ONAPSIS

ONAPSIS PLATFORM

RISE with SAP Cyber-Resilience

Let Onapsis Help You Manage Your Security Responsibilities to Achieve Cost Savings and Efficiencies

Challenge

The RISE with SAP® program is designed to facilitate the transition to the cloud with less risk. However, that doesn't mean ***zero*** risk for organizations and their InfoSec teams. The RISE customer owns responsibility in reducing this risk as well. Fundamentally, RISE is no different from other cloud offerings. SAP and the RISE customer operate a "shared responsibility model" for security. To move to the cloud with less risk requires joint collaborative effort from both parties in different areas of security.

$4.12M

Average cost of a failed, delayed, scaled back digital transformation project[1]

$2M

Average yearly cost of fines and penalties due to non-compliance [2]

While SAP owns responsibility for security ***OF*** the cloud, the customer is responsible for security ***IN*** the cloud. So if SAP will not cover ***all*** security, it's essential that RISE customers understand their responsibilities, including:

- Quality/security of migrated or new code, all transports, & change management
- Requesting application of "non-HotNews" Security Notes
- All users (including third parties) their access, and behavior
- Security audit logging, related security issues, and incident response
- Owning compliance and compensating controls

Taking on these shared security responsibilities in a new environment with less control and access than before (with onPrem) creates new challenges for RISE customers that are only compounded further with accelerated project schedules, SAP landscape complexity, under-resourced teams, and ever-growing compliance pressures.

The Solution

Better Manage Your RISE Security Responsibilities with Onapsis

Fortunately, securing complex SAP landscapes during the transition to RISE and beyond doesn't have to be complicated. That's where Onapsis comes in. As the undisputed experts in business application security with the most prolific threat research team for SAP, Onapsis has been on the frontlines securing the world's largest brands for over fifteen years. We have the expertise, successful track record and technology with the only cybersecurity and compliance solution endorsed by SAP to help our customers achieve both SAP cyber-resilience and cost and time savings

.

With Onapsis, RISE customers can:

- Build in security from the start of the project
- Achieve SAP DevSecOps for code consistency and security to keep projects moving forward
- Minimize their SAP attack surface, reduce risk, and streamline compliance
- Continuously monitor for threats and implement compensating controls

[1] Couchbase
[2] TechRepublic

Establish Good Code Security from the Beginning

Eliminate Manual Reviews
Automate code security reviews wherever developers work to eliminate errors and vulnerabilities including Eclipse for SAP BTP and others

Implement Gate Checks
Bulk scan migrated legacy code and new code and transports to prevent bad code and objects from causing issues or downtime in your RISE production environment

Validate Code from Third Parties
Verify code security and robustness from third parties before you bring it into your production systems

> "Reduced both our time and costs for reviewing code by almost 70%."
>
> – F500 Global Manufacturing Company

Minimize Your SAP Attack Surface & Streamline Compliance

> "We reduced remediation time by 83%"
>
> - F500 Bio-Pharmaceutical Company

Prioritize and Validate Patching
Identify which new/missing "non-HotNews" patches should be prioritized and requested from SAP and validate their successful application

Quickly Audit Configurations and User Permissions
Ensure SAP applications and integral components, including BTP and Cloud Connector, are configured securely with the right user access and authorization levels

Automate Compliance Efforts
Save valuable time by eliminating manual IT general control checks and evidence collection

Continuously Monitor for Threats Across New & Legacy Landscapes

Identify Suspicious User Behavior Faster
Monitor user behavior, access, and activity for insider threats, anomalies, and potential indicators of compromise

Detect and Mitigate Threat Actor Activity Faster
Get the best exploit protection available, including zero-days, and empower rapid response with detailed explanations and mitigation guidance

Easily Implement Compensating Controls
Mitigate the risk of open vulnerabilities in your environment with granular monitoring and alerts to help meet regulatory requirements

> "We're saving 20 hours of week addressing security controls around user access"
>
> - F500 Consumer Good Company

SAP Endorsed App
Premium Certified