ONAPSIS

SAP 101: RISE with SAP Cyber-Resilience

While Achieving Cost Savings and Resource Efficiencies with Onapsis

Roger Egle | Strategic Account Manager – Western Canada

September 18, 2023

SAP Landscape Complexity Creates Big Security Challenges

$4.12M Is the Average Cost of a Failed, Delayed, or Scaled Back Digital Transformation Project[1]

1

Applications Are Easy Targets

Internet-facing applications are the **easiest to attack**. The trend continues even with ERP.

2

Sprawling SAP Attack Surface

Large data volumes, massive scope across business-critical systems, and sheer size.

3

Inherent Vulnerabilities and Gaps

67% of developers admitted keeping known vulnerabilities and exploits in their code[2]

4

Risk Identification and Prioritization

Dependent on the tools used, the skillsets of the resources, and the maturity of managing application vulnerabilities efficiently and effectively.

5

High Cost of Compliance

Every business is bound by regulatory compliance requirements, such as SOX, HIPAA, etc.

[1] Couchbase [2] Secure Code Warrior

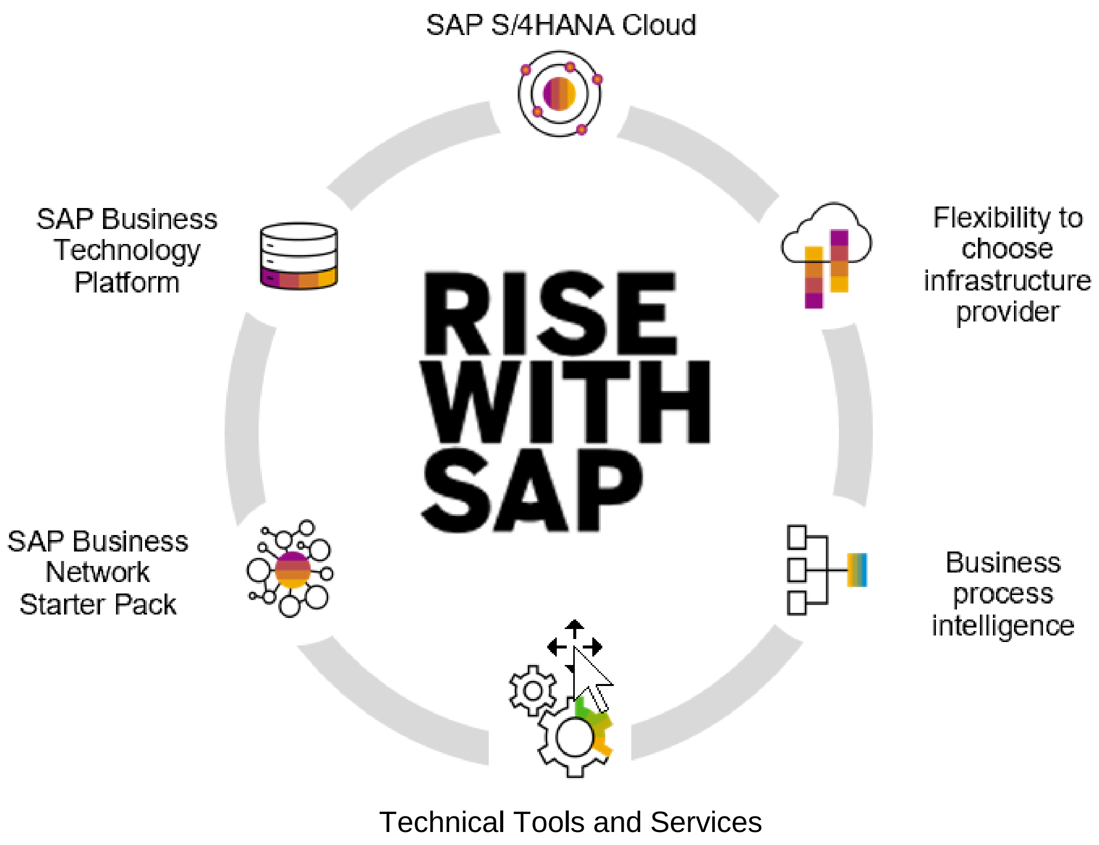
Traditional SAP Approaches We Have Seen – Now RISE with SAP becoming the Biggest

- Protecting an existing on premise ECC Landscape
- Protecting a hybrid on premise or cloud hosted ECC Landscape
- Protecting an existing S/4 on premise or hosted landscape

- *With SAP Moving to RISE, we are now seeing the need to protect pure cloud S/4 with other Cloud Assets – demand is significant*

We have customers in all forms of these scenarios

RISE with SAP: An Opportunity for a “Clean Slate”...


SAP S/4HANA Cloud
Flexibility to choose infrastructure provider
Business process intelligence
Technical Tools and Services
SAP Business Network Starter Pack
SAP Business Technology Platform
RISE WITH SAP

- Designed to facilitate an easier transition to the cloud with less risk, whether greenfield or brownfield
- Fundamentally, a “best of” combination of IaaS, PaaS, and SaaS
- Offers a ready-made bundle to guide the digital transformation journey.
- Choose your own hyperscaler, and SAP deploys and manages your S/4HANA landscape for you, **but…**

Remember: RISE Isn’t Any Different from Other Cloud Offerings

Requires A “Shared Responsibility Model” for Security

SAP

Security *OF* the Cloud

- Security for the “iron” of the cloud offering
- Includes network, OS, database, application servers, and some applications
- Only Ops and Mgmt access to applications and data
- Security and monitoring of cloud infrastructure[1]

CLOUD CUSTOMER

Security *IN* the Cloud

- Security for what goes into the cloud offering
- Also includes all data, users, their activity, access controls, configs, processes, and anything pertaining to running the business
- Security and monitoring for everything (e.g., all data) in the cloud

[1] *Unless otherwise contracted for managed security services or potentially externally managed by 3rd party*

SAP Does Not Cover All Security. Know Your Responsibilities.

For Example…

SAP

- Will own OS and cloud platform maintenance and availability
- Will own backup management & tools
- Will own patching HotNews Security Notes automatically[1]
- Patching of non-HotNews Security Notes by request
- 24/7 security monitoring of cloud platform

CLOUD CUSTOMER

- Must own quality/security of migrated or new code, transports, & change mgmt
- Must own responsibility of requesting application of "other" Security Notes
- Must bear responsibility for **all** users (incl. 3rd party), their access, and code
- Own security audit logging and any related issues
- Own compliance

ONAPSIS

[1] *Unless otherwise contracted* | Source: https://blogs.sap.com/2021/09/15/rise-with-sap-shared-security-responsibility-for-sap-cloud-services/

How Can You Better Manage RISE Security Responsibilities?

With an **expanding attack surface** and **shared responsibility**, it's more critical than ever to maintain control over **all phases of application security**:

Application Development

Application Testing

Application Protection

Being successful here leads to

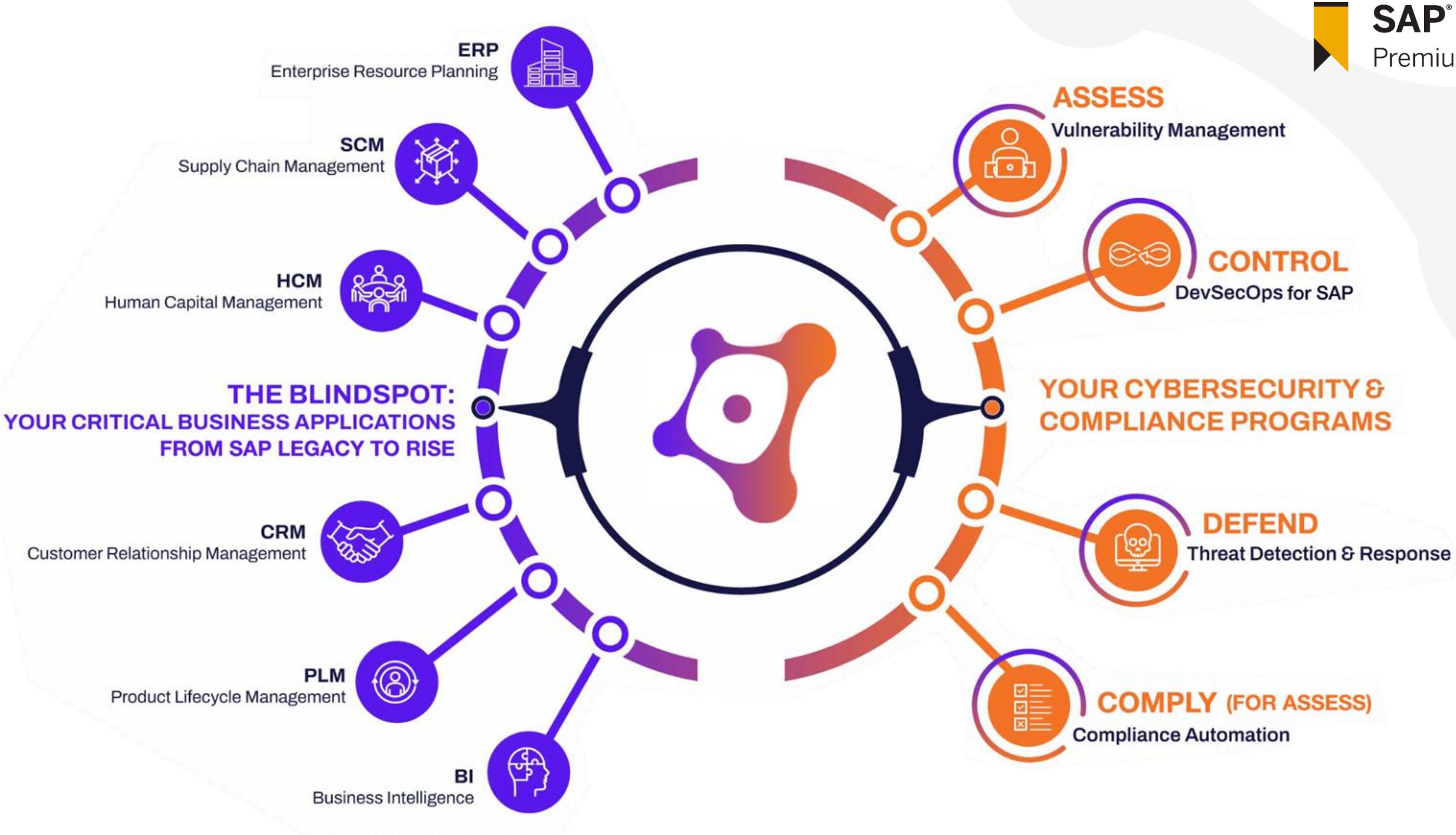
- **Shifting left** with security to reduce the financial burden on InfoSec
- Digital transformation projects **finishing on time, securely, and on budget**
- **Reduced downtime** for business-critical applications and better business continuity

BUT This Can Be Challenging and Time- and Resource-Expensive to Manage On Your Own

Onapsis: Market-Leading SAP Application Security

Gain Comprehensive Attack Surface Management for Your RISE with SAP Landscape

SAP® Endorsed App
Premium Certified



ONAPSIS

Why Do More RISE with SAP Clients Choose Onapsis?

14+ Years of SAP + InfoSec Experience at Your Fingertips

Gain access to Onapsis as a trusted SAP security advisor and reap the benefits of best practices and efficiencies.

Onapsis Research Labs: Your Secret Weapon against Threats

Let the Onapsis Research Labs guide your team with SAP threat intel, attack activity, and patch prioritization for SAP support.

More Comprehensive SAP Attack Surface Management

From code dev security to point-in-time scans and continuous pre-patch threat protection for your S/4HANA cloud, Onapsis has you covered with minimal effort.

Gain Cost Savings and Resource Efficiencies, Eliminate Downtime, Minimize Risk, and More Easily Maintain Compliance.

ONAPSIS

Shared Security: Your Responsibility Challenges with RISE

$2 Million Is The Average Yearly Cost of Fines and Penalties Due to Non-Compliance[1]

AppDev teams take shortcuts & write **bad ABAP or HANA code**

QA and code reviews **miss the security vulnerabilities** in code

Bad code from internal & external teams goes through change mgmt **without proper controls**

Ensuring SAP is configured securely with the right **user access and authorization levels**

RISE WITH SAP

S/4HANA PCE LANDSCAPE

Telling SAP **which new/missing "non HotNews" patches to prioritize and implement** is hard

Security audit logging and tracking all authorized user activity can be very challenging

Detecting and mitigating **malicious external / internal threat activity** is difficult with evolving threats

Spending **too many hours on compliance** activities instead of value-generating work

[1] TechRepublic

ONAPSIS

Where Onapsis Helps with Your Shared Responsibilities

"Lower budget across the board this year…but we still need greater visibility into evolving threats…" [1]

Control for Code **secures AppDev code as they work,** eliminating errors and vulns

Control **helps QA scan all new and migrated code** in bulk for security issues before transport

Control for Transports scans code and construct of transports to **stop bad code deployed to production**

Assess easily **detects security misconfigurations and user misauthorizations**

RISE WITH SAP

S/4HANA PCE LANDSCAPE

Assess scans your SAP attack surface and uses **ORL + AI to help prioritize patches** for SAP

Defend **monitors user activity and alerts** you to security audit log issues or anomalies

Defend monitors for real-time attacks and **provides pre-patch protection from zero-days**

Comply does the **heavy lifting for audit evidence collection,** saving valuable time for teams

You Could Spend Less Time Validating Security and Save **At Least $172K / Year** on Manual Data Extraction, Communication, and Investigation Efforts Alone

[1] SAPInsider CyberSecurity Report 2023

ONAPSIS

Why Partner with Onapsis?

RIGHT ACCESS

SAP® Endorsed App
Premium Certified

Microsoft Azure
Google Cloud
Capgemini
IBM
Deloitte.
amazon web services
SAP HANA
pwc
TURNKEY

STRONG COMMUNITY

SONY
fcc Farm Credit Canada
AMERICA'S NAVY
Schlumberger
SPARTAN CONTROLS
ATB Financial™
Pfizer
3M
OG&E
Levi's®

MARKET VALIDATED

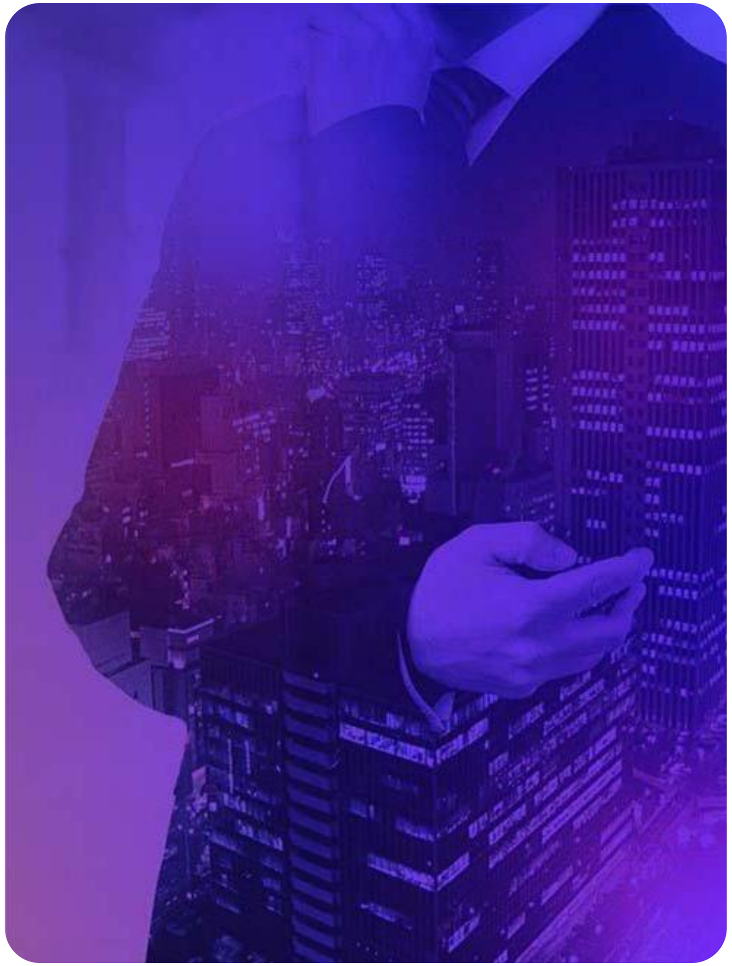
America's Fastest-Growing Private Companies Inc. 5000
Global Infosec Awards Winners Cyber Defense Magazine 2022
Gartner® Magic Quadrant
Astors American Security Today 2022 Gold Award Winner Homeland Security Awards
Infosec Awards Winners Cyber Defense Magazine
Top 10 Black Unicorns 2021 Cyber Defense Magazine

"Onapsis **removes the mystery** around SAP security by increasing visibility. We can see issues—misconfigurations, missing patches or overly privileged users—what risk they pose and how to fix them."
- Enterprise Security Lead for a $2B F500 Utility Company

"Onapsis helps us protect our SAP systems by **keeping them online, stable and available**, allowing us to be proactive with SAP security on both a system and code level."
- Global SAP Lead for a F50 Life Sciences

Let’s Talk About What We Can Accomplish Together

- Cut Security and Audit Compliance Costs for your RISE with SAP Landscape regardless of approach
- Take Full Control of Your Shared Responsibilities with Full SAP Attack Surface Management and Prioritized Guidance
- Minimize Enterprise Risk, Eliminate Costly Downtime, and Protect Your Most Critical Systems, Wherever They Reside
- Supercharge Your SAP and InfoSec Teams with Superior Threat Intelligence, Expert Knowledge, and SAP Security Best Practices



ONAPSIS

Thank You!!

Addendum

ONAPSIS

Futureproof Your SAP Security Investment with Onapsis

SAP® Endorsed App
Premium Certified

TODAY

- Full Onapsis Platform Support for ABAP and HANA systems on SAP S/4HANA PCE (as well as onPrem)
- Control for Code for HANA supports development in SAP (BTP) Business Application Studio
- Control for Code for ABAP supports scanning ABAP code within SAP-approved code repositories, such as Jenkins and Piper
- Assess scans the full RISE attack surface to prioritize the right list of Security Notes (non-HotNews) to give to SAP to patch

TOMORROW

- Enhancements to the Control product line in FY23, delivering even more support for BTP-focused use cases, such as development, migration, and code movement
- Exploring both internal and SAP-joint opportunities to extend the supported capabilities of the Onapsis Platform for RISE and BTP

OUR VISION

- Onapsis is the premier expert and market leader on SAP application security and compliance.
- Onapsis is committed to supporting our customers' SAP journeys, wherever they take them,
- We are actively enhancing and expanding our portfolio with greater support for the broader RISE with SAP program, together with SAP.
- We focus on areas where we can apply our deep security knowledge, threat research capabilities, and SAP expertise.

Confidential & Proprietary Information of Onapsis
The following information is being shared in order to outline some of Onapsis' current product plans, but it is important to understand that it is being shared for informational purposes only, and not as a binding commitment. Please do not rely on this information in making purchasing decisions because Onapsis makes no representations about future functionality, and ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of Onapsis and is subject to change.

SAP + Onapsis Joint Offerings Deliver Wide Security Coverage for Your RISE with SAP Landscape

Security Solutions from SAP and Onapsis Help Securing Cloud ERP

Value Proposition	Protecting customer data assets	"Always On" threat monitoring with managed security services	Enabling one view of security and compliance
Value Messages	Keep SAP applications safe, run processes in compliance with local legislation, and protect from malicious use	Real-time monitoring of SAP applications to help protect customer crown jewels with dedicated managed security services	Increased confidence in digital transformation and in running cloud ERP
Proof Points	**From SAP** ▪ SAP understands SAP log files best ▪ Any log type can be added SAP and non-SAP ▪ Forensic analysis over months as well as Threat Hunting, Anomaly Detection and User Behavior Analysis ▪ 100% transparent and customizable monitoring use cases ▪ 100% free correlation of all log files to achieve a complete picture of threat situation and anomalies **From Onapsis** ▪ Integrated vulnerability management for standard and custom SAP configurations ▪ Advanced detection rules and zero-day threat detection ▪ Risk and threat intelligence based prioritization ▪ Cyber team and SOC relevant dashboards and interfaces ▪ Extend SAP security controls to network security tools (ex., WAF, NGFW, IPS) **Together** ▪ Securing the source systems and the business processes supporting cloud ERP ▪ Enhanced threat monitoring and vulnerability management	**From SAP** ▪ Cloud provisioning on SAP BTP ▪ Integrated managed security service by SAP experts ▪ 24x7 alerting & 8x5 risk based & prioritized investigation of alerts ▪ Individual adaptable security analysis ▪ Collecting and storing of audit relevant information **From Onapsis** ▪ Onapsis Research Labs team of experts ▪ Threat intelligence feed ▪ Adversary monitoring ▪ Best practices and industry maturity comparisons ▪ Proactive collaboration with SAP Product Security Response team to patch critical vulnerabilities **Together** ▪ Reduce effort for managing cyber threats ▪ Always up to date on new threats, even those just announced ▪ Agile scalable to new source systems, new org units, etc.	**From SAP** ▪ Securing the fundamentals to help ensure confidentiality, integrity, and availability of assets across the technology and physical environments ▪ Customer-focused with an enhanced standard set of security features with default security configurations and extended security offerings across products ▪ Transparent and risk-based to organize, execute, measure, manage, and communicate SAP's current and future cyber states using a risk-based approach, and tie cyber risks to overall business risk prioritization **From Onapsis** ▪ Automated audit and configuration assurance for continuous compliance and optimal execution for go-live ▪ Out of the box compliance templates for major compliance requirements NIST, ISO, SOX, PCI, NERC, HIPAA, GDPR ▪ Customization for automated audit and compliance to other standards or internal controls **Together** ▪ Centralized monitoring of vulnerabilities and threats ▪ Ease the burden of security and enhance security standards with compensating controls. ▪ Joining forces with partners helps us maintain secure solutions for our global customer base

RISE and S/4HANA Cloud: Build In Security. Don’t Bolt On.

$4.12M is the Average Cost of a Failed, Delayed, or Scaled Back Digital Transformation Project

Planning

Common Challenges at This Stage

92% of organizations consider existing customizations as a problem on their path to S/4

35% of organizations expect to face security challenges during their transformation

Overcome Them with Onapsis

- Identify problems in legacy systems and custom code before migrating
- Inventory and baseline all your systems prior to migration
- Make testing as efficient as possible during the project

Implementation

Common Challenges at This Stage

71% of organizations are concerned that the skills deficit will slow down migration

New systems deployed in IaaS environments are exploited in as little as **3 hours**

Overcome Them with Onapsis

- Secure areas of customer responsibility under RISE with SAP
- Validate the custom code work of contractors and SI from QA to Prod
- Monitor for threats in real-time while you build and migrate securely

Post-Deployment

Common Challenges at This Stage

Exploit activity is observed in as little as **72 hours** after a patch is released

$5M: The average annual cost of business disruption due to non-compliance

Overcome Them with Onapsis

- Accurately measure & communicate risk facing new systems over time
- Stay protected against new SAP threats with Onapsis Research Labs
- Stay compliant with automated ITGC testing + SAP PC integration