

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—running business-critical applications and holding the sensitive data needed for businesses to function.



ERP Security 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.



In the last two years, **64% of ERP systems** were breached.



In the last five years, US-CERT published **six SAP vulnerability alerts**.



70% of organizations say their application portfolios have become more vulnerable.

Why?

Most traditional cybersecurity vendors don't provide visibility into the application layer of complex ERP implementations.

Securing ERP applications requires visibility that many organizations lack because ERP implementations are highly custom to the business, with:

Dozens of modules



Hundreds of interfaces



Thousands of custom code modifications



Standard security offerings from SAP and Oracle can't scale well with that amount of complexity.

Make ERP Security a Priority

Security of your business-critical applications cannot be 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 securing yours.



Six Steps to Secure Your ERP Applications

- Implement a risk-based vulnerability management**
 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.
- 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 solutions are not specifically focused on threats and vulnerabilities for business-critical applications.
 Threat detection and response tools that continuously monitor threat intelligence sources can detect compromised ERP credentials.
- Stay on top of software updates**
 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.
- Patch quickly with automation**
 Organizations face a growing backlog of patches. Manual patch management can 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.
- Secure custom code**
 Organizations need a way to check that custom code and the transports that bring it in don't introduce new security, performance, or compliance issues. An application security testing solution can replace the time-consuming and error-prone remediation process, enabling organizations to build security into development processes to find and fix issues as quickly as possible.
- Use threat intelligence**
 Timely, impactful threat intelligence programs can provide insightful information 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.

Take your next step

Onapsis Research Labs is the only organization focused on finding vulnerabilities within ERP applications. If you're ready to secure your ERP systems, visit our resource center.

 Videos

 Webinars

 Articles and Guides

 White Papers

Or Talk to an Expert at [Onapsis.com](https://www.onapsis.com)