SAP Security 101: RISE with SAP Cyber-Resilience Fundamentals from Onapsis

Roger Egle, Onapsis Strategic Account Manager for Western Canada

November 2, 2023

Public

ONAPSIS

SAP® Endorsed App
Premium Certified

SAP

Who is SAP's partner 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 · Farm Credit Canada · AMERICA'S NAVY · Schlumberger · SPARTAN CONTROLS · ATB Financial · Pfizer · 3M · AIR CANADA · Levi's

MARKET VALIDATED

Inc. 5000 America's Fastest-Growing Private Companies · 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

"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

Challenges to securing applications and data

600%

Rise in cybercrime since the COVID-19 pandemic[1]

26,000

Cybersecurity incidents per day on average, according to Forbes[2].

ERP systems make an appealing target for hackers

As they run business-critical processes and house sensitive corporate information, which can be used for cyber espionage, sabotage and fraud.

Growth of critical digital assets

Such as applications on the Web and data moving over the Internet of Things, creating a need for greater protection of new digital vectors and attack surfaces.

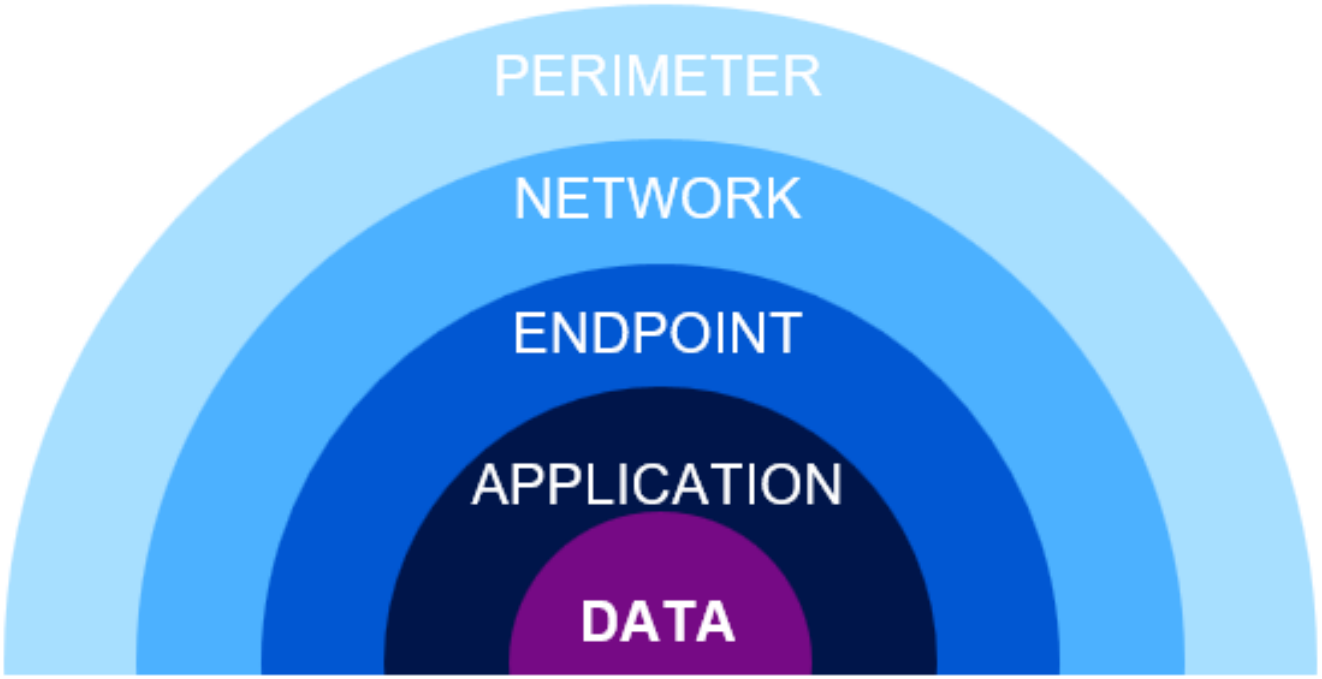
3.4 million unfilled cybersecurity jobs

This skills gap has more than doubled since 2019[3].

Why aren’t typical security efforts effective?

Defense-in-depth models surround, but ultimately neglect that critical application layer.

- **Attacks on the application layer** are the #1 concern of CIOs, which increased YoY
- **Over 70%** say their application portfolio has become **more vulnerable** in the past year
- Almost **two-thirds of organizations have a backlog** of application vulnerabilities



What are examples of consequences if a hacker attack affects an SAP application?

Logistics

- Planning gets delayed
- Confidential partner and customers information (”ship to”) can be lost
- Manipulation of delivery quantity and changes of recipients can occur

Sales and Distribution

- Customers are unable to make purchases
- Credit card, bank details, customer PII, pricing information can be lost
- Modification of business documents & data can lead to a misstatement of the financial books

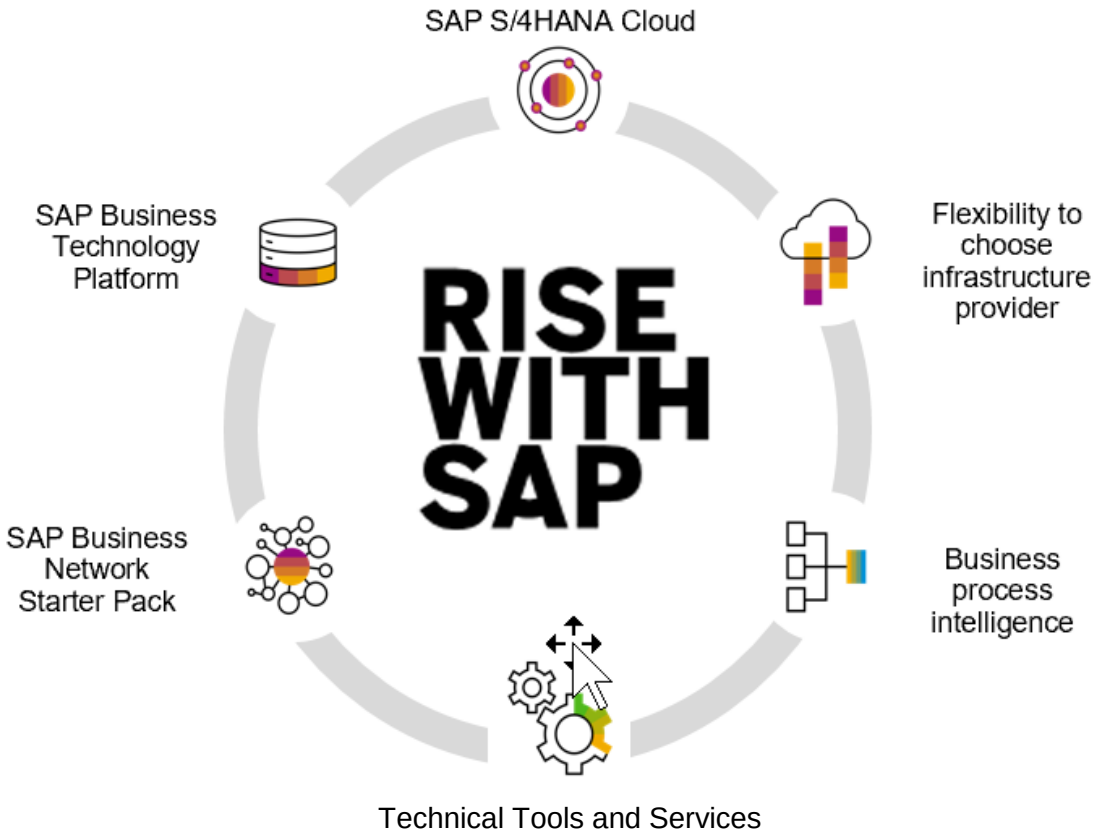
Controlling

- Business units unable to work, business processes can be interrupted
- Loss of pricing and revenue information
- Modification of business documents & data can lead to misstatement of the financial books

Finance and Treasury

- Financial data might not be available therefor decisions based on that information must be delayed
- Revenue information can be lost
- Modification of business documents & data can lead to a misstatement of the financial books

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



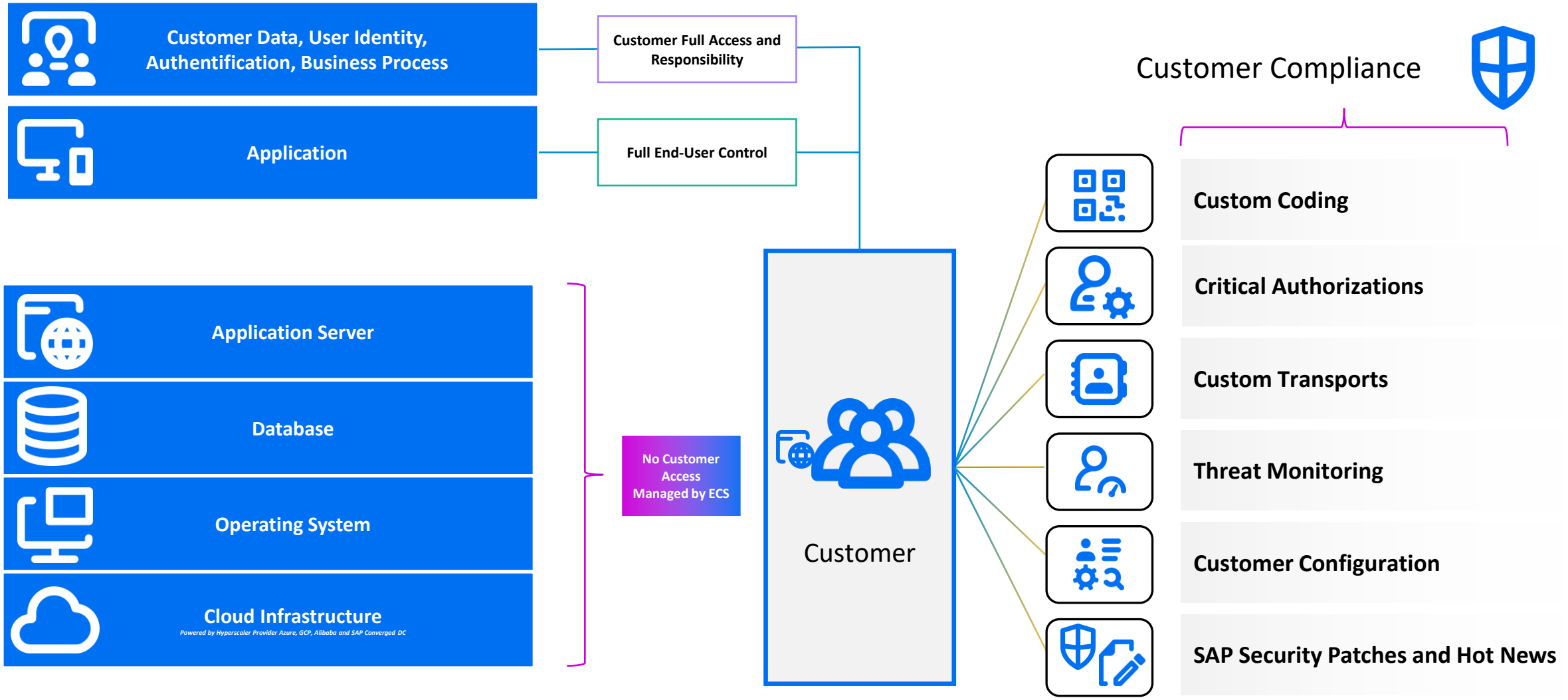
- Designed to facilitate an easier transition to the cloud with less risk, whether greenfield or brownfield or other
- Fundamentally, a “best of” combination of IaaS, PaaS, and SaaS
- Offers a ready-made bundle to guide the digital transformation journey.
- Choose your own hyperscaler, and SAP deploys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

RISE with SAP and Shared Security Responsibility

ONAPSIS

SAP

Shared Security Responsibility within RISE



Customer Security Responsibility & Challenges with RISE

Custom Coding

Most often contains vulnerabilities due to:

- Manual or missing QA
- No proper change management
- Dev teams to take shortcuts
- Missing information during dev.
- Project schedules

Threat Monitoring

- Lack of security and data protection resources and technologies to monitor business applications for anomalies and attacks
- It is very challenging to audit vast amount of logs analyzing user behavior and track hacker activities leading also to compliance issues such as NIS2, KRITIS, GDPR and US Data Privacy Laws

Critical Authorizations

- SAP customer clients must be configured securely with the right user access and authorization levels

Customer Configuration

- Ensuring SAP is configured securely

Custom Transports

- Malicious actors (both internal or external) can infiltrate and manipulate custom or SAP transport requests (i.e., software supply chain) with malicious content and thereby attack the SAP system

SAP Security Patches and Hot News

- Not all security patches < CVSS 9 and also not all hot news are implemented immediately
- Customers need to prioritize and trigger change management process

Customer Security Responsibility Solution Options with RISE

Custom Coding

- Ensure your custom app code (not only ABAP but also HANA-based coding UI5 and Fiori) is clean
- Reduce manual code review saving developer time and money, ensuring projects finish on schedule
- Catch vulnerable code before it becomes a bigger issue

Threat Monitoring

- Less effort handling security recourses, lowering cost of security resources due to shared security service CAPEX vs. OPEX.
- Automation and Machine Learning for continuous auditing, user behavior analysis and anomaly detection.
- Comply with GDPR e.g. Art. 33 (Records of processing activities)

Critical Authorization

- Catch misconfigurations and auth issues before they become bigger problems

Customer Configuration

- Protect against security misconfigurations & misauthorizations
- Gain a deeper understanding of the SAP attack surface - across legacy onPrem and cloud

Custom Transports

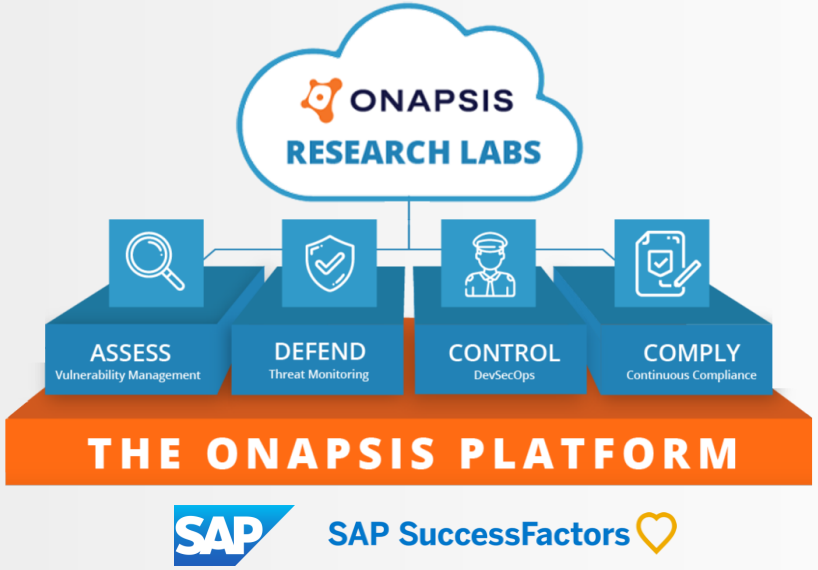
- Continuously scans Transport Requests for malicious content config and coding.

SAP Security Patches and Hot News

- Automate the prioritization of important Security Notes < CVSS 9 that are not automatically applied by SAP (high, medium, low)

ONAPSIS gives the visibility and tools to protect Business Critical Applications

- One common security compliance overview to multiple security disciplines and technologies
- Risk and threat-intelligence-based prioritization of mitigation of vulnerabilities
- Out-of-the-box compliance templates for major compliance requirements NIST, ISO, SOX, PCI-DSS, NERC, HIPAA, GDPR
- Best practices and industry maturity comparisons
- Proactive collaboration with SAP Product Security Response team to patch critical vulnerabilities



Less time to monitor vulnerabilities, less exposure to errors, better reporting

Together: SAP and Onapsis

Protecting customer data assets

- Securing the source systems and the business processes supporting cloud ERP
- Enhanced threat monitoring and vulnerability management

“Always On” threat monitoring with managed security services

- 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

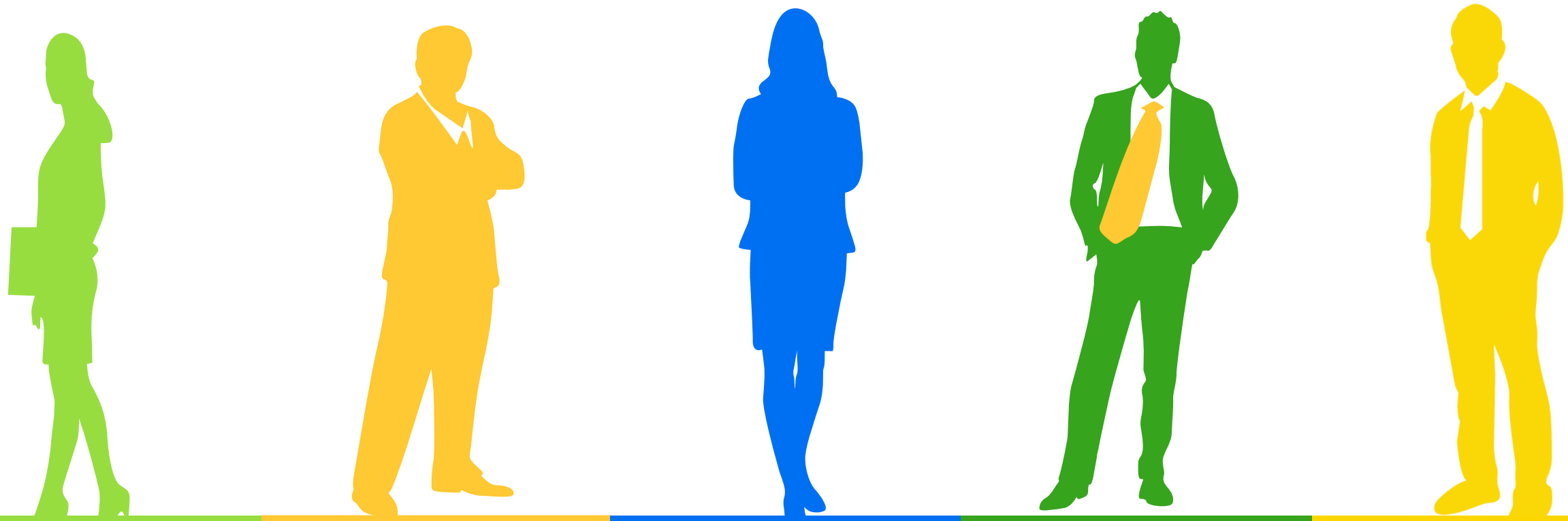
Enabling one view of security and compliance

- Centralized monitoring of vulnerabilities and threats
- Ease the burden of security and enhance security standards
- Joining forces with partners helps SAP maintain secure solutions for our global customer base

In Summary: Accelerating Secure Adoption of SAP Innovations

1. Accelerate transformation to the cloud securely, quickly & easily.
2. Secure SAP DevOps.
3. Protect the Digital Core and Supply Chain.
4. Simplify Audit & Compliance Requirements.

Who is Benefiting from collaboration of SAP and Onapsis?



CISO

How do I identify and manage the biggest risks to the business?

Compliance

How can I measure compliance posture and automate regulatory preparation to compliance standards?

ERP Admin

What actions are needed to ensure the system is running properly?

CIO

How do I ensure operational excellence across all IT processes?

InfoSec

How do I gain visibility and manage threats and vulnerabilities?

Thank You!!