

# The Complete Guide to ERP Security 101

## **ERP Applications Keep Organizations Running** Enterprise resource planning (ERP) systems, like SAP and Oracle

E-Business Suite (EBS), are the operational engine of many organizations for businesses to function.

running business-critical applications and holding the sensitive data needed









Payroll

Treasury

Inventory Management Manufacturing Operations



**-**





Billing

PII & PHI

## is Often Forgotten ERP systems often fall into a cybersecurity blindspot, left unprotected against internal misuse and external attacks. The results can be devastating for businesses.

**ERP Security** 







70% of organizations

say their application

portfolios have become

were breached.

64% of ERP systems

**US-CERT** published

six SAP vulnerability alerts.

more vulnerable.

### Most traditional cybersecurity vendors don't

Why?

provide visibility into the application layer of complex ERP implementations.



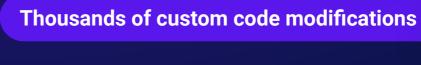
because ERP implementations are highly custom to the business, with: **Dozens of modules** 

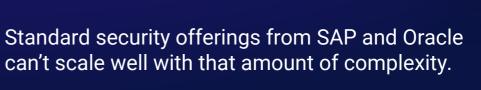
visibility that many organizations lack

**Securing ERP applications requires** 









**<>** 

#### left to someone else or pushed onto your standard cybersecurity tools. Onapsis Research Labs helps organizations find and fix vulnerabilities in their ERP systems. Here are six recommended steps toward

**Make ERP Security a Priority** 

Security of your business-critical applications cannot be

business-critical applications.



#### Firewalls and vulnerability scanners protect networks and infrastructure, but not the ERP application layer. Risk-based vulnerability management of the application can capture a complete view

of an enterprise's threat environment, and help security teams save significant time, money, and resources that would have otherwise been spent on lower-priority items.

Implement a risk-based vulnerability management

Six Steps to Secure Your ERP Applications

securing yours.

## **Continuously monitor threats** Security teams have implemented defense-in-depth strategies in an attempt to

protect the application layer from these threats. But existing defense-in-depth

Threat detection and response tools that continuously monitor threat intelligence

sources can detect compromised ERP credentials.

Update ERP regularly to prevent bugs from impacting the system and protect

information from being leaked or stolen. Keeping your system regularly up-to-date by keeping up with software updates makes the ERP less vulnerable to external threats.

solutions are not specifically focused on threats and vulnerabilities for

### be error-prone and there isn't an easy way to identify prioritization or patch gaps. Automated patch management minimizes the risk of critical vulnerabilities and protects the business' most important assets.

Patch quickly with automation

Stay on top of software updates

**Secure custom code** 

Organizations need a way to check that custom code and the transports that bring

application security testing solution can replace the time-consuming and error-

it in don't introduce new security, performance, or compliance issues. An

prone remediation process, enabling organizations to build security into

development processes to find and fix issues as quickly as possible.

Organizations face a growing backlog of patches. Manual patch management can

#### about threat actors for pre-patch protection. They can also provide early alerts about zero-day compromises, new ransomware campaigns, and assist in security control design and implementation.

**Use threat intelligence** 

Timely, impactful threat intelligence programs can provide insightful information

## Take your

Onapsis Research Labs is the only

organization focused on finding

## next step

vulnerabilities within ERP applications. If you're ready to secure your ERP systems, visit our resource center.



**Articles and Guides** 

Webinars

**Videos** 



White Papers

Or Talk to an Expert at Onapsis.com



Onapsis protects the business applications that run the global economy. The Onapsis Platform uniquely delivers vulnerability management, threat detection and response, change assurance, and continuous compliance for business-critical applications from leading vendors such as SAP, Oracle, and others. The Onapsis Platform is powered by the Onapsis Research Labs, the team responsible for the discovery and mitigation of more than 1,000 zero-day vulnerabilities in business-critical applications. Learn more at https://www.onapsis.com. © 2023 Onapsis Inc. All Rights Reserved.