KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

April 20, 2020

Soterion for SAP

Soterion for SAP is a GRC (Governance, Risk & Compliance) solution targeted at SAP environments and delivering major capabilities in that space. The solution is available as both on premises solution and in an as-a-service model. Soterion has put specific emphasis on delivering a solution for GRC and access control in SAP environments that is easy-to-use, coming with a business-friendly user interface.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

SAP security and GRC (Governance, Risk & Compliance) are getting more and more important for many of today's organizations. While traditional systems like HR (Human Resources), ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), SCM (Supply Chain Management) or BW (Business Warehouse) are at the core of fundamental business processes, the move towards SAP HANA, Big Data and cloud solutions introduces another, either parallel or integrated, pillar of technology.

Ensuring an adequate level of security and compliance for the continuously changing SAP infrastructure system landscape is of utmost importance. Achieving compliance to legal and regulatory requirements is one essential business driver. Beyond that, more and more organizations understand that providing an adequate level of security is a key requirement for protecting the organization's intellectual property and for safeguarding essential business data, e.g. highly sensitive customer information.

Forward thinking organizations integrate strong security into all of their processes and systems which surely is a unique selling proposition for security-savvy partners and customers. An adequate corporate security strategy (typically defined in an appropriate policy framework) covers a wide range of aspects from Audit and Fraud Management to IAM and Risk and Process Management.

Conventional SAP Security focuses on Access Governance, i.e. the management and control of authorizations, users, roles and profiles. This includes role modelling capabilities and the design and implementation of life cycle and workflow processes, including request approval and recertification. A typical next step is the control of business-oriented processes such as applying SoD (Segregation of Duties) rules or maintaining compliance with the principle of least privilege access.

Being highly important criteria, these business aspects must not be the only focus when it comes to SAP security. SAP systems are sophisticated and complex software infrastructures, that have to be secured on every relevant level. Starting at the system level this requires a hardened and well-tested operating system basis. On the network level inappropriate access to the system has to be prevented. All SAP components and all additional third-party components have to be kept up-to-date by applying mature software update management. Comprehensive information (e.g. Security Notes) about required patches and the vulnerabilities of outdated software versions is available. The application of well-defined best-practices for the configuration of individual components and the overall SAP infrastructure is a constant challenge. Detecting and preventing information leakage are probably one of the most important aspects when it comes to protecting essential

data assets. When looking at the constantly changing threat landscape involving internal and external threat actors, the real-time detection or prevention of anomalies and undesirable behavior by implementing sophisticated analytics technologies becomes more and more important. Ideally this is complemented by initiating targeted notifications or applying adequate, automated responses.

The market for GRC solutions for SAP systems is constantly evolving. Soterion, a company headquartered in Johannesburg, South Africa, delivers a solution targeted at today's common SAP environments, but differentiating from others in the ease-of-use provided by focusing on business-centric user interfaces and paradigms for using and implementing that solution.

2 Product Description

Soterion focuses only on delivering GRC products for SAP environments. In contrast to other vendors in the market segment, Soterion is not primarily a consultancy and system integrator, but devoted to deliver standard software solutions for that respective market segment. The offerings are, with some variations regarding the breadth of available capabilities, available in three form factors:

1. On premise software: Soterion for SAP can be run on premises within the enterprise, which is still a common deployment model for many organizations, specifically in sensitive areas such as the GRC related capabilities.
2. Managed Service: Soterion offers managed service deployments where they run and manage the solution, including providing specific expertise e.g. on SoD controls. This offering is targeted at smaller businesses lacking the GRC expertise, and provided by Soterion and its partners.
3. Software-as-a-Service: Last not least, Soterion also offers using their solution as Soterion Compliance Cloud Platform, with focus on Access Risk management. This approach is based on a pay-per-use model.

Soterion is able offering this range of deployment options due to a major difference compared to several of the other vendors in the market, which is that Soterion for SAP 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 will simplify the extension of Soterion for SAP to other solutions, specifically the SAP SaaS services such as Ariba or SuccessFactors, which currently are roadmap items and work in progress.

Soterion for SAP 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.

All data is displayed in dashboards, supporting drag-and-drop capabilities for grouping, filtering, and re-arranging data. Thus, 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 amount of authorizations could be removed without impacting business operations.

Once an initial clean-up has been performed, the Access Risk Manager also supports a range of additional capabilities. It comes with an out-of-the-box rule set as foundation for creating clean authorization models, supports the implementation of mitigating controls for SoD (Segregation of Duties) conflicts that are approved, and supports simulation of changes to authorizations ahead of their enforcement.

A second module is Soterion's Basis Review Manager, for inspecting the SAP Basis for compliance. This includes parameter checking, role checks including options such as identifying the use of wildcards for transactions in production environments, and user checks for critical configuration such as production users with developer keys or test users working in production environments.

The Elevated Rights Manager focuses on managing elevated entitlements and mitigating associated risks. This process includes identifying and mapping users that have elevated rights access, checking their level of access, and monitoring emergency activities performed by such users. Reviewers then can analyze the SAP activities performed in emergency and elevated access.

Another key component is Soterion Periodic Review Manager, which supports regular access review e.g. by business managers. However, this is not limited to user access review, but also supports controls review and rule set review, by the appropriate persons in the organization. Thus, different persons can perform their review tasks independently, but Soterion Periodic Review Manager allows managing and tracking the state of reviews across all levels of review activities.

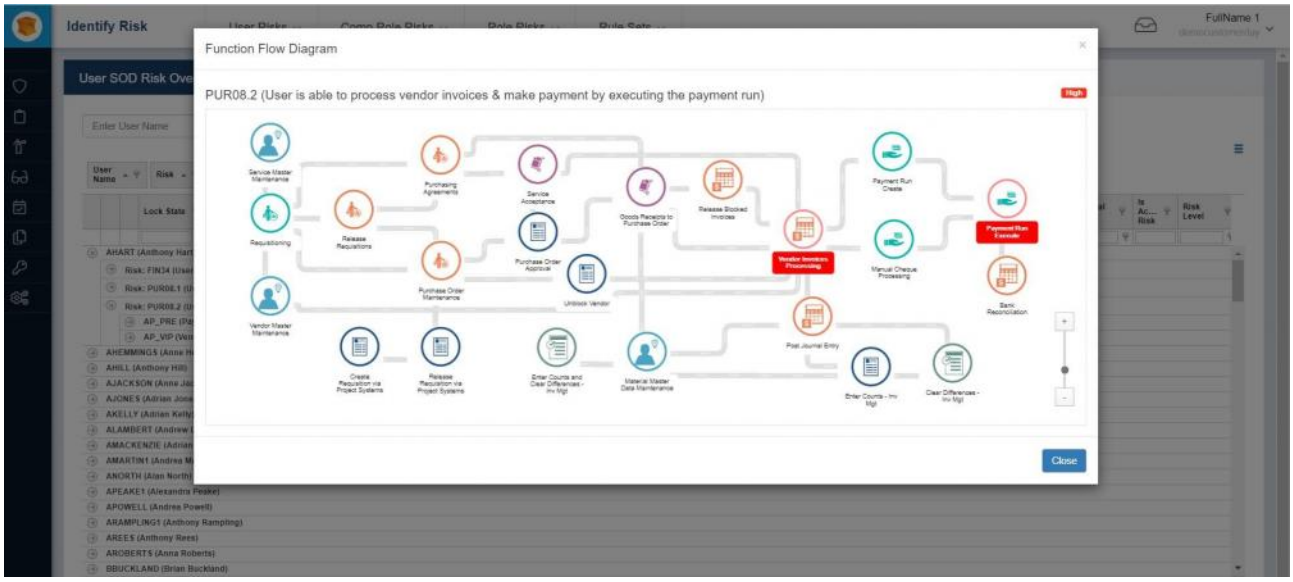

Figure 1: The Business Process Flow functionality allows access risks to be displayed in relation to a Business Process Flow diagram in order to provide the business users with more context. (Source: Soterion).

Further modules are the Employee Self-Service Module, supporting users requesting access and managers in approving the access, at all relevant levels of access within the SAP model, such as Business Roles and SAP Composite Roles. The module integrates a Risk Impact Analysis for requested access, based on the defined rule set.

Last not least, there is the Soterion SAP Licensing Manager, supporting license optimization for SAP environments.

As indicated ahead, a specific strength of Soterion for SAP is the well-thought-out user interface plus mapping capabilities, translating a technical perspective on SAP authorizations into information that relates to the perspective and understanding of business managers. This includes the ability to provide graphical representations of business flow in the context of authorizations and access reviews, giving business managers an understanding about the activities in the business flow and their relationships.

3 Strengths and Challenges

Soterion for SAP 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.

A specific strength is the graphical representation of business flows, which helps users in understanding the context of authorizations, e.g. when performing an access review. Generally speaking, the UI with its dashboards and drag-and-drop capabilities is well-above what commonly is found in that type of solutions.

Amongst the challenges, we identify the current lack of support for SAP SaaS services such as Ariba and SuccessFactors. Furthermore, some feature areas such as also managing the user lifecycle, beyond access entitlements, are still lacking. Soterion also is still a relatively small vendor with a limited, but growing partner ecosystem. In sum, specifically due to the innovative user interface, we recommend adding Soterion for SAP to evaluations for solutions in that particular segment.

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
- 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

Challenges

- No support for SAP SaaS services such as Ariba and SuccessFactors yet, but on the roadmap
- Relatively small vendor with still small, but growing partner ecosystem
- No user lifecycle management capabilities provided

4 Related Research

Leadership Brief: SAP Security Priorities – 72017
Leadership Compass: Access Control / Governance for SAP environments - 71104

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, 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 back 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.