KuppingerCole ANALYSTS

Access Control Tools for SAP Environments

Martin Kuppinger

July 27, 2023

This report provides an overview of the market for Access Control Tools for business application environments that are centered around SAP solutions, including traditional SAP ECC environments. The main focus is on these environments, including SAP S/4HANA, SAP S/4HANA Cloud and other SAP cloud applications, with a limited focus on support for other Line of Business (LoB) applications. We examine the market segment, vendors, product functionality, relative market share, and innovative approaches to providing solutions that increase security in these business application environments primarily for SAP, by restricting access, controlling break-glass access, and related capabilities.

Contents

Contents 2
Figures 3
Introduction / Executive Summary 4
Highlights 4
Market Segment 5
Delivery Models 5
Required Capabilities 7
Leadership 9
Overall Leadership 9
Product Leadership 11
Innovation Leadership 13
Market Leadership 15
Correlated View 17
The Market/Product Matrix 18
The Product/Innovation Matrix 19
The Innovation/Market Matrix 20
Products and Vendors at a Glance 22
Product/Vendor evaluation 24
Spider graphs 24
ComplianceNow – by Nagarro 25
EmpowerID – EmpowerID Platform 28
One Identity – One Identity Manager 31
Pathlock – Pathlock Cloud / Pathlock Native 34
SailPoint – Security Identity Platform 38
SAP – Access Control / Identity Access Governance (IAG) 42

Saviynt – Enterprise Identity Cloud 45
Sivis – Enterprise Security 48
Soterion – Access Control Suite 51
Wikima4 – Mesaforte Compliance Suite 55
Xiting – Xiting Authorization Management Suite (XAMS) 58
Vendors to Watch 61
Methodology 64
Types of Leadership 64
Product rating 65
Vendor rating 66
Rating scale for products and vendors 67
Inclusion and exclusion of vendors 68

Figures

Figure 1: In this market segment, we find a range of solutions with varying scope and different deployment models. 7
Figure 2: Overall Leaders for Access Control Solutions for SAP Environments (graphic only has a vertical axis) 9
Figure 3: Product Leaders for Access Control Tools for SAP Environments. 11
Figure 4: Innovation Leaders for Access Control Solutions for SAP Environments. 13
Figure 5: Market Leaders for Access Controls Solutions for SAP Environments. 15
Figure 6: The Market/Product matrix for Access Control Solutions for SAP Environments. 18
Figure 7: The Product/Innovation matrix for Access Control Tools for SAP Environments. 19
Figure 8: The Innovation/Market matrix for Access Control Tools for SAP Environments. 21
Figure 9: Nagarro ComplianceNow's additional ratings 27
Figure 10: EmpowerIDs additional ratings 30
Figure 11: One Identity's additional ratings 33
Figure 12: Pathlock's additional ratings 37
Figure 13: SailPoint's additional ratings 41
Figure 14: SAP's additional ratings 44
Figure 15: Saviynt's additional ratings 47
Figure 16: Sivis' additional ratings 50

Figure 17: Soterion's additional ratings 54
Figure 18: Wikima4's additional ratings 57
Figure 19: Xiting's additional ratings 60

Introduction / Executive Summary

For many enterprises, SAP systems are an essential part of their corporate IT infrastructure. Critical business information is stored within ERP systems, and the favored source for employee data is the SAP HR system. Business processes are implemented through portal solutions relying on SAP infrastructure. Data is held in SAP HANA; the migration to S/4HANA is ongoing, and highly individualized functionality is coded right into the existing standard SAP modules by using ABAP or Java.

Although there are many other systems in place which also contain critical information, many businesses still rely on the availability of well-designed and well-protected SAP Systems. Traditionally, SAP systems are a major focus area for internal and external auditors. For the successful implementation of adequate controls, it is essential that all existing SAP systems are covered by an effective solution for managing risks, and within that for managing access control and SoD controls and implementing adequate Access Governance.

> SAP solutions remain at the core of the LoB infrastructure of many organizations. Managing access entitlements including roles, but also SoD (Segregation of Duties) rules, firefighter access, and other aspects around identity, access, and security is essential for protecting these business-critical applications.

Many critical business systems are following the trend of shifting to the cloud, using either solutions provided by SAP such as SuccessFactors or Ariba, or to other vendors' solutions, SAP systems remain at the core of the LoB (Line of Business) application infrastructure of many organizations. While the scope for managing access controls is expanding beyond the traditional ABAP systems and even beyond SAP, these systems are of high criticality for many organizations.

This Leadership Compass focuses on the support for the SAP environment, while a separate document takes a broader perspective across a heterogeneous LoB landscape.

Highlights

- While the customer requirements for access control solutions for their business applications are expanding in the context of the journey towards SaaS services, many organizations still build their LoB infrastructure primarily on traditional and modern SAP solutions, operated both on premises and in the cloud
- Customers that continue to focus on their traditional SAP environments, with the SAP department being the buyer, commonly look for deep integration into these environments and familiar user interfaces

- In this market segment, we find several vendors with a high degree of specialization in SAP environments, frequently delivering both software and services
- Aside from some large players such as SAP itself and Pathlock, several smaller vendors primarily serve their local markets
- Some of the vendors from the IAG (Identity and Access Governance) space also provide deep support for SAP environments, but in most cases with lesser coverage for extended capabilities such as roll-out support and other features that are provided by the SAP-focused vendors
- With the acquisition of various vendors by Pathlock (formerly Greenlight GRC), a large competitor to SAP has emerged in the market
- Overall Leaders are (in alphabetical order) Pathlock, SailPoint, SAP, and Saviynt
- Product Leaders are (in alphabetical order) Pathlock, SailPoint, SAP, Saviynt, and Xiting
- Innovation Leaders are (in alphabetical order) Pathlock, SailPoint, SAP, Saviynt, and Soterion
- Market Leaders are (in alphabetical order) Pathlock, SailPoint, SAP, and Saviynt

Market Segment

In this KuppingerCole Leadership Compass, we analyze solutions that support managing access controls specifically for SAP environments, with a limited focus on support for other vendor's business applications or LoBs (Line of Business applications). The main focus is on delivering the depth for implementing management and controls across SAP environments.

Deployment models for both the managed services and the solutions is changing, with more SaaS services to manage, and deployment in different ways – as ABAP solution, with SAP Fiori user interface, or separately from SAP as web applications or, becoming the new standard, as SaaS services.

The core of functionality remains in the management of access controls including critical entitlements and SoD conflicts in SAP and other LoB environments. However, solutions frequently also cover additional features such as break-glass access management (firefighter, emergency access), user lifecycle management, role optimization, and more. In this Leadership Compass, we put a strong focus on both the core capabilities and add in features.

The solutions span from those which target SAP core systems to comprehensive suites covering a broad range of capabilities around access control and security for a heterogeneous set of LoB solutions, including SAP solutions.

Delivery Models

We did not restrict our analysis in this Leadership Compass regarding the delivery models. There is a broad range of implementation models, from pure-play ABAP solutions to solutions which have a Fiori app added to full SaaS services, while some SaaS services

integrate with ABAP modules back to SAP. Although the trend is towards SaaS solutions, we covered all types of deployment models in this report.

The focus of our rating is on the amount of flexibility available for customers. There are advantages and disadvantages to all approaches. A full integration as ABAP solution is great for supporting the traditional SAP environments, but reaches its limit when supporting other vendor's SaaS solutions. Although the user interface might be favored by experienced SAP users, many users – including experienced SAP users –prefer a modern user experience.

Fiori or SAP UI5 as a user interface is something that someone who is familiar with SAP environments might prefer, while others might favor another web UI, this is not limited to the Fiori UX (user experience) paradigms.

Solutions that run separately from SAP environments are better suited for supporting SaaS services and applications beyond SAP solutions. Some of these also excel in user experience, based on modern UIs with high usability.

The delivery model that is best suited to each individual customer's needs depends on the current and future scope of applications to manage, and the features in focus. However, there is a clear trend away from traditional ABAP, towards modern user experience, supporting the increasingly heterogeneous business application infrastructure, and being delivered as SaaS.

Factually, solutions can be grouped into four types:

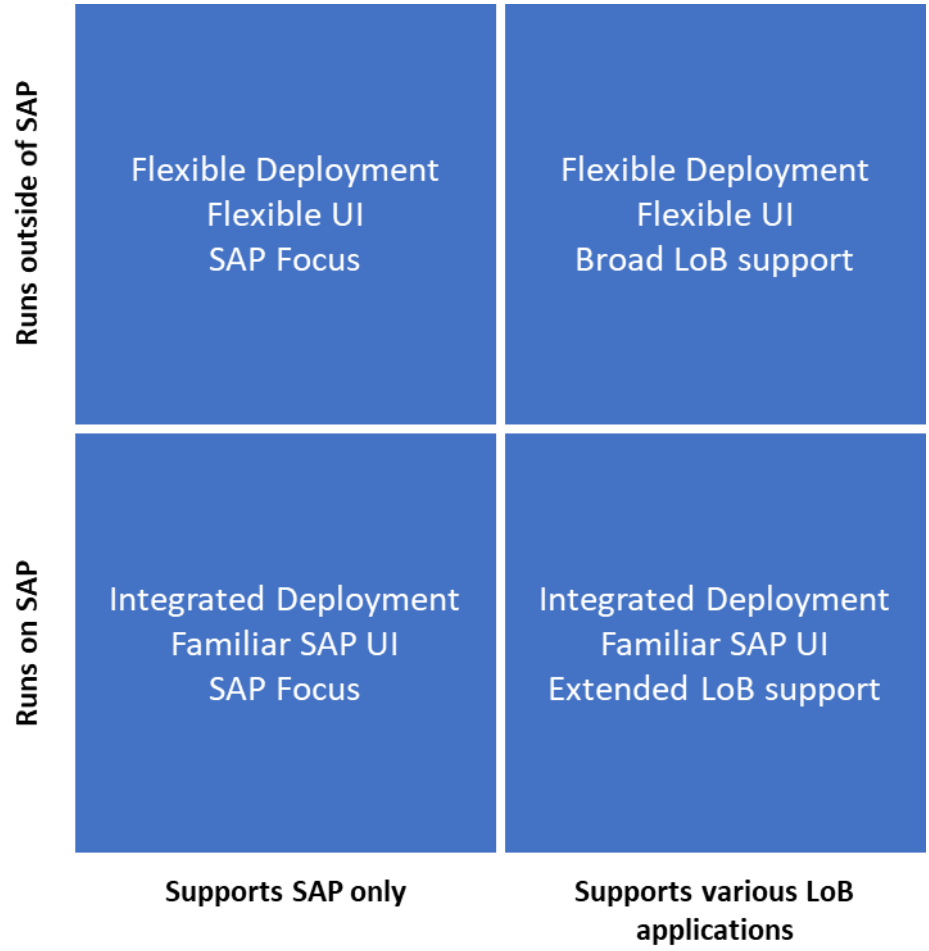


Figure 1: In this market segment, we find a range of solutions with varying scope and different deployment models.

Solutions can run in the SAP ecosystem or outside of it, the latter commonly being deployed as SaaS. They can focus on SAP only or extend beyond that ecosystem. The number of vendors that stick to an SAP-only approach has decreased significantly since the previous edition, with most vendors including SAP adding interfaces and increasingly adding support for non-SAP LoB solutions.

Required Capabilities

Due to the variety of capabilities provided by the solutions which are currently available and with respect to the changing environments, there is a broad set of capabilities we are looking for, split into baseline capabilities and advanced capabilities. The baseline capabilities dominate the rating, with other capabilities being additional to this.

The exception is broad support for systems, beyond the traditional SAP Business Suite. The breadth of support for LoB applications beyond the traditional SAP scope has a high impact on our rating, given that we see increasing demands and strategic changes within business system environments.

Baseline capabilities we are looking for:

- Flexible deployment models, including as-a-service deployments
- Support for all major SAP systems and versions
- Analysis of the current status of entitlements/roles at all levels, from transactions to business roles, including Access Risk Analysis
- Role and entitlement management
- Access management, i.e., assignment of entitlements (Access Management)
- SAP super-user management and privileged user management for other LoB solutions (see below)
- Identity Lifecycle Management for the target applications, i.e. creating and managing accounts (User Management)
- SAP Firefighter capabilities, and ideally emergency access management for other LoB applications (see below)
- SoD controls management, check, and enforcement across all supported systems
- Central Reporting and Dashboarding
- Access Review support

Advanced capabilities we are interested in seeing as part of these products:

- Support for hybrid deployment models or pure SaaS deployment
- Automated role optimization
- Support for non-ABAP systems
- Support for SAP cloud solutions such as SAP Hybris, SAP Customer Cloud, Concur, Ariba, SuccessFactors, etc.
- Support for non-SAP business applications, both on premises and SaaS, including Enterprise Service Management solutions such as ServiceNow and Jira
- Go-Life support for SAP systems (specifically S/4HANA) with focus on entitlements, i.e. transferring entitlements
- Password Self Service and Single Sign-On
- Integration capabilities to cross-platform IGA solutions (covering non-SAP-systems for both Identity Lifecycle Management and Access Governance)
- Auditor support and run-time execution for audits
- Support for specifics of platforms such as SAP BI, S/4HANA, and SAP HANA In Memory Database
- Super user management for other business applications
- Firefighter capabilities for other business applications
- System hardening capabilities
- Capabilities for managing exports and transfers of critical data, such as HR data

Inclusion criteria:

- Solutions covering all or most of the baseline capabilities
- All deployment models – solutions can run on premises as ABAP applications, on premises in other models, hybrid, or as SaaS applications
- Solutions covering only SAP environments

Exclusion criteria:

- Solutions that only cover singular baseline capabilities such as Firefighter access for SAP only
- Solutions that are targeted on read-only analysis of entitlements and risk analysis for auditors, but don't support active management of users and entitlements
- Solutions that don't support the entire depth of entitlement/roles at all levels, i.e. solutions that e.g. only can assign users to SAP business roles but can't manage entitlements of such roles

We reached out to many vendors in order to provide a comprehensive overview of the current state of the market. Picking the right vendor will always depend on your specific requirements and the current and future landscape that must be managed.

Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

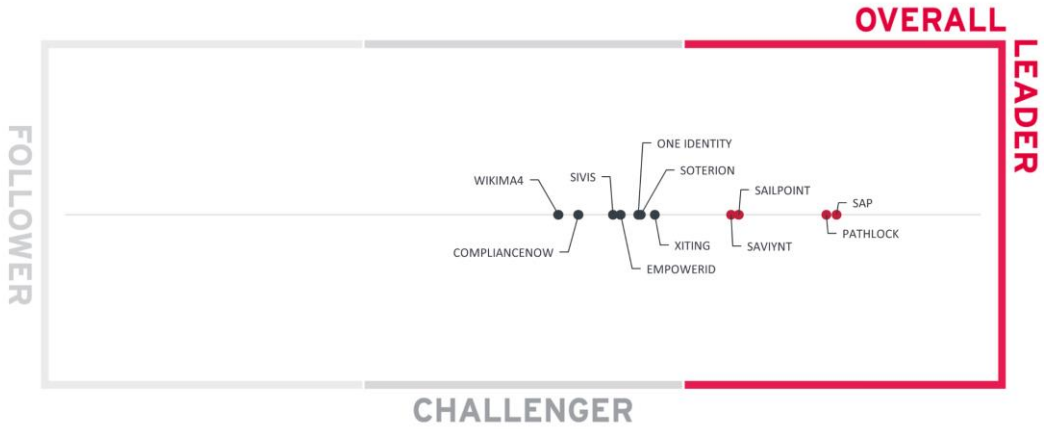


Figure 2: Overall Leaders for Access Control Solutions for SAP Environments (graphic only has a vertical axis).

The Overall Leadership chart is divided into three groups of vendors. To the right and leading, we see SAP and Pathlock being close to each other. SAP benefits from its strong

market position, customer base, and partner ecosystem, also offering proven solutions, while Pathlock comes with a feature-rich set of solutions after integrating the various acquisitions the vendor has made in this market segment.

Following them is SailPoint, which has strengthened its position with the ERP Maestro acquisition, and Saviynt, which always had a strong focus on supporting SAP environments. These two vendors add to the Leaders segment.

In the Challenger segment, we find both IGA vendors with strong SAP support and various vendors specializing in supporting SAP environments. Amongst the latter, we find – in alphabetical order – ComplianceNow (part of Nagarro group), Sivis, Soterion, Wikima4. The two IGA vendors that participated and come with very good support for SAP environments are EmpowerId and One Identity.

Overall Leaders are (in alphabetical order):

- Pathlock
- SailPoint
- SAP
- Saviynt

Product Leadership

Product Leadership is the first specific category examined below. This view is based on the analysis of service features and the overall capabilities of the various services. **Product Leadership** is where we examine the functional strength and completeness of services.

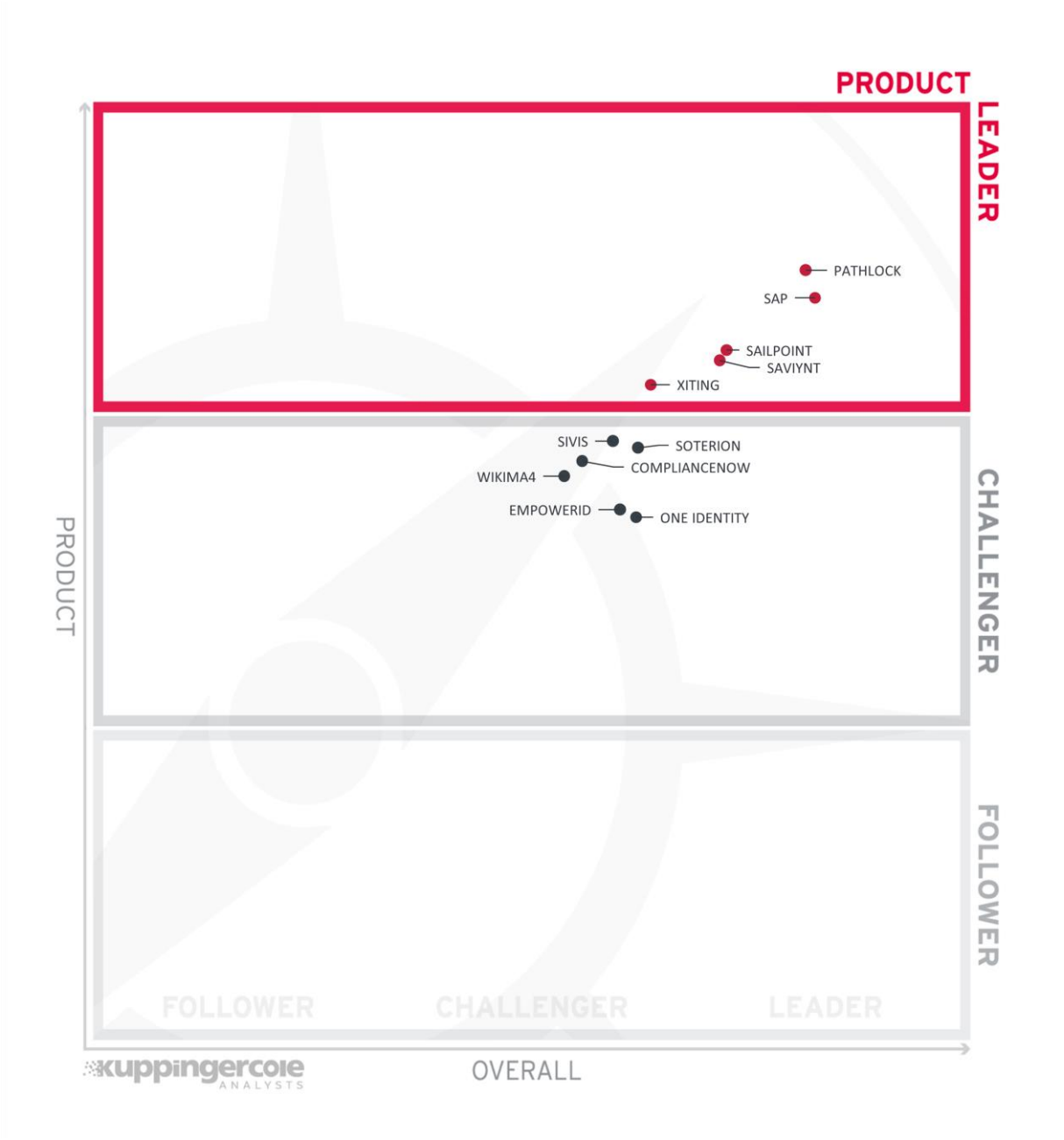


Figure 3: Product Leaders for Access Control Tools for SAP Environments.

Due to various acquisitions, Pathlock has a product portfolio in place that is very feature rich. Despite the fact that there is a SaaS and an on-premises version, customers will need to make a decision about which product(s) to use – as with SAP, which offers two products – Pathlock excels with the overall capabilities on offer. SAP is close to Pathlock, continuously expanding and modernizing their product portfolio.

SailPoint comes with an interesting combination of SAP-specific capabilities through the ERP Maestro acquisition and strong overall IGA capabilities from their traditional platforms, but also adding more and more other capabilities such as AI-/ML-based analytics. This makes them a strong contender in this market, head-to-head to Saviynt. Xiting, a SAP specialist, has also entered the Leaders segment with their deep support for SAP-specific capabilities.

The Challenger segment contains, at the top, the four other SAP specialists. These are (in alphabetical order) ComplianceNow, Sivis, Soterion, and Wikima4. They are positioned close to each other, with different strengths. ComplianceNow excels by its deep integration in SAP ECC environments, while Soterion comes with innovative business process support and Wikima4 with a broad set of GRC related capabilities.

Closely following them we find EmpowerID and One Identity, which also come with good support for SAP-focused environments, but specifically lack the breadth of added features for SAP environments such as system hardening, go-live support etc. that are common to the solutions provided by the specialists.

Product Leaders (in alphabetical order):

- Pathlock
- SailPoint
- SAP
- Saviynt
- Xiting

Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet ever evolving and emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

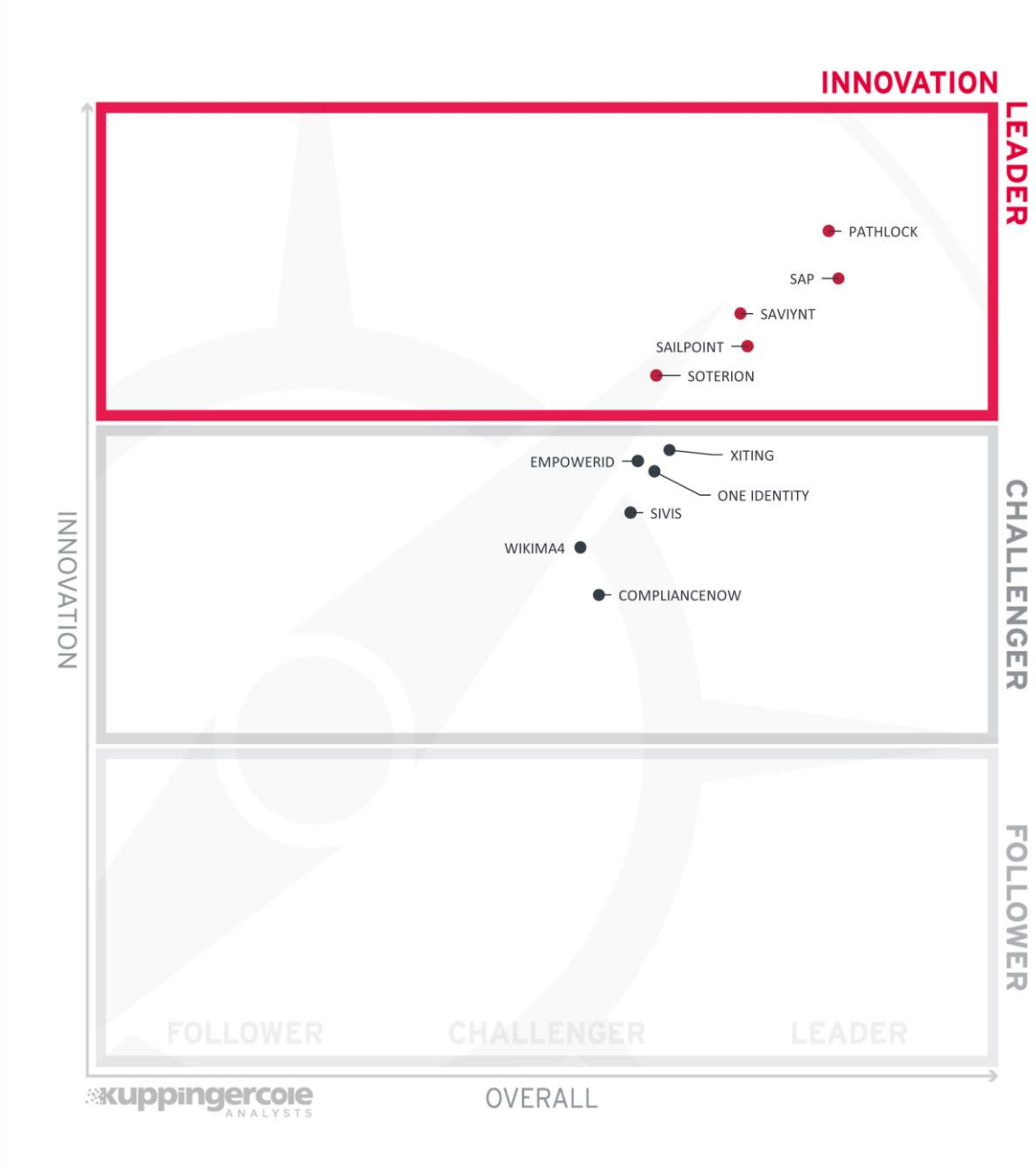


Figure 4: Innovation Leaders for Access Control Solutions for SAP Environments.

In the Leaders segment, we again find Pathlock ahead of SAP, benefiting from the various innovative capabilities that have been brought in through the acquisitions. SAP is also

expanding their capabilities. Saviynt and SailPoint are following closely, adding new features, and benefiting from their innovativeness in the broader IGA market segment. Soterion also has made it into the Leaders segment, with their innovative capabilities around business process to risk mapping.

EmpowerId and One Identity are leading in the Challenger segment, benefiting from their underlying broad IGA platforms and the innovations they add there. Xiting and Sivis are close to them. Wikima4 has some strong innovations in their product portfolio, but not across the entire portfolio. ComplianceNow, on the other hand, is a rock-solid solution for customers that are focusing on traditional SAP environments.

Innovation Leaders (in alphabetical order):

- Pathlock
- SailPoint
- SAP
- Saviynt
- Soterion

Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

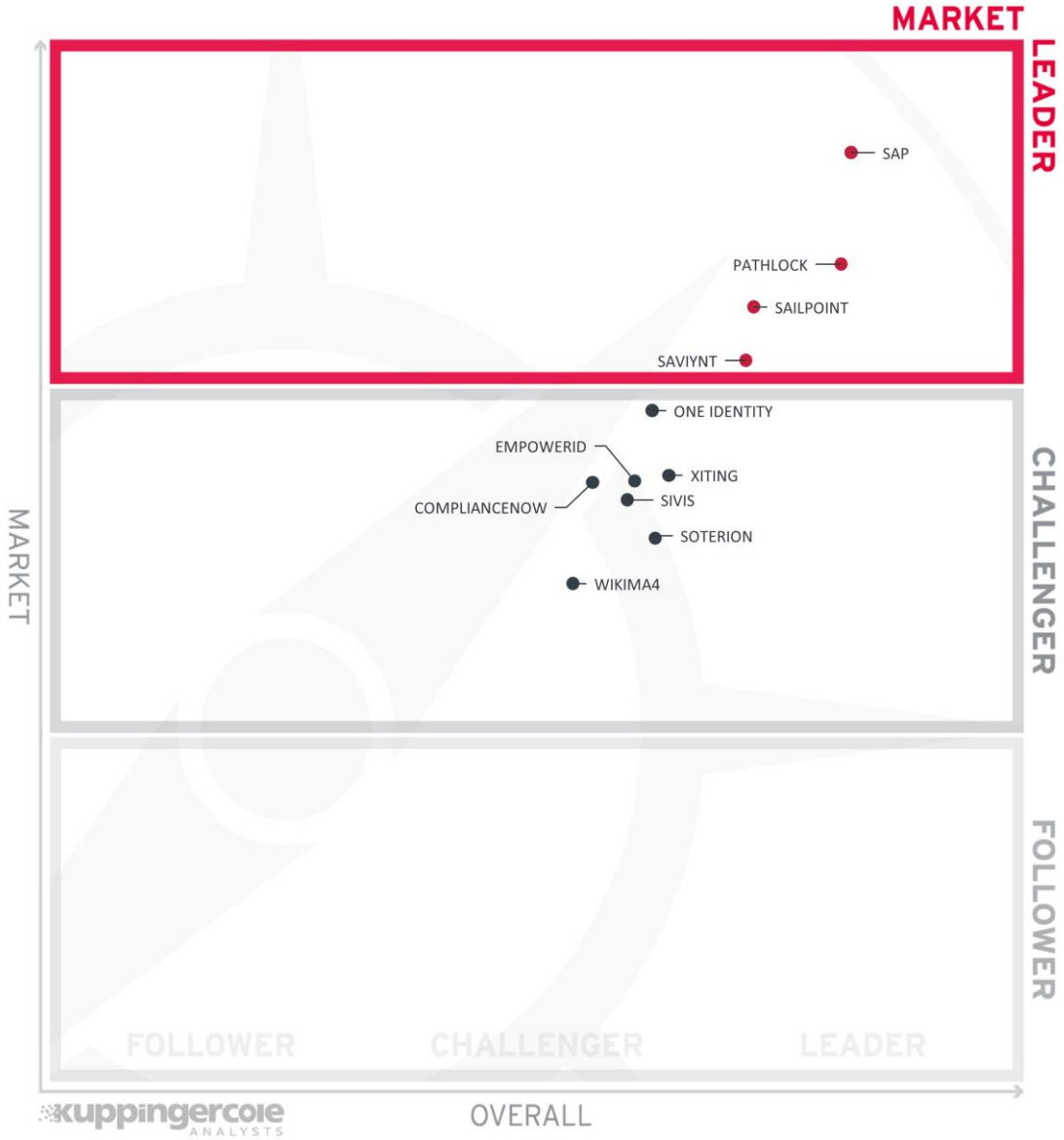


Figure 5: Market Leaders for Access Controls Solutions for SAP Environments.

In this analysis, we specifically focus on the market position for SAP environments and not on the overall IAM market position of vendors. Thus, a larger vendor such as One Identity that supports SAP environments but does the majority of its business in other areas does not

qualify as a Market Leader. However, not only the number of customers but also the partner ecosystem and other factors impact this rating.

In the Leaders segment, we find SAP ahead of the competition, having the by far largest market share. Pathlock is following them with some distance, having improved from the previous edition of this report by way of their various acquisitions. SailPoint and Saviynt are the other two vendors that we see in the Leaders segment.

In the Challengers segment, One Identity is on top. EmpowerID as well as the smaller SAP specialist vendors (in alphabetical order) ComplianceNow, Sivis, Soterion, Wikima4, and Xiting, are all positioned close to each other in this segment.

Market Leaders (in alphabetical order):

- Pathlock
- SailPoint
- SAP
- Saviynt

Correlated View

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

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

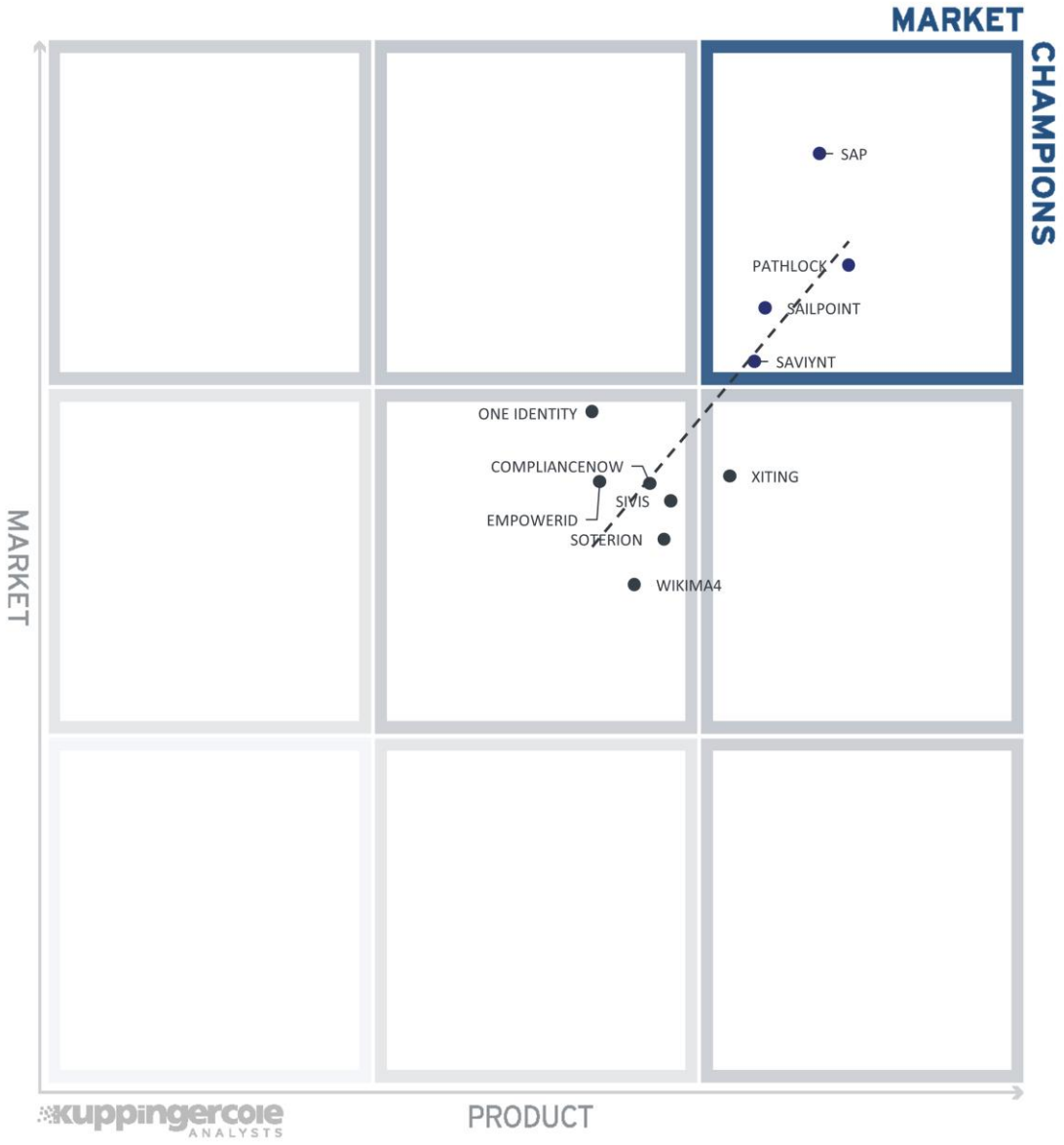


Figure 6: The Market/Product matrix for Access Control Solutions for SAP Environments.

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are somewhat “overperformers” when comparing Market Leadership and Product Leadership. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The correlation between product and market rating is good overall. SAP, due to its outstanding market position, is somewhat separate from the other vendors, while some of the specialists such as Sivis, Soterion, Wikima4, and Xiting have strong product offerings that

have a good potential for increasing their market share. On the other hand, the IGA vendors with strong SAP support benefit from their overall market position.

The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a clear correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

Figure 7: The Product/Innovation matrix for Access Control Tools for SAP Environments.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The major exceptions here are on one hand the IGA specialists, One Identity and EmpowerID, benefiting from their innovation at the platform level, and Soterion with their innovative approach to mapping business processes and risks.

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. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

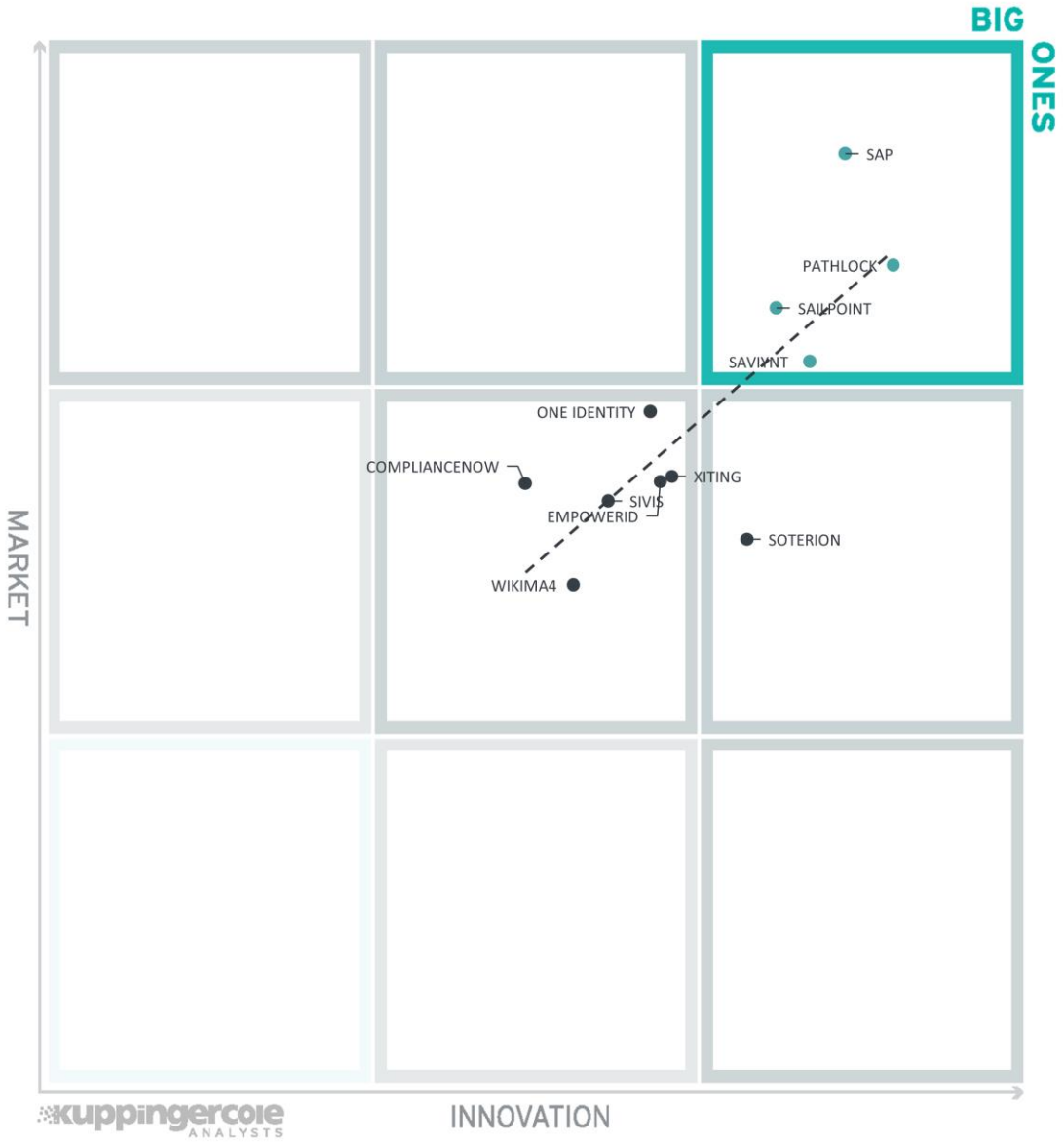


Figure 8: The Innovation/Market matrix for Access Control Tools for SAP Environments.

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Of the vendors, Soterion stands out as an Innovation Leader with a still rather small market share, while SAP, due to the strong market position, is placed quite a bit left of the line.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Access Control Tools for SAP Environments. 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.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
COMPLIANCENOW	positive	positive	positive	neutral	positive
EMPOWERID	positive	positive	neutral	positive	strong positive
ONE IDENTITY	strong positive	positive	neutral	positive	strong positive
PATHLOCK	strong positive	strong positive	positive	strong positive	strong positive
SAILPOINT	strong positive	strong positive	positive	positive	strong positive
SAP	strong positive	strong positive	positive	positive	positive
SAVIYNT	strong positive	strong positive	positive	positive	strong positive
SIVIS	positive	positive	positive	positive	positive
SOTERION	positive	positive	positive	neutral	strong positive
WIKIMA4	positive	positive	positive	neutral	positive
XITING	positive	positive	positive	positive	positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
COMPLIANCENOW	neutral	positive	positive	neutral
EMPOWERID	positive	neutral	positive	neutral
ONE IDENTITY	positive	neutral	strong positive	positive
PATHLOCK	strong positive	positive	positive	positive
SAILPOINT	strong positive	positive	strong positive	positive
SAP	positive	strong positive	strong positive	strong positive
SAVIYNT	strong positive	positive	positive	positive
SIVIS	neutral	neutral	positive	neutral
SOTERION	positive	neutral	neutral	neutral
WIKIMA4	neutral	neutral	neutral	neutral
XITING	positive	neutral	positive	positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor 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.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the Leadership Compass Access Control Tools for SAP Environments, we look at the following eight categories:

- SAP ECC support: Support for traditional SAP ECC environments.
- SAP HANA support: Support for SAP S/4HANA environments.
- SAP cloud application support: Support for SAP cloud applications including S/4HANA Cloud.
- Role & Entitlement Management: Managing roles and entitlements is another key capability of solutions, including support for role modeling and other related capabilities.
- Risk & SoD Management: The focus in this area is on the analytical capabilities for the state of entitlements and risk, i.e., identifying critical assignments of entitlements and other risks. We also look at the level of management provided for SoD controls and critical access. This also covers aspects such as the rule books provided for SoD matrixes or critical access.
- User Lifecycle Management: Managing the users' lifecycle and accounts in the systems as well as integration to IGA solutions is another set of capabilities, we are rating.
- Emergency Access Management: Managing, controlling, and analyzing firefighter access also counts amongst the common and expected capabilities of solutions in this market segment.
- Extended Capabilities: This is an amalgamation of various other capabilities extending the core scope of this analysis, such as system hardening, data governance, and other features.

ComplianceNow – by Nagarro

ComplianceNow is a unit of Nagarro, a large, European headquartered, IT Service Provider with around 19,000 employees in various locations around the globe. The solution was created back in 2008 and focuses on the core SAP platforms ECC and S/4HANA. It is built using a mix of SAP Add-Ons and an external application server but focuses on a lean deployment and operations and does not requiring complex installation.

The architecture allows the solution to be delivered as SaaS, where all communication from the internal SAP systems is outbound to the application server, and never inbound from an external entity to the SAP systems.

The solution covers a broad range of capabilities, ranging from access control and emergency user access to internal controls, testing and management for process authorizations, usage monitoring, and self-service password reset. ComplianceNow is delivered with a risk library. The risk management capabilities also support solutions that are outside of the core focus and is positioned as an alternative to SAP Process Control. Risks are managed manually.

The user interface is based on the SAP Fiori Launchpad, providing access to the various capabilities of the solution. ComplianceNow is focused on customers that primarily use SAP systems respectively and are looking for a solution that is specialized in SAP environments. The solution supports them in improving the authorization concepts and user provisioning as well as emergency access concepts and SoD management. Features include role simulation, license impact analysis based on roles, and various other solutions.

The firefighter/emergency access capabilities also are focused on the SAP ABAP core. It supports starting emergency sessions, automatically closing such sessions, and auditing the session based on the relevant SAP logs. This provides a good set of baseline capabilities in this area.

As previously mentioned, the focus is on SAP ECC and SAP S/4HANA. ComplianceNow is targeting SAP environments, specifically in mid-market organizations.

Nagarro offers a rapid deployment approach for ComplianceNow based on fixed price installations. This allows for the fast installation of the solution in SAP environments, demonstrating the strength and experience of the vendor in these environments. As one of the solutions in the market targeted at the core SAP environments and partially relying on SAP Add-Ons, it is well-suited for organizations that rely heavily on SAP but are not looking for a solution with support for a broader range of SaaS services or non-SAP line of business applications.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 3: Nagarro ComplianceNow's rating

Strengths

- Proven solution with a significant number of customers
- Rapid deployment and fixed price installations
- Support for SaaS based deployments with secure communication with SAP systems
- Broad set of capabilities beyond pure access control management
- Strong process control capabilities
- Provided with an internal risk library
- Allows for analyzing the license impact of access controls
- SAP-certified solution for on-premises systems and SAP Cloud Extended systems

Challenges

- Only support for SAP ECC, ABAP-based systems, and S/4HANA
- Limited capabilities for user lifecycle management, but API-based integration with IAM systems
- User interface with support for SAP GUI and Fiori is targeted more on experienced SAP users than on business users
- Current focus on DACH/GSA and Nordics, but has global reach via Nagarro, being present in 34 countries

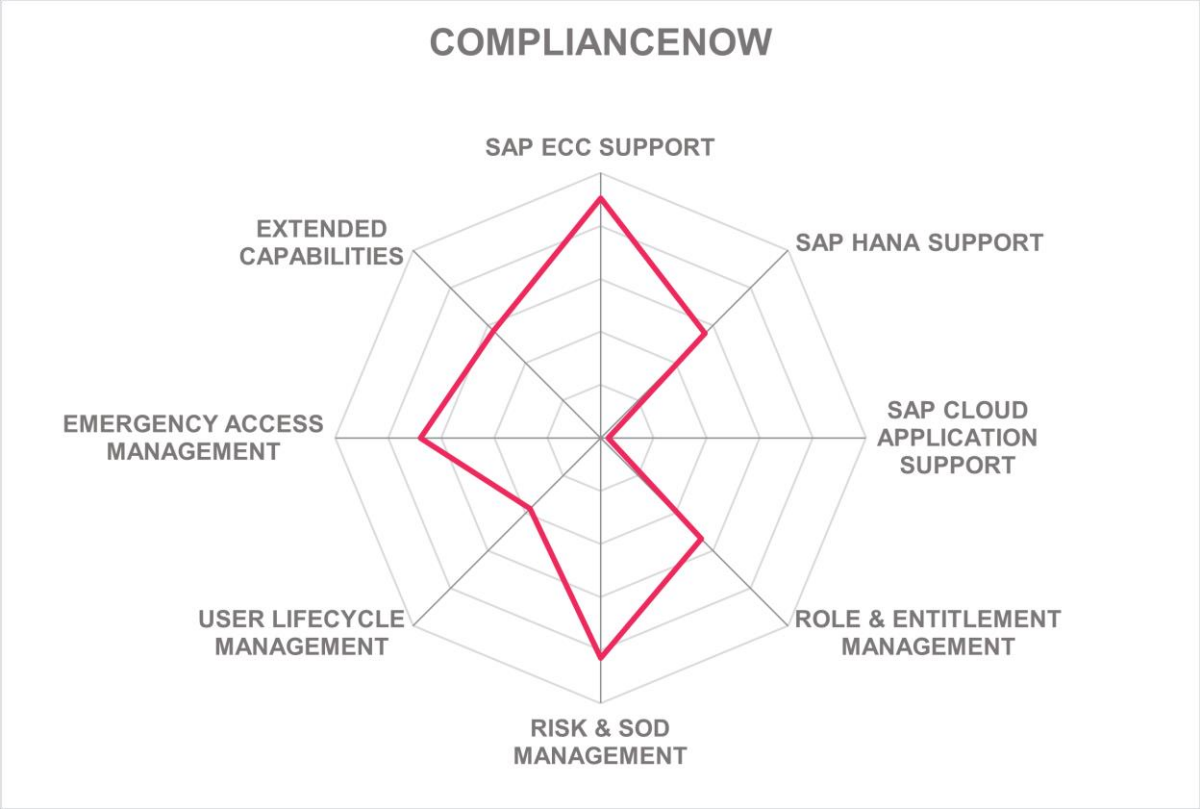


Figure 9: Nagarro ComplianceNow's additional ratings

EmpowerID – EmpowerID Platform

EmpowerID is an established vendor in the IAM space that provides a comprehensive set of solutions. These include access risk analysis, user lifecycle management and provisioning, SoD analysis, critical access management and other capabilities. With their specific capabilities in supporting SAP environments, EmpowerID positions itself also as an alternative to specialized solutions for access controls management in SAP environments.

Being a provider of a generic IAM solution, the approach EmpowerID takes on access control management for SAP environments is different than the one of most of the specialized vendors in this market segment. Everything on the EmpowerID is low-code orchestration between systems and thus factually a workflow. An example of this is the approval policy engine where different policies and the approval flow are mapped. Most customization requires some degree of (low code) coding, but there is also graphical visualization of orchestration and process flows available.

For SAP environments in specific, EmpowerID offers a wide range of connectors. These include approximately 15 connectors for SAB ABAP systems and another five that connect to Java-based solutions, plus connectors for SaaS-based solutions provided by SAP and other LoB applications. The connectors provide a deep integration into SAP environments, down to T-Codes and authorization objects and can gather and control information at all levels.

EmpowerID offers a function mapping/analysis engine that can map functions to entitlements and other objects in order to assign a risk level. While EmpowerID don’t provide their own rule books out-of-the-box, they can extract and analysis in-depth information from SAP environments into their own model, but also can import rule books from SAP Access Control. With this approach, they can convert SAP specific information into a common model which can then be analyzed. Automated mapping and conversion is supported for some environments such as Microsoft Entra Azure Active Directory and the SAP core systems, but requires customization for other applications. The unification approach taken by EmpowerID allows for efficient analysis across systems, based on that unified model. Information about risks can be displayed on dashboards.

EmpowerID comes with a modern UI including dashboards and strong reporting and analytics capabilities, but also the ability for managing access. They offer strong capabilities in user lifecycle management, access risk analysis and access risk management. The weaker spots are the limited Emergency Access Management and the lack of additional capabilities that are specific to SAP environments such as go-live management.

EmpowerID provides strong support for SAP environments and is an alternative where integration of access and risk controls with other solutions, including Microsoft environments, is preferred over a specific solution for SAP and/or other LoB applications.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Strong positive

Table 4: EmpowerID's rating

Strengths

- Strong IAM solution with a wide range of capabilities for managing users and their access
- Connectors for a range of solutions beyond SAP
- Workflow- and policy-based approach with low code support for customization
- Wide range of SAP connectors for both ABAP and Java-based solutions
- Unfied model for access risk across various applications, include SAP and Microsoft Azure Active Directory
- Automated import, analysis and conversion of SAP entitlements at all levels into the unified model
- Modern user interface with various dashboards
- Precompiled risk analysis for high performance
- Strong capabilities for access risk management and analysis and user lifecycle management

Challenges

- No own books of rules, but import capabilities
- Very limited support for SAP Emergency Access Management
- No support for additional capabilities specific to SAP environments
- Primarily focused on use cases of a generic IAM solution with strong SAP, but lesser on SAP-only implementations

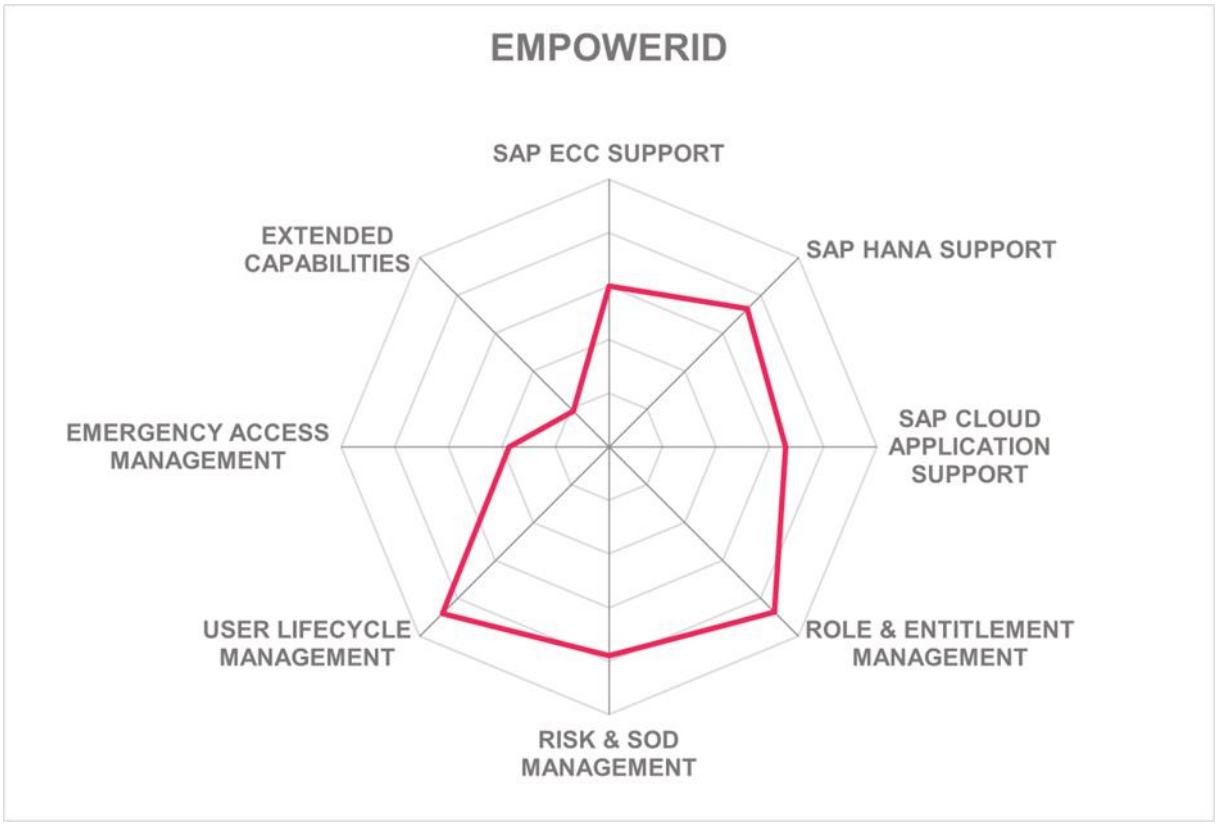


Figure 10: EmpowerIDs additional ratings

One Identity – One Identity Manager

One Identity counts amongst the leading vendors in the IAM space. They have been providing a comprehensive portfolio of IAM solutions since their acquisition of OneLogin, covering IGA, Access Management, PAM (Privileged Access Management) and Active Directory Management. One Identity Manager is their product for IGA that is also targeted at supporting managing access controls and access risks in SAP environments, in integration with IGA support for other systems and applications in the organization. Additionally, their Safeguard PAM solution also can support restricting privileged access to SAP systems, including emergency access scenarios, while not being an SAP-specific “firefighter” solution. Also, One Identity offers SAP-certified solutions for SSO (Single Sign-On) and password encryption to both SAP GUI and NetWeaver implementations.

One Identity Manager comes with strong support for SAP environments. It provides a unified console for managing SAP accounts and privileged access across the enterprise and allows putting all resources under governance by correlating SAP accounts to corporate identity. Based on that, SAP-optimized SoD rules and access reviews can be performed, but also self-service request for all SAP access can be implemented, integrated with other access requests, but also allowing for building SAP-specific workflows and business logic.

One Identity is a certified SAP partner. The integration approach One Identity has chosen is conscious about the specifics of SAP environments. Integration builds on the One Identity BAPI and does not step on SAP internal security. The SAP teams can continue creating profiles, groups, roles etc., while One Identity Manager manages the memberships and delivers access risk analytics and other capabilities. This allows for having a clear and well-defined segregation between SAP teams and IAM teams.

One Identity Manager can analyze access-related information from the SAP environments across all levels. It provides an out-of-the-box integration to SAP Access Control. With that, it can add – with or without SAP Access Control in place – cross-platform support for managing users, entitlements, and SoD rules. The SoD rule checks can be initiated and executed in various places, allowing for a flexible integration between SAP Access Control and One Identity Manager. Rules can be imported and exported bi-directionally between these two environments.

One Identity Manager comes with strong workflow capabilities, dashboards and other features. It provides leading-edge support for Access Governance features such as recertification campaigns.

One Identity Manager, with its good integration into SAP Access Control but also a strong level of direct integration with a wide range of SAP solutions and other LoB systems, is interesting as both a cross-system counterpart to SAP Access Control and a unified solution for managing access entitlements and risks in SAP environments via a strong IGA solution.

Security	Strong positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Strong positive

Table 5: One Identity's rating

Strengths

- Leading-edge IGA solution with strong SAP support
- Certified SAP partner
- Provides an own BAPI for integration
- Well-defined integration points for a clear segregation between SAP-specific tasks and generic IAM tasks
- Support for all levels of entitlements and security objects in SAP environments
- Out-of-the-box integration with SAP Access Control
- Can import and export rule sets bidirectionally with SAP Access Control
- Strong workflow features
- Strong support for SoD management for SAP and cross-platform
- Modern UI and dashboards

Challenges

- Limited emergency access support, requiring One Identity Safeguard as separate PAM solution
- No support for SAP specific additional features such as system hardening or go-live support that are frequently found in SAP-centric solutions
- No own book of rules, but import and export capabilities; also has a partnership with IBS Schreiber for importing and customizing books of rules

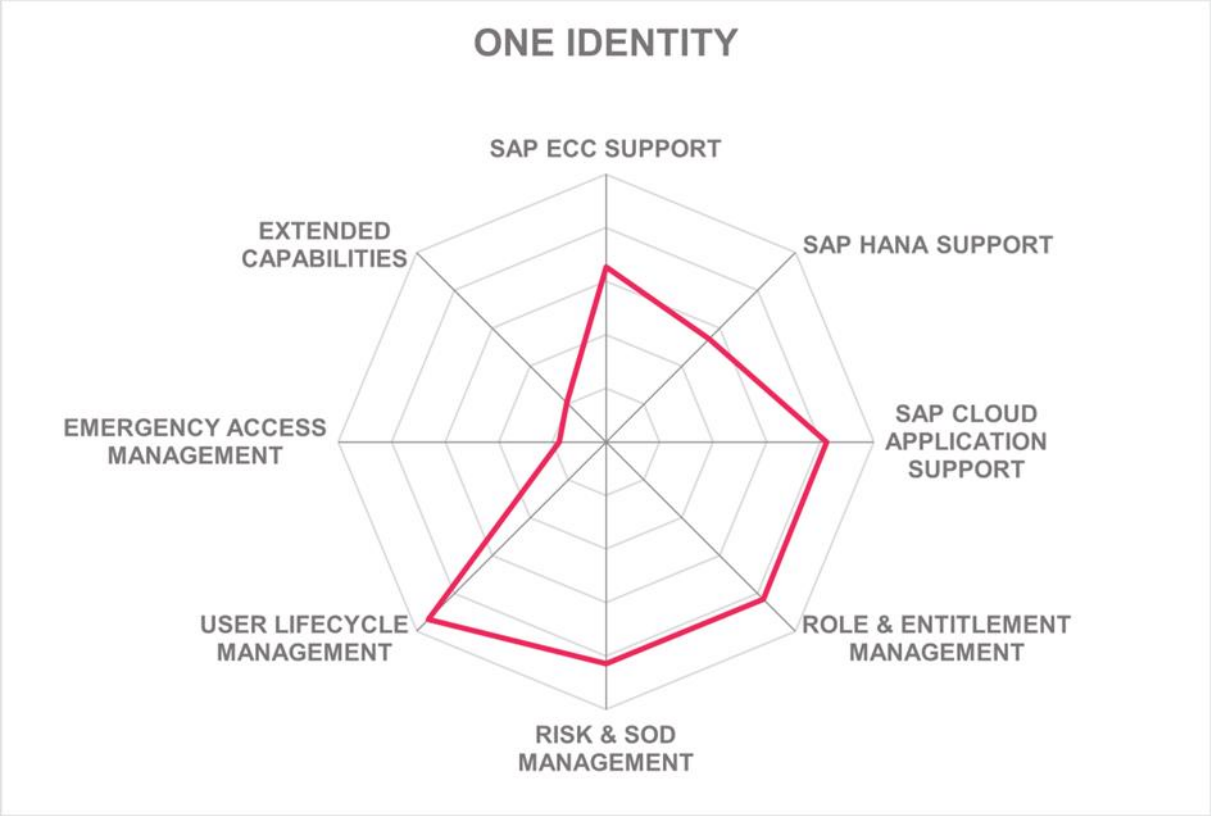


Figure 11: One Identity's additional ratings

Pathlock – Pathlock Cloud / Pathlock Native

Founded as Greenlight Technologies and providing the well-known Greenlight GRC connectors extending SAP Access Control, Pathlock has acquired Appsian, Security Weaver, CSI Tools, and SAST Solutions in 2022, delivering both a SaaS-based and an on-premises solutions for application GRC, supporting SAP, Oracle, PeopleSoft, and a wide range of other LoB solutions.

Pathlock focuses on delivering a 360-degree platform for protecting critical business applications, data, and processes. The Pathlock Platform supports more than 140 business applications on-premises and in the cloud. Pathlock focuses on risk mitigation and the automation of controls, reducing the manual effort required for achieving compliance with external and internal regulations and policies. The solutions are delivered in two variants. The strategic product is the SaaS-based Pathlock Platform, running in the public or private cloud. For customers with a stronger set of legacy systems, Pathlock also delivers a set of on-premises solutions. The focus of this report is on the SaaS-based Pathlock Platform.

The core capability areas of the Pathlock Platform are:

- Fine-Grained, granular SoD Analysis at business-function level and across systems
- Provisioning, including support for simulation of changes and automated mitigation assignment
- Continuous monitoring of the use of entitlements for “can do” analysis
- Role creation and analytics for application and business (cross-application) roles
- Emergency Access Management support, offering both role and ID options
- Recertication automation, with support for complex data-driven triggers
- Controls playbooks/libraries, providing pre-defined repositories of controls
- Workflow-support, including rule-based assignments
- Transaction monitoring for real-time “did do” analysis and conflict monitoring

The core platform then provides the common services across all functional solutions. These services include the rule engine for creating, managing and enforcing rules, for instance SoD rules or critical entitlement rules. This includes the workflow capabilities to automate request, approval, and review processes, as well as creation and maintenance of audit trails. The platform, an engine for a unified approach on risk metrics, such as the reporting and quantification of SoD violations (the aforementioned ‘did do’ analysis). Pathlock’s simulation engine supports risk assessments for both roles and users prior to provisioning. The platform also captures and reports on user activities (usage tracking).

These technical capabilities are used by a range of functional services, including user access management, role management, emergency access and PAM (Privileged Access Management), SoD enforcement, and License Management.

Pathlock is executing on a well-thought-out roadmap and will add a range of further improvements to their platform, including AI-driven controls, expanded risk quantification, CCM (Continuous Controls Monitoring), and application security features.

The Pathlock platform is a leading-edge solution in the access control market for SAP and other LoB applications. While providing leading-edge support for SAP environments, its particular strength stems from the excellent support for a wide range of other LoB applications including the extended Oracle portfolio (eBusiness Suite, PeopleSoft, JD Edwards), thus serving the needs of customers running heterogeneous LoB application environments. Certain SAP-specific capabilities require the deployment of Pathlock Native as additional solution.

Security	Strong Positive
Functionality	Strong positive
Deployment	Positive
Interoperability	Strong positive
Usability	Strong positive

Table 6: Pathlock's rating

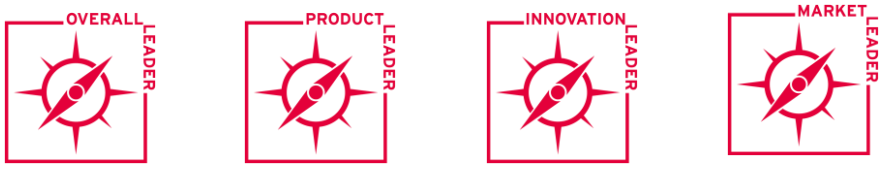
Strengths

- Broad support for a wide range of LoB applications
- In-depth support for SAP environments
- Modern user interface, including dashboards
- Broad set of capabilities around access control and emergency access
- Well-thought-out roadmap
- Proving significant progress on integrating the various acquired solutions
- Supporting cross-LoB SoD (Segregation of Duties) rules
- Broad range of capabilities for SAP-specific requirements

Challenges

- Adding process control, but current capabilities still baseline and limited to financial operations
- Pathlock Cloud integrates outside of the SAP environment, thus not leveraging capabilities such as transports, but flexible integration options (Pathlock Native product line provides such deep integration into the SAP environment)
- SaaS deployment may not suit all customer's need regarding supported platforms and regions, but available as a self-hosted, web-based solution as well for private cloud deployments
- Certain SAP-specific features require deployment of Pathlock Native in addition

Leader in



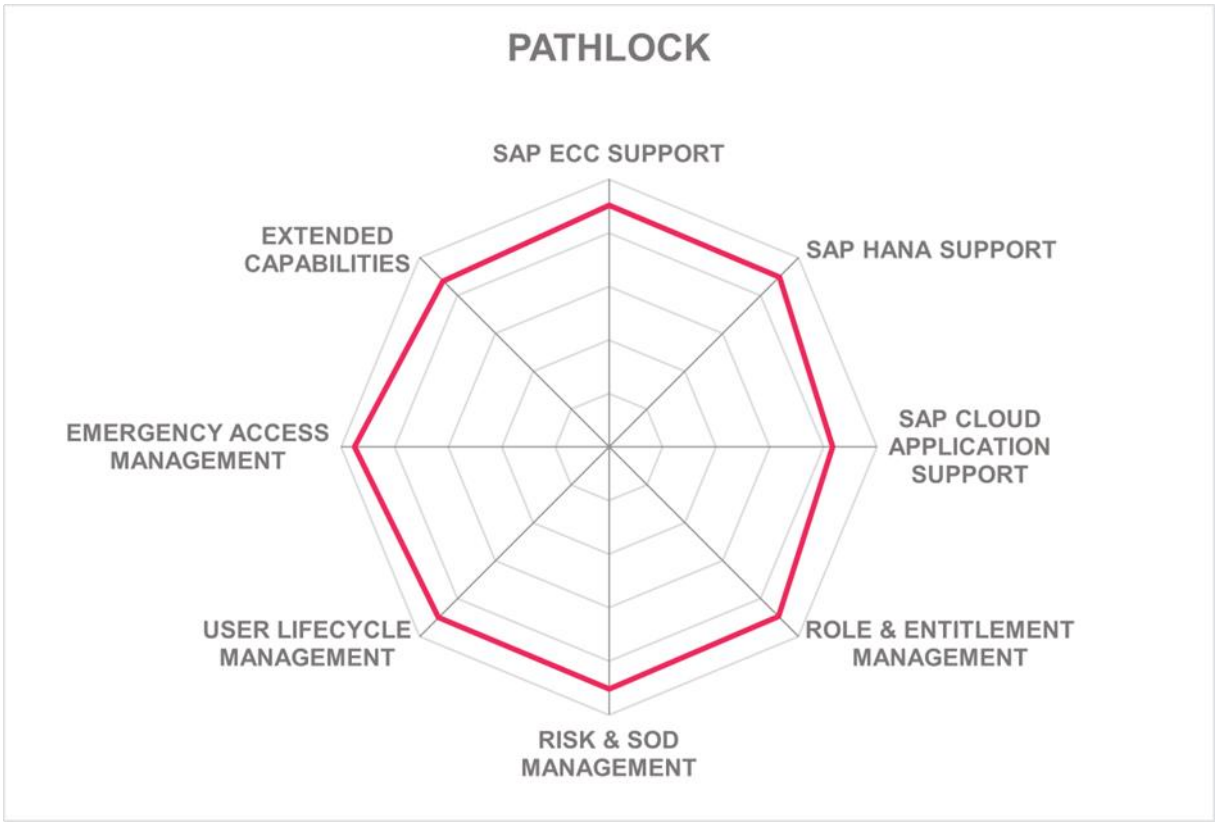


Figure 12: Pathlock's additional ratings

SailPoint – Security Identity Platform

SailPoint Application Risk Management (ARM) is a solution for managing users, their access entitlements, and the related access risk across a range of Line of Business applications, including SAP. SailPoint Application Risk Management delivers in-depth control in these environments. It is part of the broader SailPoint Security Identity Platform which combines a variety of solutions for IGA (Identity Governance & Administration), B2B Identity Risk Management, AI/ML-based analytics and other use cases. The SailPoint IGA solutions add support for cross-system controls across the entire breadth of critical business applications. The recent acquisition of SecZetta adds support for non-employee application risk management.

SailPoint Application Risk Management delivers a series of capabilities, centered around three main areas. Unified Risk Management focuses on delivering comprehensive insights across all types of applications and unifying ARM and SoD management with IGA across various LoB (Line of Business) applications and beyond. Enterprise-wide visibility is closely related to Unified Risk Management but focuses on multi-application SoD controls and risk visibility, as well as cross-application risk simulation ahead of granting access. Compliance and Audit delivers unified access reviews and reporting across the full range of applications complements the proactive parts of SailPoint ARM.

As commonly used for modern solutions, the entry point for users are dashboards, delivered as pre-defined parts of the SaaS solutions. These dashboards allow for a drill-down into details and they can be filtered and customized. This allows users of various levels, be it more technically oriented application owners, risk managers, or managers, to get the insights they require to understand the risk status and posture for LoB applications and beyond.

For some of the LoB applications such as SAP ECC, there are out-of-the-box rule books with audit-compliant controls, allowing for a quick start in implementing SailPoint Application Risk Management. For access review, SailPoint Application Risk Management supports common review campaigns, but also dashboards for administrators, risk managers, and reviewers showing the status of current review campaigns. Being an Application Risk Management solution focusing on LoB applications, there is also the depth for reviews at various levels, such as roles, transaction codes, or risks, including contextual enrichment features that inform the reviewer of actual usage and a simulated impact on risk should the access in question be removed.

Last but not least, SailPoint Application Risk Management benefits from the analytics capabilities of the SailPoint Identity Platform. It delivers advice for remediations, allows the discovery of risks from various perspectives such as roles, users, or business processes, and immediately identifies SoD conflicts.

Regarding support for other LoB applications, the current focus is on ABAP-based SAP applications and SuccessFactors, plus the SAP S4/HANA environment. Other applications including Oracle EBS (Enterprise Business Suite), Workday, Salesforce, or ServiceNow are on the roadmap. Additionally, the SailPoint Identity Platform provides integration to the full range of other business applications via their native connectors and delivering capabilities,

e.g., for user lifecycle management and baseline Application Risk Management, including cross-application SoD controls, to a broad variety of products. We expect to see a significant broader native in-depth support for LoB applications in the SailPoint ARM solution, building on the experience in both IGA and Application Risk Management coming together.

The solution is of specific interest to organizations looking for deeper integration between the management of risks in line of business applications, and between cross-platform IGA solutions.

Security	Strong positive
Functionality	Strong positive
Deployment	Positive
Interoperability	Positive
Usability	Strong positive

Table 7: SailPoint's rating

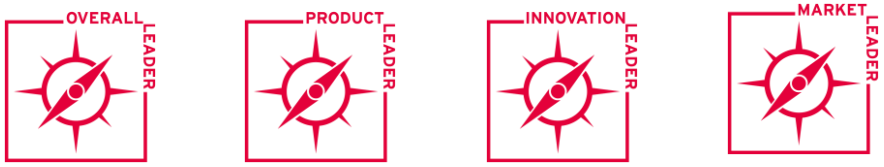
Strengths

- Easy deployment due to SaaS delivery
- Integration with the IGA capabilities of the SailPoint Security Identity Platform
- Modern UI and configurable dashboards for different user personas
- Strong set of capabilities for managing access risks and SoD controls in SAP environments and beyond, including simulation capabilities
- Good set of APIs provided as RESTful APIs
- Leverages AI & ML capabilities of the SailPoint Identity Platform for enhanced analytics
- Provides out-of-the-box rule books for SAP
- Targeted at business users, not only SAP experts, with visualization of access usage in the context of risks
- Benefits from platform enhancements such as improved workflow capabilities made for the SailPoint Identity Platform
- Full suite of Access Controls that address the needs of the auditors

Challenges

- Broad support for non-SAP line of business applications, but with limited depth for application risk management; in-depth ARM support on the roadmap for various non-SAP LoB applications
- Requires utilizing a broader range of capabilities within the SailPoint Identity Platform
- No support for managing both Fiori frontend entitlements, but backend entitlements
- No support for additional SAP-specific capabilities

Leader in



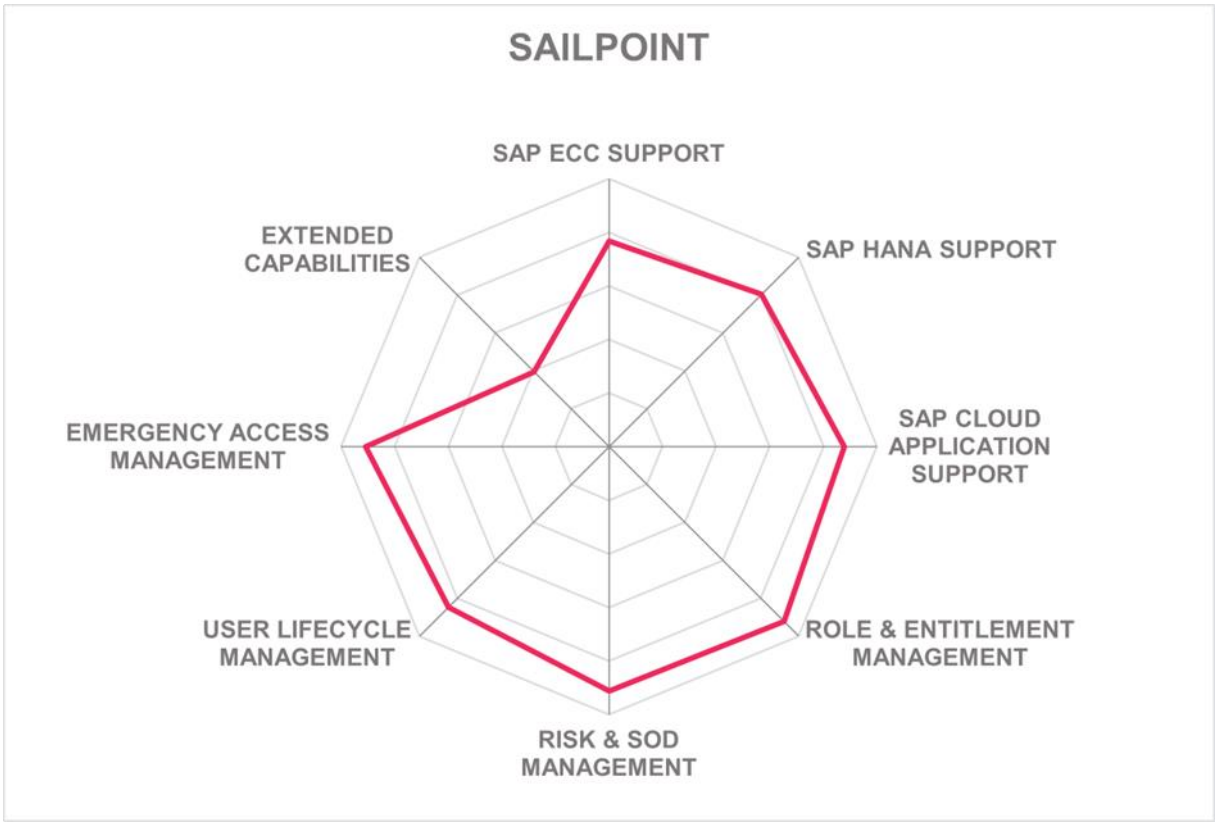


Figure 13: SailPoint's additional ratings

SAP – Access Control / Identity Access Governance (IAG)

SAP Access Control is the market-leading solution in the market for access control solutions for SAP environments – which is not a surprise given that it is SAP's own solution in this market segment. SAP Access Control is complemented and can also be replaced by SAP Identity Access Governance (IAG), which adds support for other SAP SaaS services. Customers currently have the choice between both solutions, with SAP IAG being the solution that is easier to customize and to extend towards other platforms.

SAP Access Control comes with strong support for all major features to be expected in that type of solution. It provides support for managing roles and authorization objects, has strong features in SoD management, and provides proven emergency access/firefighter support. SAP Cloud IAG comes with a rather similar set of features, but provided in a SaaS deployment model and simpler in configuration and customization. New features include capabilities such as a workflow designer for access requests or the ability for linking request tickets to firefighter log entries for review.

SAP S4 RISE PCE and SAP S4 Public Cloud are supported by Access Control PCE, extra stack and Access Control PCE S4 add-on respectively. SAP has also supported qualification of Pathlock AVM for PCE landscapes.

The solutions also integrate with SAP Identity Management (also available as PCE solution) for user lifecycle management and with other solutions of the SAP GRC solutions for managing risks. For integration with SAP SaaS solutions such as SuccessFactors, it requires SAP IAG. This might cause the need for upgrading to the latest version of SAP Access Control, which requires customers to operate a mixed environment of SAP solutions. For SAP IAG, SAP is expanding the range of supported solutions, specifically for a comprehensive support of the various SAP SaaS solutions.

SAP as the undisputed market leader, has the largest partner ecosystem of all vendors in that market segment, providing services in every region globally. This differentiates SAP from many other vendors that are limited to certain regions.

SAP Access Control and SAP IAG as the solutions provided by SAP itself, are a logical option for any shortlist in this market segment. While SAP Access Control counts amongst the more heavyweight solutions, SAP IAG as a SaaS services provides simplified deployment and customization. A major challenge for the SAP solutions is their limited support for non-SAP business applications. However, aside of relying on partners such as PathLock (formerly Greenlight GRC), SAP has added additional integration points to SAP Cloud IAG, such as the SCIM (System for Cross-Domain Identity Management) support and an API library for easier integration with other applications. Both SAP solutions can work together seamlessly.

Security	Strong positive
Functionality	Strong positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 8: SAP's rating

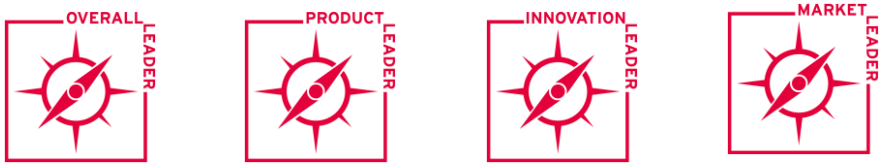
Strengths

- Proven solutions with a very large number of customers
- Very feature-rich specifically for SAP environments
- Provided by SAP itself
- Very large partner ecosystem with global reach
- Strong support for all major capabilities of access control solutions for SAP environments
- Well-integrated into the SAP environment
- SAP IAG with a growing set of integration points to non-SAP solutions
- SAP IAG with support for SAP SaaS applications

Challenges

- Focused primarily on SAP business software, 3rd party software support by partner or through interfaces in SAP IAG
- SAP Access Control requires SAP IAG for supporting SAP SaaS solutions such as SuccessFactors
- SAP Access Control being a relatively complex solution

Leader in



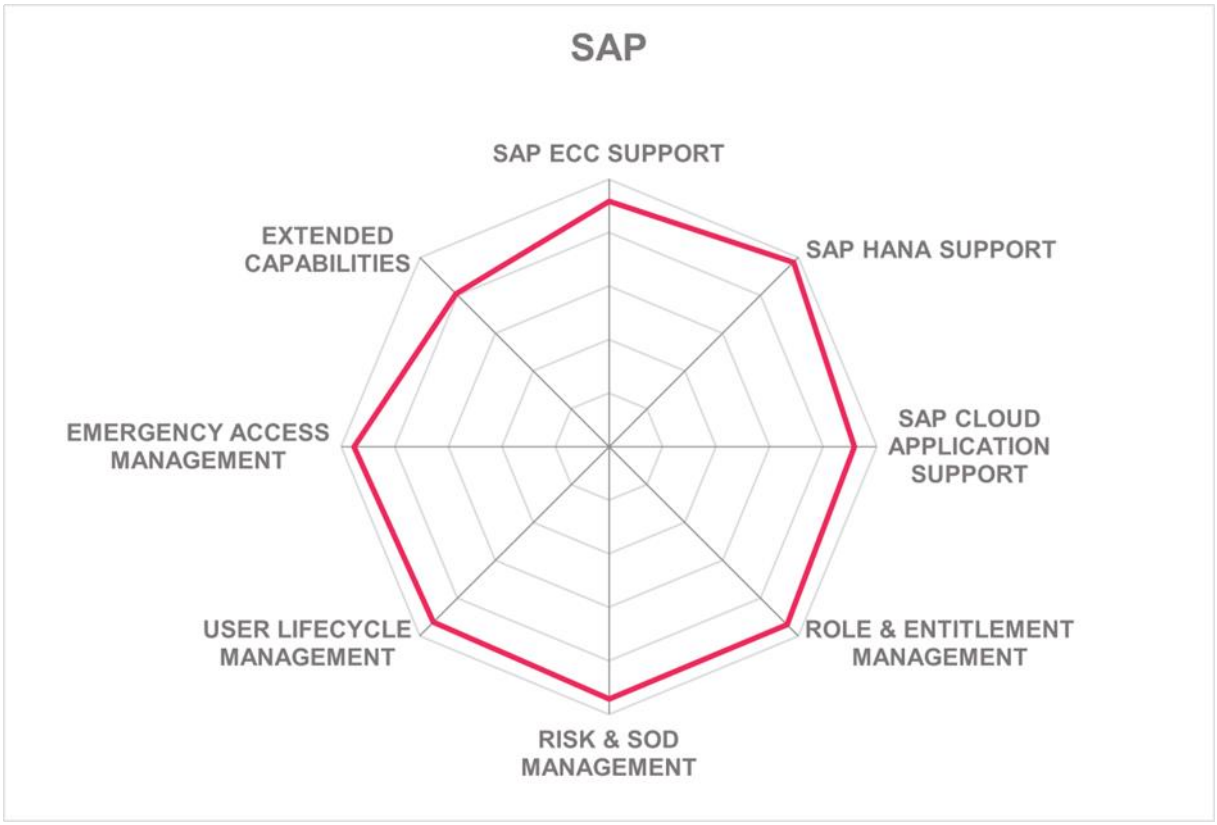


Figure 14: SAP's additional ratings

Saviynt – Enterprise Identity Cloud

Saviynt differs from most other vendors in this market segment because of their focus on delivering security and access governance solutions for a broad variety of systems, including full support for IGA (Identity Governance and Administration). They also provide in-depth support for SAP environments, qualifying them for this analysis. Saviynt provides it solutions as SaaS service, but also allows them to be run in other deployment models.

As a provider of a solution that supports the full breadth of IGA capabilities, Saviynt supports a broad set of target environments. SAP is only one of these. However, Saviynt comes with deep expertise and integration for SAP environments, provided in their specific Saviynt for SAP solutions, with SAP environments being a primary target of Saviynt from the beginning.

Features include pre-defined controls for compliance management, role management and role engineering, and other capabilities. Support is provided for all levels of SAP authorizations and access controls down to transaction codes, i.e., not limited to the high-level business role view most other IGA tools provide. They deliver preventative risk analysis for access provisioning. Saviynt also supports access reviews and can manage temporary, just-in-time (JIT) assignments of entitlements, in contrast to common standing privileges.

Saviynt has improved its workflow capabilities and also supports graphical workflow development. They support the integration of a variety of applications that are commonly used, for instance simplifying access reviews by integrating them into solutions such as Slack, Microsoft Teams, or ServiceNow.

Out-of-the-box rule sets are provided for a range of business applications, including SAP, Oracle, Infor, Epic, and Microsoft Dynamics. Another interesting capability is their support for activity monitoring, allowing to implement a CCM approach, which is based on out-of-the-box controls for a range of regulations where Saviynt delivers up to the minute status information.

Furthermore, Saviynt comes with some advanced capabilities such as the management of SAP licenses and emergency management capabilities supporting both SAP environments and non-SAP environments, based on their privileged access management capabilities. The latter includes comprehensive traceability of firefighter access. However, in contrast to some of the specialized vendors, their support for certain specialized capabilities adding to access control solutions is not their primary focus. Saviynt can address many of these use cases anyway, for instance via reporting.

Saviynt successfully combines two sets of capabilities. On the one hand, they provide strong support for SAP specifics in access control and management. On the other hand, Saviynt is not limited to SAP environments, but delivers services for a broad range of target systems, plus comprehensive IGA capabilities. This allows the creation of a central solution for IGA and business software access control. Saviynt also excels with innovation and a strong, global partner ecosystem.

Security	Strong positive
Functionality	Strong positive
Deployment	Positive
Interoperability	Positive
Usability	Strong positive

Table 9: Saviynt's rating

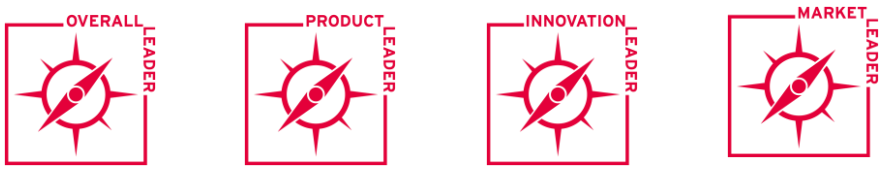
Strengths

- Strong support for common features of access control and management for SAP environments
- Supports SAP license management features
- Support for emergency access/firefighter management
- Supports user behavior analytics and continuous monitoring
- Supports standard rule books and control sets for various use cases
- Broad support for other target systems, including rule books for various business applications
- Full support for all major IGA capabilities, beyond SAP management
- Good partner ecosystem at global scale
- Wide variety of integrations to front-end applications and mobile applications

Challenges

- Some specialized add-on capabilities for SAP environments such as HCM read access supported only via reporting, but overall strong SAP specific capabilities
- Strategy focuses on delivering cross-application solutions spanning a lot of capability areas
- Limited support for SAP-specific capabilities such as go-live management

Leader in



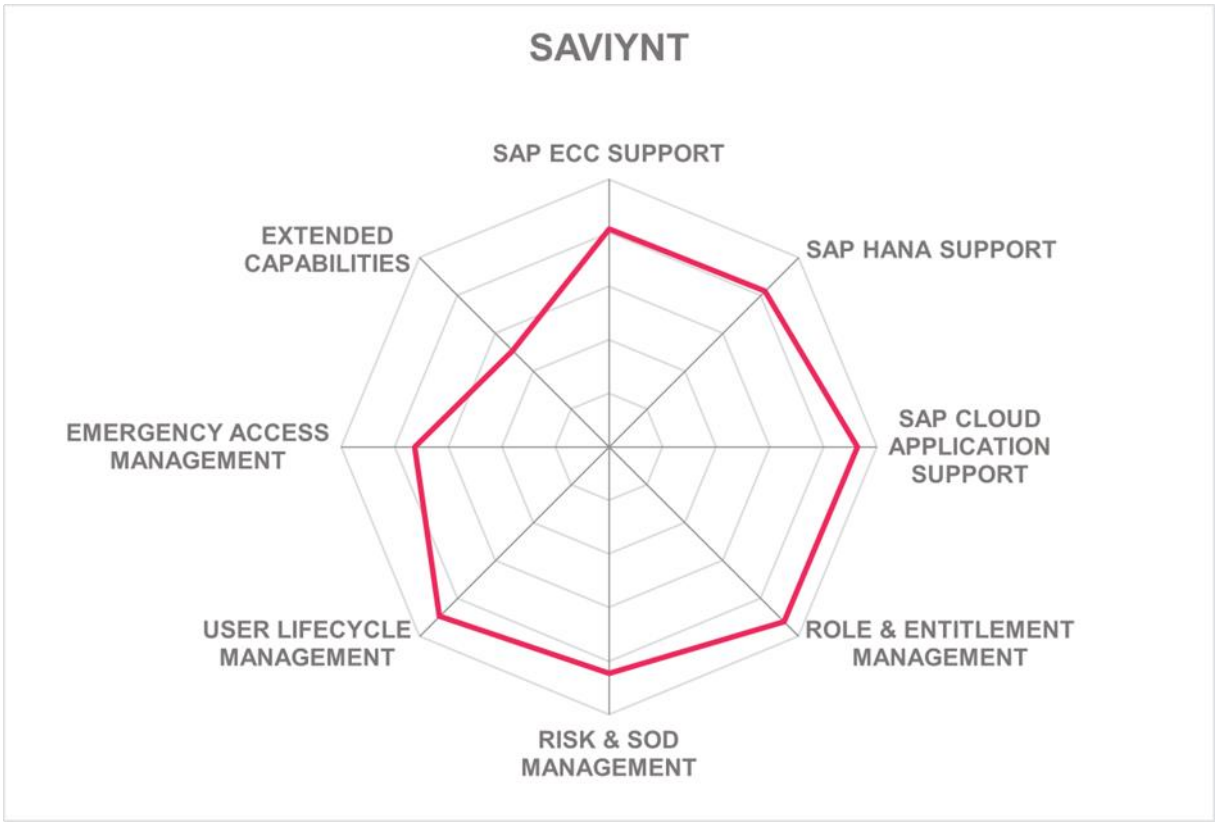


Figure 15: Saviynt's additional ratings

Sivis – Enterprise Security

SIVIS is a German provider of a solution for managing access control and related settings in SAP environments, with their SIVIS Enterprise Security solution. The company delivers an integrated set of capabilities that can be selected by the customer depending on its requirements. SIVIS Enterprise Security runs as a container-based solution in Docker, but still utilizes some components running in the SAP landscape and using the SAP transport system. Additionally, it now contains an IGA solution focused on Microsoft environments, extending support into this domain.

While having been focused on traditional SAP environments, the scope is extending beyond SAP ECC and S/4HANA. Frontends are provided as web applications, including the ones for user self-services. Furthermore, SIVIS just released a cloud connector, which allows integrating SaaS solutions as well. Available integrations include SAP Ariba and Jira. Additional integrations will be added in the future.

Overall, there are close to 20 separate modules which can be used. This includes capabilities such as the Identity Manager for managing user profiles, the Role Manager for role management including a separate module providing more than 1,000 pre-defined roles, the Compliance Manager for SoD management, altogether with pre-defined SoD controls, and many more. They also focus on optimization of entitlements in SAP environments, following a model that in future can be extended to other business applications.

Beyond the common capabilities found in most products in that market such as recertification management, alerting, and emergency access management, there are others such as the Concept Manager for automated documentation of the SAP access entitlement model. SIVIS also provides a license manager for SAP environments.

Furthermore, there are several connectors for integration with other systems for user lifecycle management and analytics, and for integrating further SAP platforms. SIVIS Enterprise Security can work with HR systems and Microsoft Active Directory, and it can connect for instance to SAP BI and HANA. With the new cloud connector, they also can integrate to other SaaS services of both SAP and other vendors. They also provide direct integration to Microsoft Dynamics 365 and Microsoft Active Directory and Microsoft 365 environments.

SIVIS currently primarily targets the German-speaking countries but has successfully expanded in the French speaking market over the last two years, partnering with major local SAP Partner and increasing their customer base in this region. They provide a good set of capabilities, and they are opening up from an SAP-only focus towards supporting a broader range of applications. SIVIS also comes with a well-integrated, modular, and easy-to-use solution for SAP environments, providing a strong alternative to other offerings in that market. With their expansion to support Microsoft environments as well, SIVIS strengthened their position as a provider of integrated access control solutions for a broader range of systems.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 10: Sivis' rating

Strengths

- Modular approach, allowing customers picking the specific capabilities these require
- Good feature set across all major areas of SAP access control
- Provides both pre-configured roles and SoD controls
- Supports automated documentation of entitlement model in SAP environments
- Supports emergency access
- Includes an SAP license manager
- Available as SaaS solution with modern architecture and container-based deployment
- IGA capabilities with specific focus on Microsoft Active Directory and Microsoft 365 provided
- Out-of-the-box integration to Microsoft Dynamics 365

Challenges

- Focused on traditional SAP environments and S/4HANA, but cloud connector allows for integrating SaaS solutions with a growing number of integrations
- Still some gaps in supporting the various SAP SaaS applications out-of-the-box
- Still small but growing partner ecosystem
- Currently primarily focused on German-speaking countries

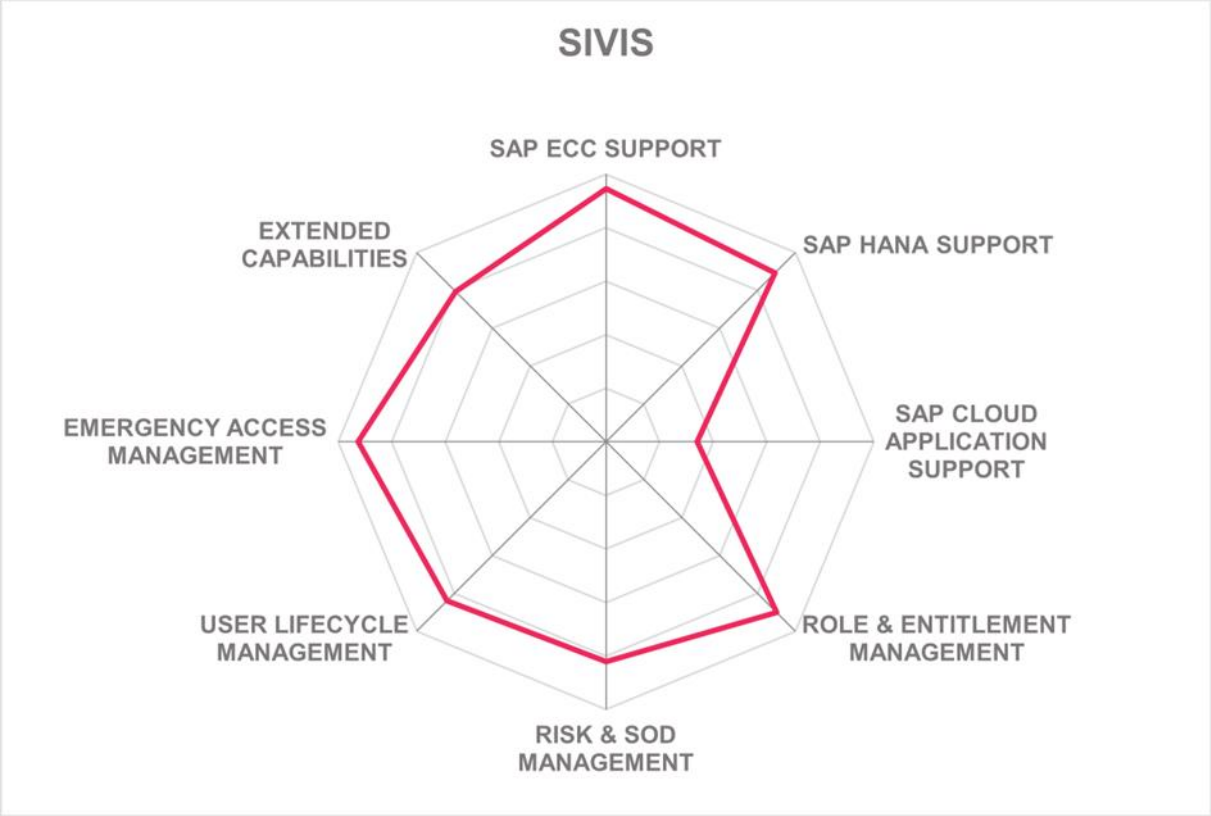


Figure 16: Sivis' additional ratings

Soterion – Access Control Suite

Soterion's Access Control Suite is an access control solution targeted at SAP environments and delivering major capabilities in that space. The solution is available as both an on-premises solution and in an as-a-service model. Soterion has put specific emphasis on delivering a solution for access control in SAP environments that is easy-to-use with a business-friendly user interface.

Soterion is able offer this range of deployment options due to a major difference compared to several of the other vendors in the market, which is that Soterion Access Control Suite isn't an ABAP application that is locked into the SAP ecosystem but runs as an independent application interfacing to the SAP ecosystem. This approach has the additional benefit that Soterion has far more flexibility in building a modern, intuitive, and business-centric user interface (UI). It also simplifies the extension of Soterion for SAP to other solutions, specifically the SAP SaaS services such as Ariba or SuccessFactors, which are newly supported, as there are interfaces to Microsoft Dynamics and Salesforce.

Soterion Access Control Suite consists of several modules, all sharing the same UI. The main module is the Access Risk Manager, which provides insight into current access risks in the SAP environment. It analyzes the user authorizations, also incorporating historical transaction usage data, to analyze the current status of authorization and their usage in the past. While analysis of the static authorizations within SAP environments is common, adding the historical usage data provides better insight into the real access risks, but also identifies excessive entitlements that aren't used in practice.

The most compelling and innovative capability is the mapping of access risks to business processes. Reviewers can work from a business process flow to understand where and which risks occur in the various business processes. This simplifies and improves reviews and risk management by taking a business perspective instead of a technical view on entitlements.

Other important modules include the Data Discovery and Classification module for identifying PII (Personally Identifiable Information) and other sensitive in SAP systems, and the Elevated Rights Manager for managing firefighter access. A specific strength is their ability to map risks to business process flows, so that users can easily understand where risks derive from.

All data is displayed in dashboards, supporting drag-and-drop capabilities for grouping, filtering, and re-arranging data, so users can easily identify high-risk areas and other relevant information. Based on that, authorizations can be optimized. One of the capabilities of the Soterion Access Risk Manager is focused on reducing redundant access. Risk clean-up wizards support the users in mitigating access related risks, but also in optimizing the role model. The tool also provides a risk clean-up projection, indicating which number of authorizations could be removed without impacting business operations.

Soterion Access Control Suite is a user-friendly, well-thought-out solution for managing authorizations, critical/emergency access, and licenses in SAP environments. It is targeted at

efficient usage, supporting business users that don’t come with a deep understanding of SAP specifics in performing both their routine jobs such as approving access as in the regular access reviews. With its innovative user interface and focus on business processes, Soterion Access Control Suite is an interesting alternative to some of the established solutions in this market segment.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Strong positive

Table 11: Soterion's rating

Strengths

- Very user-friendly and innovative user interface
- Supports all major capabilities to be expected in this type of SAP GRC solutions
- Supports transferring information into business-relevant representation by mapping risks to business process views
- Graphical representation of business processes in the context of access reviews
- Supports efficient identification and mitigating of access risks
- Well-thought-out process for access review
- Transfers emergency access information into business-friendly reports with Elevated Rights Manager
- Data Discovery module allows for identifying sensitive information in SAP
- Lean solution with efficient roll-out and implementation

Challenges

- Relatively small vendor with still small, but growing partner ecosystem
- While supporting some solutions aside of SAP ECC and SAP S/4HANA, most capabilities are targeted at traditional SAP environments
- Limited user lifecycle management, can create SAP users and highlight users with HR changes
- Clear focus on access risk management, with limited support for additional capabilities commonly found in SAP-centric access control solutions

Leader in

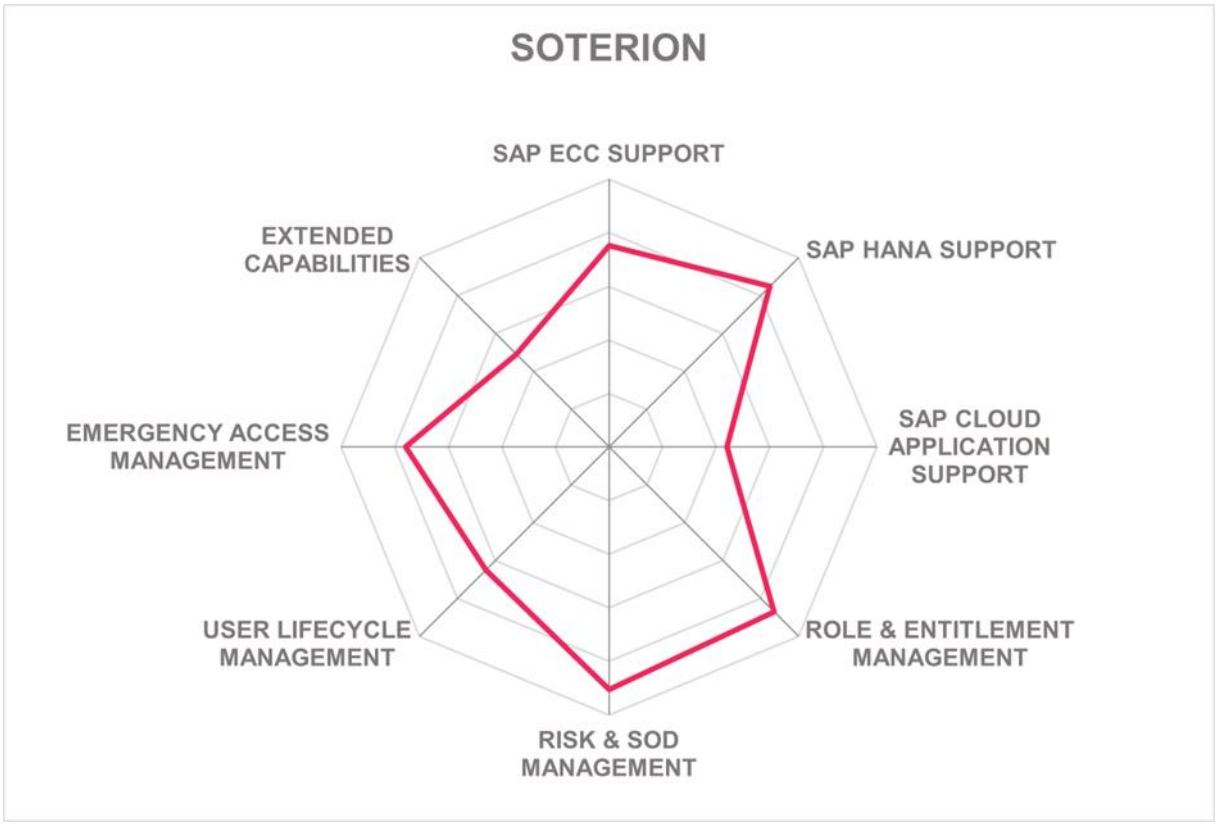


Figure 17: Soterion's additional ratings

Wikima4 – Mesaforte Compliance Suite

Wikima4 is a Swiss-based provider of SAP Security Consulting and offers their own GRC and access control solution for SAP environments. The core module of which Wikima4 has named GRC-in-a-box is Mesaforte Compliance Suite. Together with rolebee for role design and role management, the solution provides support for all core requirements we expect to see in such solutions.

While the solution is offered as an integrated suite, it consists of several separate modules, which can be licensed separately. Wikima4 not only offers generic best practice rule sets and templates, but also industry-specific ones. This allows for more efficient implementation, because the rule sets, controls catalogs, and templates are already targeted at the specific use cases within the industries.

The modules provide capabilities ranging from defining and monitoring compliance and SoD rule sets to automated analysis and monitoring of SAP security settings, usage analysis and license optimization to a range of capabilities around managing users and their access. The latter include role design and optimization as well as temporary access, e.g., for emergency access, and automated entitlement management. Furthermore, there is a module targeting the specific requirements of GDPR (General Data Protection Regulation).

For compliance and SoD management, Wikima4 has a simulation component and a dashboard with drill-down functionality. In advanced risk analysis, the capabilities include a wizard for efficient processing of violations. For the firefighter modules, specific emphasis is on improved forensics for identifying changes made during emergency access.

Recently, the focus has been expanded towards ICS support (Internal Control System) and analytical functions for business users. This includes CCM (Continuous Controls Monitoring) capabilities based on real-time data.

The Wikima4 solutions are tightly integrated into SAP environments and benefit from the consulting practice of the organization, such as with the industry-specific catalogs. The main focus is on traditional, homogeneous SAP environments. This might impose a restriction for customers that run an environment with a heterogeneous set of business applications, or which increasingly build on SaaS services. However, Wikima4 can integrate on demand with further applications, including homegrown applications.

The solution is focused on key requirements of customers, for rapid implementation, not overloaded with specialized capabilities. Wikima4 is primarily focused on the German-speaking countries, with only few customers outside of that region. The partner network is very small. However, Wikima4 offers its own consulting services in their core region, being able to directly serve the customers.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 12: WIkima4's rating

Strengths

- Focused and modular solution for core requirements of managing SAP access controls
- Provide industry-specific rule sets and controls catalogs
- Strong experience in SAP security consulting
- Integrates security analytics for SAP security configuration
- Strong capabilities in building and maintaining role models
- Supports simulation and advanced risk analysis for rule violations and SoD conflicts
- Strong forensic capabilities in firefighter module
- Rapid implementation
- SAP S/4HANA ready
- Good baseline support for CCS

Challenges

- Very small partner network, but various global customers headquartered in Switzerland
- Primarily focused on German-speaking countries
- Focus on core SAP services, lack of broad out-of-the-box support for SaaS services, but ability to integrate, e.g., with homegrown solutions
- Not all SAP SaaS applications supported out-of-the-box

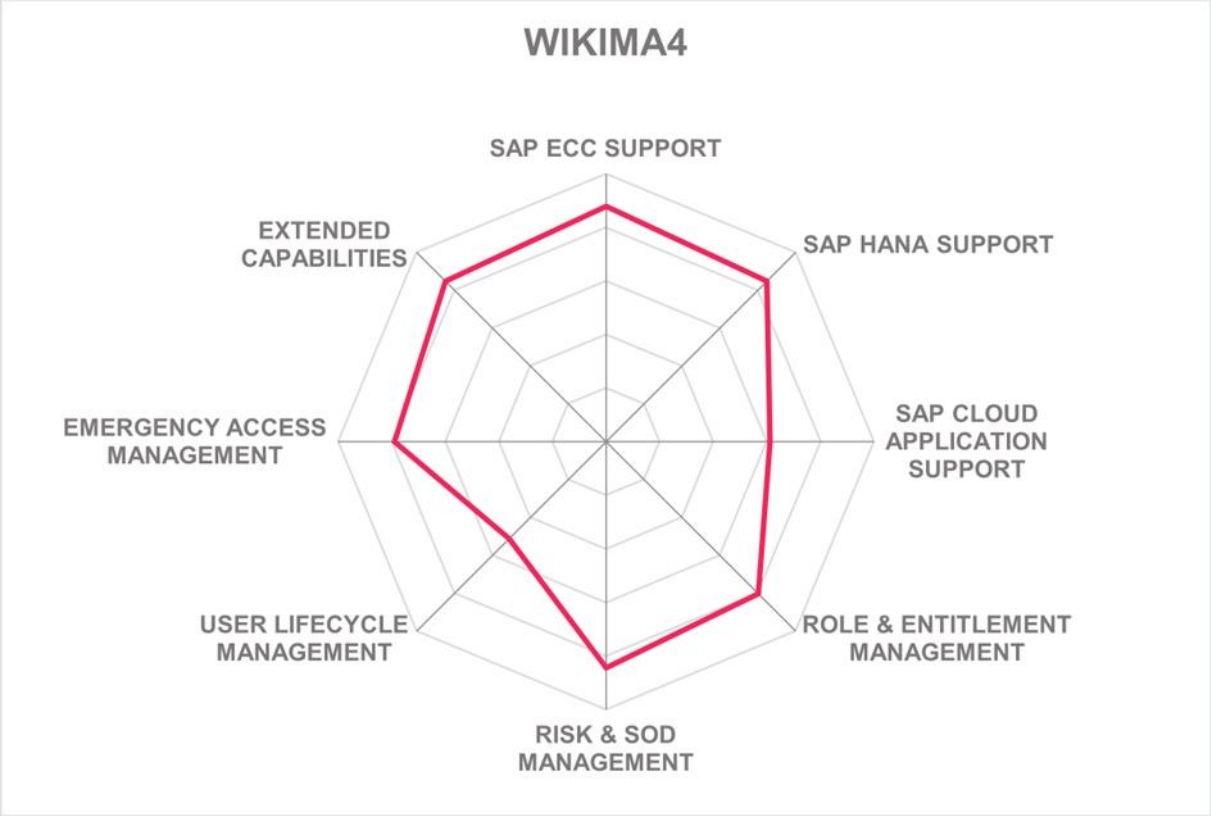


Figure 18: Wikima4's additional ratings

Xiting – Xiting Authorization Management Suite (XAMS)

Xiting is a product and consulting services company in the SAP market that offers a wide range of services, especially around security and authorizations. This includes RFC cleanups as well as the development or cleanup of SAP authorization concepts.

Xiting has developed their own products based on their experiences in consulting. The core product is XAMS, the Xiting Authorization Management Suite. This is supported by the XCW module (Xiting Centralized Workflow) in order to implement processes and workflows in a uniform manner. Xiting's various solutions are currently bundled in XSP (Xiting Security Platform), which supports a wide range of additional security functions.

XAMS provides comprehensive functions for the development and implementation of authorization systems, but also for user management and risk management. The modules within XAMS can also be licensed individually and are often very powerful. The Role Profiler, for example, supports over 100 different functions such as role mining or simulation functions.

At the same time, many other supplementary security functions in the SAP environment are also supported via the other modules. XAMS itself is primarily geared towards classic SAP systems, while the extended XSP provides standardized and unified support also for cloud-based solutions such as the various SAP SaaS products. Centralized, dynamic rule sets can also be used.

XAMS can be used flexibly in different scenarios. It can be used in close integration with SAP Access Control, for example, to perform role design in XAMS and then check against the rule set in SAP Access Control. In this area, Xiting takes a leading role in the market, supplementing also various other solutions in this market segment when extended capabilities are required by the customers.

For customers with less complex SAP infrastructures, XAMS can also be used as a standalone solution or in conjunction with third-party IAM/IGA solutions to provide core access control and access risk management functionality for SAP.

With XAMS and the complementary components, Xiting offers a comprehensive solution portfolio in the area of Access Control/Risk for SAP environments, which is continuously being expanded and is characterized by a very deep functional scope.

Xiting delivers an interesting alternative to other solutions in this market segment that can be used either standalone or in integration with other solutions. The solutions provide a deep set of capabilities, built based on a long and rich experience in SAP security management.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 13: Xiting's rating

Strengths

- Proven solutions based on deep SAP expertise
- Strong feature set across access controls and risk management, including managing and cleaning up entitlement models
- Own workflow solution
- Moving towards a modern, unified application architecture with reuse of capabilities across components
- Very close integration into the SAP application environment
- Xiting provides consulting and integration services
- Modern Fiori-based UI on top, but specific modules with traditional SAP GUI, focused on SAP administrators
- Flexible licensing model
- Strong integration options with SAP Access Control, but also IGA tools
- SIEM interface for delivering information to security monitoring solutions

Challenges

- Platform integration not fully executed yet, but defined roadmap
- No full replacement of all SAP Access Control functions
- Very limited support for non-SAP environments

Leader in

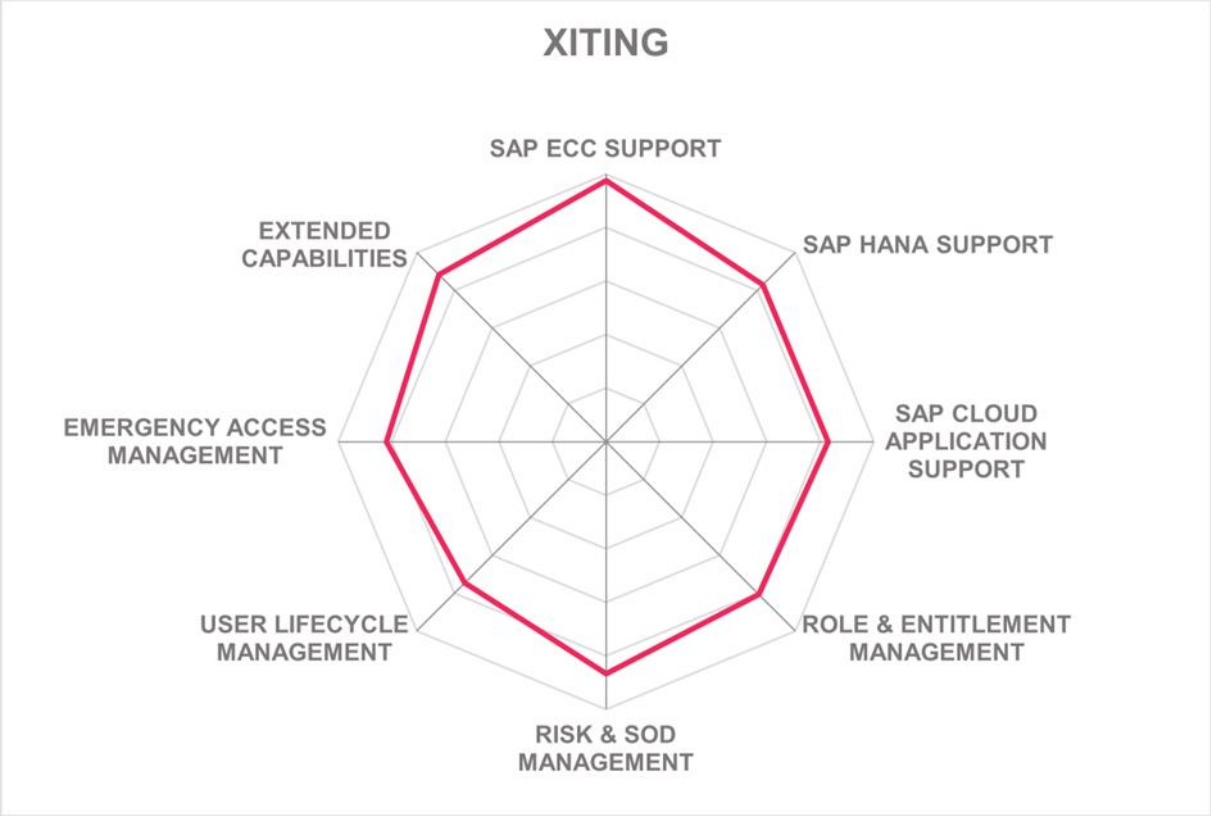


Figure 19: Xiting's additional ratings

Vendors to Watch

Besides the vendors covered in detail in this document, here are some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition, but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment, or may be a fast-growing startup that may be a strong competitor in the future.

CerPass

CerPass provides a solution focused on managing access risk and monitoring these risks for SAP environments, based on a modern, Fiori-based UI and providing various dashboards that provide insight into the SAP access risks.

Why worth watching: Modern solution that enables access risk monitoring and management in SAP environments.

Fastpath

Fastpath provides a cloud-native platform for managing compliant access control and delivering IGA capabilities for multi-application environments. Fastpath, after the acquisition of Ideiio, comes with a portfolio combining access control for multi-vendor LoB applications with IGA capabilities into a single platform. This makes them an interesting alternative for both the SAP-centric access control market and for organizations that need to manage LoBs provided by multiple vendors. Integrations are provided for a wide range of LoB applications, including SAP, Oracle, Microsoft, Salesforce, and Workday. Additionally, Fastpath provides integrations to various other platforms, IGA systems, and authentication platforms such as Okta and OneLogin.

Why worth watching: Powerful solution with good IGA support and broad support for a variety of LoB applications.

IBM

IBM provides with its cloud-based Security Verify (Identity Governance & Administration) a solution that is primarily targeted at the IAM market. The solutions come with well-above average capabilities in managing SAP environments, including authorization objects, and thus exceeding what is commonly found in that type of tool. With its strong support for heterogeneous environments, it might become an option to specialized solutions, despite not offering the same level of specialization.

Why worth watching: Option if cross-platform IGA capabilities are in focus and some good level of support or access control management for SAP is required.

IBS Schreiber

IBS Schreiber delivers a solution for analyzing authorizations in SAP environments with their CheckAud product. The focus is primarily on read-only access, i.e., a rapid analysis e.g. for consultants and auditors. Thus, it is not a full-featured solution for managing access controls in SAP environments. On the other hand, the product benefits from the extensive knowledge on SAP audits IBS Schreiber has accumulated since the 1990s. CheckAud is a strong solution for a rapid analysis of the status of SAP systems and for auditors that require a lean solution for either auditing SAP systems themselves or delivering the required information to external auditors. While some of the other vendors provide audit-only options, IBS Schreiber CheckAud is one of the few targeted solutions in that segment.

Why worth watching: Solution that is targeted on analyzing the security status of SAP environments and thus well-suited for audit-centric use cases.

NTT Managed Services

NTT Managed Services has acquired ControlPanelGRC from Symmetry. The product is an easy-to-use solution covering the major aspects of managing access control and access related GRC requirements in SAP environments. It comes with a modern UI and is well-integrated into the SAP ecosystem. It also can integrate with SAP GRC solutions to complement these. ControlPanelGRC consists of a number of modules, covering the major areas within this market segment. This includes SAP SoD Risk analysis and management of SoD controls, monitoring SAP Transaction Usage and thus adding an element of Continuous Controls Monitoring, plus using such information for SAP license management, and SAP Audit Management. The solution also provides the full breadth of user provisioning and role management capabilities for SAP environments, as well as user access reviews. It also can integrate with SAP HCM in such processes, but also by securing HCM data in compliance with relevant regulations.

Why worth watching: An interesting alternative to the solutions in scope of this rating, in particular for customers focusing on SAP ecosystems.

Protect4S

Protect4S is a security add-on for SAP environments. The solution targets security scans of SAP environments and to a lesser degree the specific challenges around access controls and auditing. Protect4S can complement most of the solutions covered in this Leadership Compass with its additional capabilities.

Why worth watching: Add-on for further increasing security in SAP environments by adding scanning and analysis of security-related events.

SafePaaS

SafePaas is an established vendor in this market segment, providing good support for both SAP and non-SAP environments. A specific strength is their ability to normalize data from different sources and apply common rule sets. Additional business applications are easy to connect, and the set of out-of-the-box integrations is constantly growing.

Why worth watching: Good support for non-SAP business applications and a straightforward approach for adding further integrations.

SecurEnds

Solution for analyzing and monitoring user access and entitlements, supporting capabilities such as user access reviews, access certifications, and entitlement audits for a range of applications, including Workday, PeopleSoft, Oracle, but also certain SAP components. SecurEnds is an interesting alternative specifically for customers where SAP plays a minor role in the environment, but that are focusing on modern SaaS services for delivering their business applications.

Why worth watching: Alternative to the solutions in this Leadership Compass specifically for cross-platform requirements and managing access risks in modern SaaS solutions, but also delivering some level of SAP support.

Valantic

Valantic is a SAP consultancy and solution provider, delivering a broad range of services and solutions in the SAP market segment. With apm Suite, Valantic also offers a solution for managing authorizations in SAP environments. Other modules of apm include emergency access management, biometric access control, or password self-service. Valantic apm is another solution in this market segment that might be evaluated, beyond the products covered in this Leadership Compass.

Why worth watching: Solution specialized on improving SAP entitlement management, provided by an SAP solution provider.

Methodology

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

Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders 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 certain 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 vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

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

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates 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
- Deployment
- Interoperability
- Usability

Security is primarily a measure of the degree of security within the product/service. This is a key requirement. We look for evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer, including authentication measures, access controls, and use of encryption. The rating includes our assessment of security vulnerabilities, the way the vendor deals with them, and some selected security features of the product/service.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, 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 the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). 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. Vendors must support technical standardization initiatives. 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. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. 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.

Rating scale for products and vendors

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

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

Inclusion and exclusion of vendors

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

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

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

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

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

Related Research

Leadership Compass Identity Governance & Administration

Leadership Compass Access Governance

Leadership Compass Identity Fabrics

Executive View One Identity Manager SAP Integration

Executive View Pathlock Platform

Executive View SailPoint Identity Security Cloud

Executive View SAP Cloud Identity Access Governance

Executive View Saviynt Enterprise Identity Cloud

Executive View Soterion for SAP

Copyright

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

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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