KuppingerCole Report

EXECUTIVE VIEW

by Matthias Reinwarth | March 2015

ERPScan Security Monitoring Suite for SAP

ERPScan Security Monitoring Suite for SAP is an enterprise level solution for SAP security. By addressing vulnerability management, source code security and the analysis of Segregation of Duties (SoD) violations, it provides comprehensive security analytics covering all relevant aspects of enterprise SAP deployments.

by **Matthias Reinwarth**
mr@kuppingercole.com
March 2015

Content

Related Research

Leadership Compass: Access Control / Governance for SAP environments - 71104 (upcoming)

Executive View: SAP Audit Management - 71162

1 Introduction

For many enterprises SAP systems are the backbone of the IT infrastructure. Critical business information is stored within ERP systems, and the golden source for employee data is the SAP HR system. Customer data is stored within the CRM system, business processes are implemented through portal solutions relying on SAP NetWeaver and highly individualised functionality is coded right into the existing standard SAP modules by using ABAP or JAVA.

While most also have other systems in place, which contain critical information as well, business relies on the availability of well-designed and well-protected SAP Systems. Traditionally SAP systems are major targets for internal and external auditors. And usually they are especially vulnerable to attackers from both inside and outside the organization due to the high level of complexity and individual configurations.

- Usually the first (and often the only) aspect that is being considered when it comes to SAP security is the business logic security, i.e. the identification of Segregation of Duties (SoD) issues and their mitigation with SAP's own GRC system or adequate third-party GRC solutions. A comprehensive analysis of this market segment will be available as a KuppingerCole leadership compass later this spring.

While SoD does in fact form a major part of SAP security, the scope of aspects to take into consideration for implementing and continuously maintaining secured, robust and reliable SAP systems goes beyond that. A more complete view of SAP security has to take at least two more aspects into account:

- Application platform security: Just like any other IT system, SAP systems are vulnerable infrastructures themselves. Each component of the application platform along with their interactions and the communication of all components are potentially endangered. Misconfiguration, missing patches, weak passwords or both known and newly discovered vulnerabilities put the system and thus stored corporate data at risk of unauthorised access from insiders.
- Custom code security: Additional functionality is coded into the SAP platform by using programming languages such as ABAP and Java. Weak, unclean or even rogue code can compromise an SAP system, which has to be appropriately detected and cleaned up.

2 Product Description

ERPScan was founded in 2010 with the U.S. headquarters located in Palo Alto, California. An additional European headquarters located in Amsterdam, NL has been added recently. ERPscan maintains its own highly networked research subdivision focusing on critical enterprise applications, which provides up-to-date expertise about SAP security resulting from hands-on analyses, partially in cooperation with SAP. These teams and their continued analysis work is widely recognised in research and business alike, which directly influences the quality of the products and services provided by ERPScan.

The ERPScan Security Monitoring Suite is the flagship product of ERPScan and is designed to cover all areas of SAP security by providing individual modules well integrated into one comprehensive user interface.

The solution can be operated as software installed on-premise, in a cloud deployment or in a "Software as a Service" (SAAS)-deployment scenario.

Typical use case scenarios vary between individualised one-off scans and continuous deployment for on-going maintenance of system security and sustainable system management processes.

The system is divided into three basic, functional areas:

- **Data input via connectors:** Interfaces to the SAP environment, so called connectors, retrieve information from installed SAP modules.
- **Data processing:** Collected information is consolidated and processed. This is logically divided into modules. Available modules include functionality for maintaining the risk associated with each vulnerability (risk management), creating tasks and following up on them (task management), creating and scheduling individual scans (project management) and automated landscape scan and detection for complex SAP systems and their available services (landscape management), among others.
- **Output of results:** Results are provided in various ways including management–type dashboards, reports, trends and statistics and notification mechanisms such as mail or tickets.

All components are designed to be read-only, passive and detective, with a clear focus on identifying and reporting existing vulnerabilities. Common SAP access protocols are deployed, so no agents are installed and no modifications are required to the existing SAP environment. Connectors are available for a variety of SAP data sources, including ABAP via RFC functions, Java, HTTP, SOAP, WEBRFC, SAProuter, SAP Business Objects, Mobile and databases such as Oracle and SAP HANA.

The system benefits heavily from its underlying security and vulnerability information database, containing in-depth information for conducting assessments and analysing potential vulnerabilities. This database includes information as provided by SAP itself and is enhanced with information from the research teams associated with ERPscan. It is updated on a monthly basis to allow for up-to-date checks and to identify newly discovered vulnerabilities and threats.

Scans and analyses are configured as so-called projects, which allow the design of many different, preconfigured and tailor-made scan types that can be executed either manually or scheduled and allow for statistical evaluation, subsequent comparisons and the identification of trends.

The product suite includes feature-rich modules for the three areas of SAP security:

- **Business logic security:** SoD module provides in-depth, configurable analysis features for identifying critical access and Segregation of Duties conflicts.
- **Application platform security:** The vulnerability management module allows for several types of checks for vulnerabilities in a high number of SAP services. The types of checks include blackbox penetration testing (scans without authentication, like an external attacker would do), whitebox security assessments (scanning for system misconfiguration regarding authentication, encryption, monitoring, excessive user access and generally insecure system configuration) , password brute

force checks, health check analysis (whether all latest available updates, patches and SAP security notes are installed and configured), and several more.

- **Custom code security:** Modules for scanning individually developed code for programming errors or intentionally left security issues, such as e.g. backdoors, SQL or ABAP injections or cross site scripting (XSS).

Due to its characteristic as an analysis system operating passively no modifications or adjustments to configurations or actual data is intended; nevertheless the system is capable of notifying key stakeholders by sending out configurable email notifications or integrating with ticketing and task management systems.

The ERPScan Security Monitoring Suite is designed to integrate into an existing IT Security architecture. Tasks and tickets to act upon security vulnerabilities can be created via an API interface in existing workflow systems or ticket management systems. Evaluation data from actual scan projects can be provided to existing Real-time Security Intelligence (RTSI), SIEM systems, to IT GRC or ITSM platforms. SoD rules and findings can be shared with an existing GRC platform, either from SAP or from third-party vendors.

3 Strengths and Challenges

The ERPScan Security Monitoring Suite implements a unique product design by externally and passively monitoring SAP systems as well as entire landscapes, covering all relevant security aspects (including Segregation of Duties but going far beyond that) of SAP systems from a single security monitoring platform.

The platform provides strong features for the discovery of existing SAP infrastructures. By scanning designated network segments the system can identify individual SAP components and their connections. This information is then enriched by associating identified risk information and visualised as a highly intuitive, so-called threat map.

The reporting features include the generation of customised reports for online usage or for export as static documents like PDF or PowerPoint for management communication. Deploying prebuilt compliance modules for requirement specifications like SOX, PCI-DSS or ISACA that come with the product can substantially increase efficiency during the process of achieving compliance for an SAP platform.

ERPScan, with a relatively low number of active customers worldwide as yet, is not as established as other competitors in the SAP security market segment. Nevertheless we recommend that organisations looking into improving the overall application security and compliance for their SAP landscape should consider evaluating the ERPScan Security Monitoring Suite or individual modules thereof, no matter whether there is a dedicated SAP GRC solution already in place or not. For customers outside of North America, the support of ERPScan and its partners in implementation projects needs to be carefully reviewed.

Strengths	Challenges
• Unique, complete SAP security solution covering all relevant aspects of potential SAP vulnerabilities. • Strong integration into the SAP security research Community resulting in comprehensive and up-to-date threats and vulnerabilities information. • Highly configurable for various scans and continuous monitoring scenarios. • Comprehensive landscape scanning and visualisation features, including a unique threat map approach. • Strong features for statistics and trend evaluation. Audit-ready logging and scheduled reporting capabilities. • Easy deployment (software on-premise, cloud deployment, SaaS) as a virtualized or physical appliance.	• Relatively small, but quickly growing market share outside the US. • Worldwide partner ecosystem needs to grow. • Low overall number of active customer installations. • Read-only monitoring approach focusing on auditing systems and detecting vulnerabilities might not be suitable for every deployment scenario.

4 Copyright

The Future of Information Security – Today

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

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

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

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden| Germany

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