Comparative overview of the ratings for vendors.

Table 50 requires some additional explanation regarding the “critical” rating.

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

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

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

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

12.2 The Market/Product Matrix

Beyond that, we've compared the position of vendors regarding combinations of our three major areas of analysis, i.e. market leadership, product leadership, and innovation leadership. That analysis provides additional information.

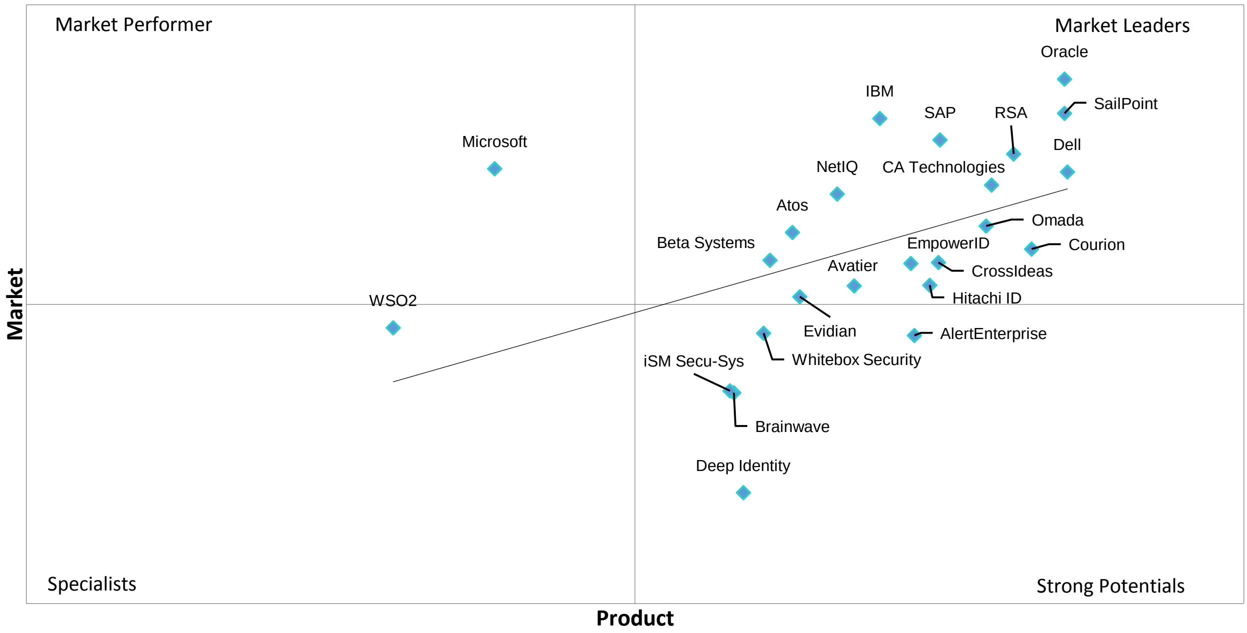

Fig. 9: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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

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

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

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

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

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

The matrix shows a picture that is symptomatic for relatively new market segments. Many vendors still do not have a strong market presence, but already show acceptable strength regarding the product functionality they provide.

The majority of vendors have made it into the Market Leaders segment. A number of them, such as Oracle, IBM, or SAP are over-performing compared to the product capabilities, indicated by a position significantly above the line. Several others such as Evidian, Avatier, Hitachi ID, or CrossIdeas, an IBM Company, made it just to this segment.

More interesting are the other segments. In the Market Performer segment, we only find Microsoft, with a strong position in the market but somewhat limited overall capabilities in Access Governance.

Among the Strong Potentials, we find a number of vendors that potentially can move up into the Market Leaders segment. While Deep Identity still has a long way to go, the others are quite close to that segment.

Finally, there are the Specialists. Here we find WSO2 with its strong platform approach. However, they lack a number of out-of-the-box core features we expect to see in Access Governance products. Nevertheless, they might be a good choice for particular requirements.

12.3 The Product/Innovation Matrix

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

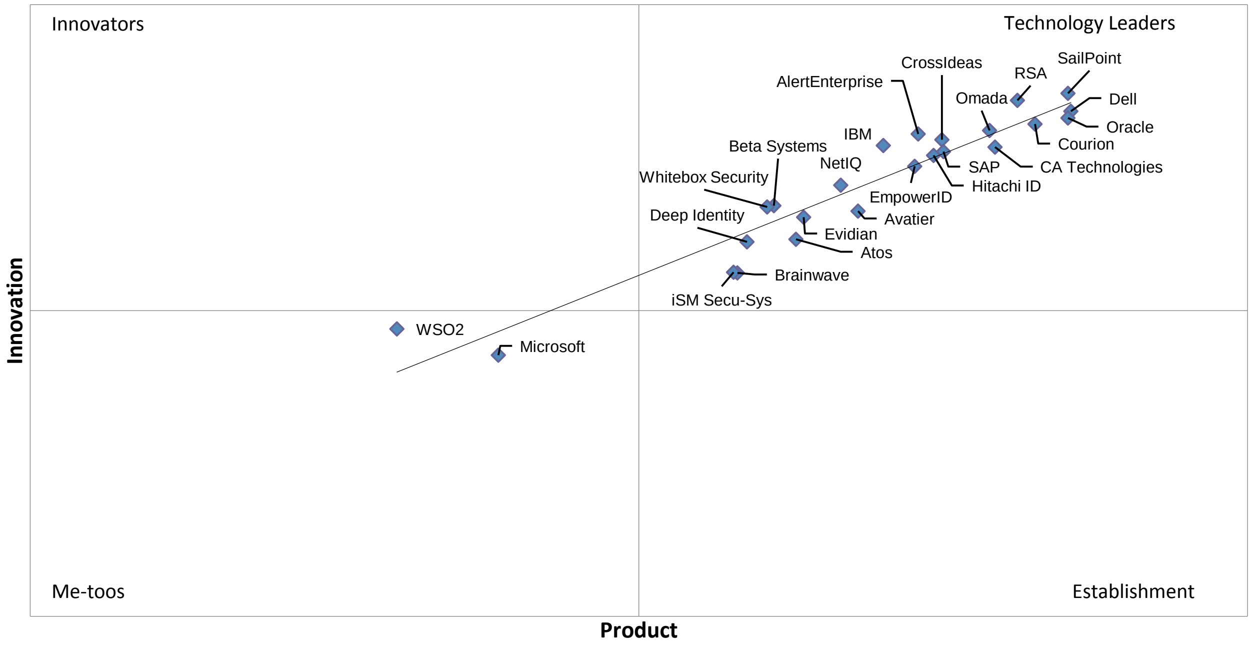

Fig. 10: The Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.

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

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

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

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

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

Here we see an interesting view in that most vendors are placed very close to the line, indicating that there is a tight correlation of overall product rating and innovativeness. Vendors that innovate and continue doing so in the Access Governance market segment also have a quite good product rating.

12.4 The Innovation/Market Matrix

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

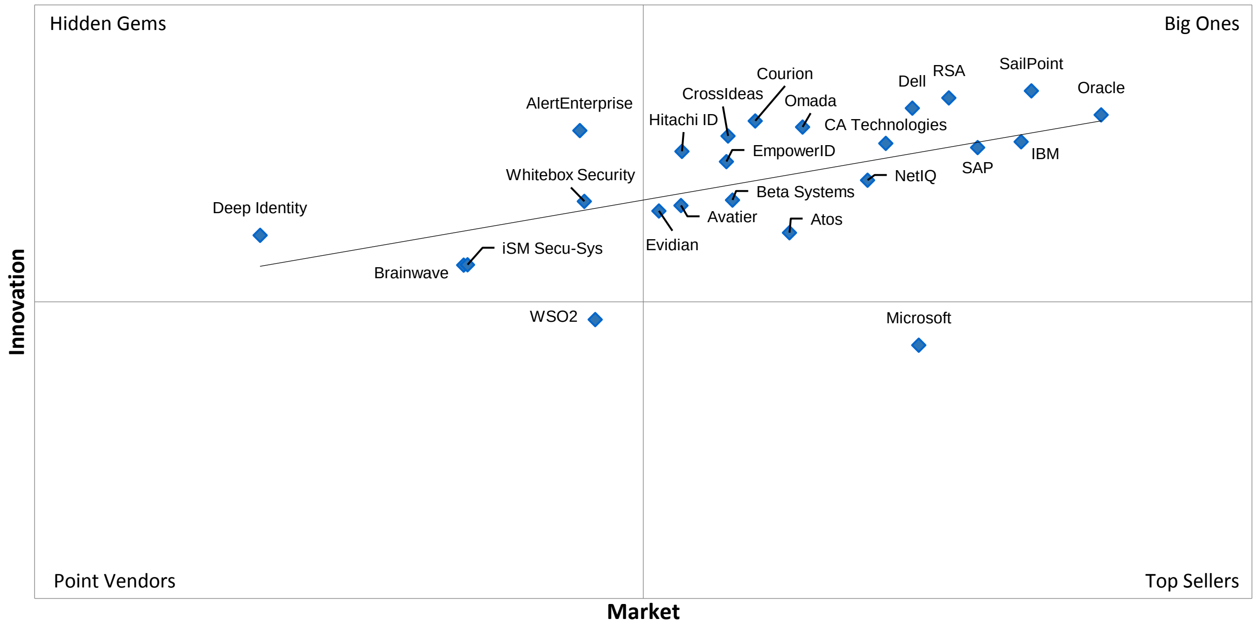

Fig. 11: The Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relative weak position in the Innovation Leadership rating, while vendors above the line show based on their ability to innovate, the biggest potential for improving their market position.

The four segments we have defined here are

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

Top Sellers: In this segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of “customer customers”, i.e. a loyal and powerful group of contacts in the customer organizations.

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

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

Here we see a number of vendors being placed in the Big Ones segment, with some under-performing (below the line) and some over-performing in innovation, when compared to their market position.

In the Top Sellers segment we again see Microsoft as the only vendor, which maps well to the Product/Market view above.

There also in one Point Vendor, which again is WSO2 with its very specific approaches. Again, they are worth a look, because they just might provide what customers are looking for in particular scenarios.

Finally, there are the Hidden Gems. Here we see a number of vendors, all with a good potential for improving their market position over time, given that they are quite innovative today, which gives them a great opportunity for succeeding in sales as well. Compared to the former edition of this Leadership Compass, Avatier and CrossIdeas, an IBM Company, have already made it from the Hidden Gems segment to the Big Ones segment.

13. Overall Leadership

Finally, we've put together the three different ratings for leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 12.

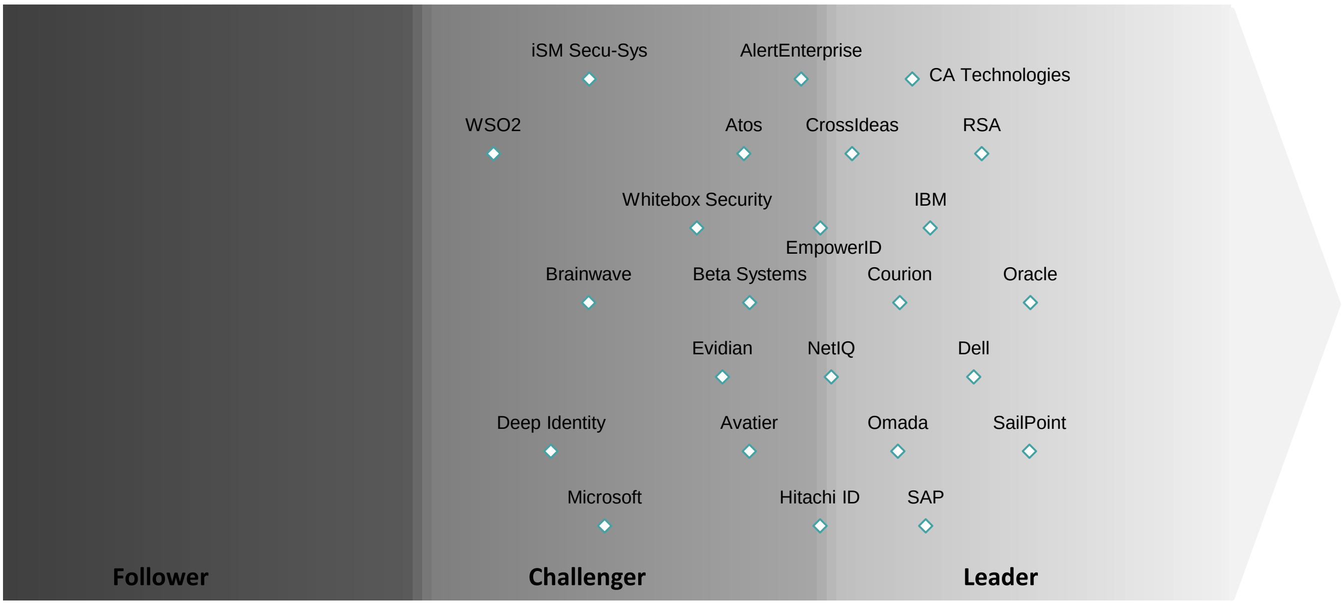

Fig. 12: The Overall Leadership rating for the Access Governance market segment.

When looking at the Overall Leadership, we see a number of vendors in the Leaders segment. Oracle and SailPoint are leading, closely followed by Dell and RSA/Aveksa.

Following these, we see some other big names out of the software industry. CA Technologies, IBM, NetIQ, and SAP all score well in the Overall Leadership rating. This is on one hand caused by their strong market position, but also based on product capabilities and their ability to consequently innovate based on their roadmaps.

We also see Omada and Courion among the leaders in this market segment. Both are quite innovative, with Courion being among the first ones delivering advanced Access Intelligence capabilities as part of their offering and Omada with their new governance workbench. Finally, there is CrossIdeas, an IBM Company, in the Leader segment, which after their recent acquisition by IBM now has a stronger financial background, in addition to their long-standing strength in product capabilities and innovation.

There are a number of vendors in the Challenger segment that are very close to moving into the Leader segment. EmpowerID, Hitachi ID, AlertEnterprise, and NetIQ all are candidates for becoming Leaders in the next edition of this Leadership Compass. Aside from them, several other vendors are placed in good positions in this rating.

Only a few vendors fall somewhat behind. However, all of them have their particular strengths. While Deep Identity is innovative, they have still a very limited market presence. WSO2 takes a fundamentally different approach on IAM/IAG, based on a business process integration platform. As of now, the built-in feature set is somewhat limited, but flexibility for customization and scalability are strong, which makes them an interesting pick for specific use cases.

Again: Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the features provided by the vendor's products is mandatory.

Overall Leaders are (in alphabetical order):

- CA Technologies
- Courion
- CrossIdeas, an IBM Company
- Dell
- IBM
- Omada
- Oracle
- RSA
- SailPoint
- SAP

14. Vendors and Market Segments to watch

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

14.1 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.

14.2 Bay31

Bay31 is a small company headquartered in Switzerland that focuses on role management and access risk analytics. Their Role Designer product comes in two variants, with the Role Designer for SAP specifically designed for SAP environments, as the name indicates.

With that focus on role analytics, access risk analytics, and role design, Bay31 does not yet provide a fully comprehensive solution for Access Governance. Various capabilities, including key capabilities such as access recertification, are still missing.

Bay31 Role Designer is a point solution with particular strength in its area of role mining, analytics, and design. While a number of other vendors also show strengths in these areas, Bay31 is the only one offering a stand-alone solution for these areas. That can make them quite interesting for customers using other IAM/IAG solution that lack sufficient support for such requirements. However, Bay31 Role Designer is not yet a fully-fledged Access Governance solution.

Aside from the limited functional breadth, Bay31 as a relatively young vendor has only a limited footprint in the market and a rather small partner ecosystem. However, their specific strength in some areas makes them a quite interesting addition to both vendor and system integrator portfolios.

14.3 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.

14.4 E-Trust

E-Trust is an IAM/IAG vendor headquartered in Brazil that delivers its own IAM/IAG 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.

14.5 Fischer International

Fischer International this time did not answer the questionnaire for this KuppingerCole Leadership Compass and thus is not included in the document. Based on a comprehensive IAM/IAG platform being available as both on-premise product and Cloud service, Fischer delivers a solution which is flexible in configuration and overall feature-rich. Fischer International is an alternative to the vendors covered in this document. They have a very limited footprint outside of North America.

14.6 Indeed-Id

Indeed-Id is another Russian software vendor in the IAM market. While their primary focus is on Single Sign-On, they also offer limited capabilities for core IAM/IAG features. However, they clearly are more relevant for Single Sign-On requirements, including strong authentication on mobile devices.

14.7 OpenIAM

OpenIAM provides an open source identity stack that also is available in an appliance form factor. They provide a number of features such as access request management and audit features, but cover also various other areas of IAM/IAG such as Identity Federation. In most areas, depth of capabilities is limited but can be extended by customization. OpenIAM is particularly interesting for customers looking for a simple-to-deploy appliance for IAM.

14.8 SmartAIM

SmartAIM is a company delivering a number of IAM/IAG 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.

14.9 Tools4ever

Tools4ever provides an IAM solution, particularly focused on medium-sized businesses. While their provisioning capabilities are at a good baseline level, with a broad set of connectors, Access Governance features are not as elaborated. Again, they might take a more prominent role in this market over time.

Besides these vendors which are close to the Access Governance market segment or even part of it but not covered in this KuppingerCole Leadership Compass for various reasons, there are some related market segments of relevance when looking at Access Governance:

Identity Provisioning

As described in this document, Access Governance is tightly related to Identity Provisioning. Many vendors either provide both Access Governance and Identity Provisioning or fully integrated solutions. Thus we recommend looking at both segments when defining the future strategy for these core areas of IAM or selecting Access Governance vendors. More information on the Identity Provisioning market is delivered in the KuppingerCole Leadership Compass Identity Provisioning (#70,151).[6]

Entitlement and Access Governance (EAG)

An emerging market segment is called Entitlement and Access Governance[7]. It is related to the Access Governance segment but focuses more on unstructured data and, within that segment, specifically on file servers and increasingly on Microsoft SharePoint environments. Data Governance supports features like defining data ownership and processes for requesting and granting access to file shares and other resources.

Some of the vendors in the Access Governance market such as Dell and RSA deliver integrated support for Data Governance in their products. Others like Omada have specific solutions for SharePoint management.

Besides these vendors, there are several players out there focusing mainly or only on Data Governance, like Blackbird (recently acquired by BeyondTrust), Protected Networks, and Varonis. Due to its high importance, this segment will be covered in a separate KuppingerCole Leadership Compass document at a later point in time.

IT Risk Management

Some vendors focus specifically on IT Risk Management, which includes the management of access risks and SoDs across systems. Thus there is some overlap to Access Governance. Especially for Access Governance projects with a strong focus on high-level IT Risk Management, it is worthwhile to consider these vendors. Examples include Agiliance, but also SAP with its Risk Management product. SAP’s strength lies in their support not only for Access Governance but also IT Risk Management and Process Risk Management within an integrated solution.

IT GRC (Governance, Risk Management & Compliance)

Finally there are several vendors for IT GRC. Some of these vendors support controls which can be used to implement an Access Governance solution. However, such vendors typically are focused more on manual controls and lack support for automated controls and technical integration. In most cases, these solutions are more suitable in combination with Access Governance tools. There are a few out-of-the-box integrations, such as the one between MetricStream and CrossIdeas, an IBM Company.

[6] http://www.kuppingercole.com/report/leadershipcompidentityprovisioning7015115102012

[7] http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214

Access Governance – Platform-specific Solutions

Besides SAP GRC, there are several additional platform-specific solutions for Access Governance, mainly in relation to core business applications like SAP and Oracle Applications. Due to their specific nature, these are not covered within this KuppingerCole Leadership on Access Governance which looks at solutions that support heterogeneous environments. The exception is SAP Access Control itself which is focused on SAP environments but provides some support for other environments as well, plus interfaces and integrations with other systems. There also will follow a separate Leadership Compass on this market segment.

15. Copyright

The Future of Information Security – Today

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

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

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

Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

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