

# Enterprise SAP Security Monitoring with ERPScan and IBM QRadar

*How large enterprises can benefit from combining ERP Security and Security Intelligence platforms*

## WHY ERPSCAN?

- ▶ **Complete.** Identify and Analyze security issues, including vulnerabilities, misconfigurations, and SOD violations. React on them in a timely manner.
- ▶ **Unique.** The only award-winning solution to provide 360° protection of the SAP and Oracle platforms.
- ▶ **Enterprise.** Continuous management of large landscapes.
- ▶ **Detailed.** Largest database of 10000+ Security Checks.
- ▶ **Industry-specific.** Specific checks for industry solutions, such as Oil and Gas, Retail, Banking, etc.
- ▶ **Cloud and SAAS support.** Can be implemented as a virtual appliance, in cloud or as SAAS.
- ▶ **Nonintrusive.** Doesn't require any agents or modification of SAP or Oracle Platforms.

## PROBLEM

ERP security is a huge issue at a time as all those who use ERP systems are under constant threat of being attacked for espionage, sabotage or fraud purposes. The recent data breach revealed at USIS, a US federal agency that provides security solutions, lends an evidence to it. As it turned out the data breach happened because of a vulnerability in an SAP system.

Due to the extreme complexity and extensive customization, business applications that store the most critical corporate data can be accessed in a blink of an eye.

The fact that numerous general security solutions, from security scanners to IDS systems, scarcely protect SAP is also of no consolation.

Take, for example, well-respected security analytic companies, Gartner, IDC, 451 Research, KuppingerCole, Qoucirca – not once their representatives mentioned that functionality of traditional ERP testing tools is very limited.

Although SAP releases about 30 vulnerability patches every month, some vulnerabilities can't be easily patched. Vulnerability Management process for Large Enterprises with hundreds of business applications involves several challenges in patching: system complexity, lack of resources and backwards compatibility. Thus some vulnerabilities can't be easily patched which leaves the systems open to attacks.

As a solution these Enterprises would like to easily analyze vulnerability data across multiple systems and monitor systems for potential attacks.

Enterprise applications and systems are spread across multiple datacenters and lines of business, driving the need to implement multiple instances of ERPScan.

However, HQ and executives demand a single unified view into "the health" of their business applications across the enterprise. Typically, SIEM solutions would fulfill that purpose, however they all lack support for gathering ERP vulnerability data.

## SOLUTION

ERPScan Security Monitoring Suite for SAP can collect most comprehensive set of security data from SAP Systems combining 10000+ security checks. Distributed instances of the comprehensive ERPScan Security Monitoring Suite implemented in multiple data centers can now be natively clustered and monitored with the IBM QRadar Security Intelligence platform using XML integration to provide complete Enterprise Business Application Security Management in one platform.

The combined solution delivers a simplified central point for advanced analysis of SAP Security Data such as vulnerabilities, Misconfigurations, code issues and SoD conflicts. In addition, all collected vulnerability data can later on be correlated and utilized in IBM QRadar to prevent SAP-specific attacks.

## BENEFITS

*Enjoy the benefits when the most detailed ERP security solution comes together with the most powerful and comprehensive Security Intelligence platform to help you secure your most critical Business Applications.*

- ▶ **Get unlimited scalability.** Manage Business Application Security from a single place, where you can accumulate, analyze and report the most comprehensive ERP security data on vulnerabilities, configuration issues, compliance, source code issues, and SOD violations from every single application in your landscape.
- ▶ **Gain actionable insights.** Get clear management level view with management dashboards to better understand highlights and represent the most common, damaging or imminent vulnerabilities across the landscapes; or which locations, business areas and assets are more secure or vulnerable in terms of compliance to regulations.
- ▶ **Get deeper understanding.** Add invaluable context from ERPScan's data about specific application vulnerabilities in ERP, SRM, CRM, HR, and Industry solutions from SAP and Oracle to OS and Network security events and data collected by IBM QRadar Security Intelligence.

“ We're thrilled to recognize next-generation innovation in the information security marketplace and that's why ERPScan has earned this award from Cyber Defense Magazine

*Pierluigi Paganini, Editor-in-Chief,  
Cyber Defense Magazine.*

“ 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 of SAP systems from a single security monitoring platform.

*Matthias Reinwarth, KuppingerCole*

“ ERPScan embraces SAP platform security, source code review for custom ERP applications and segregation-of-duties (SoD) enforcement.

*Scott Crawford, Research Director,  
451 Research*

“ As Attackers compromise the ever-expanding sections of organizations networks, retain long-term access, and venture deeper into corporate IT Resources, the attacks on ERP Systems are anticipated to Increase.

*Anton Chuvakin, Research VP, Gartner*

## About ERPScan

ERPScan is the most respected and credible Business Application Security provider. Named as an 'Emerging vendor' in Security by CRN and distinguished by more than 25 other awards - ERPScan is the leading SAP SE partner in discovering and resolving security vulnerabilities.

ERPScan's primary mission is to close the gap between technical and business security, and provide solutions to evaluate and secure ERP systems and business-critical applications from both, cyber-attacks as well as internal fraud.

We use 'follow the sun' principle and function in two hubs, located in the Netherlands and the US to operate local offices and partner network spanning 20+ countries around the globe.

## About IBM QRadar Security Intelligence

IBM® QRadar® Security Intelligence Platform products provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics and configuration and vulnerability management. These products offer advanced threat detection, greater ease of use and lower total cost of ownership.