A WEBINAR BY



IT-Conductor

THE FOUR PILLARS OF SAP AUTONOMOUS CYBER OPERATIONS



WEDNESDAY,
AUGUST 5TH, 2026



8:30 AM PDT
11:30 AM EDT
5:30 CEST



HOSTED BY LINH NGUYEN,
CEO, AND CO-FOUNDER OF IT-CONDUCTOR

PART OF A SERIES

Building toward one idea, one session at a time

SESSION 1

Why existing SAP security approaches leave a remediation gap

SESSION 2

Why SAP needs its own cyber operations platform

SESSION 3

Anatomy of an SAP cyber attack

SESSION 4 · TODAY

The Four Pillars of SAP Autonomous Cyber Operations

BEFORE THE FRAMEWORK

Security in silos creates gaps

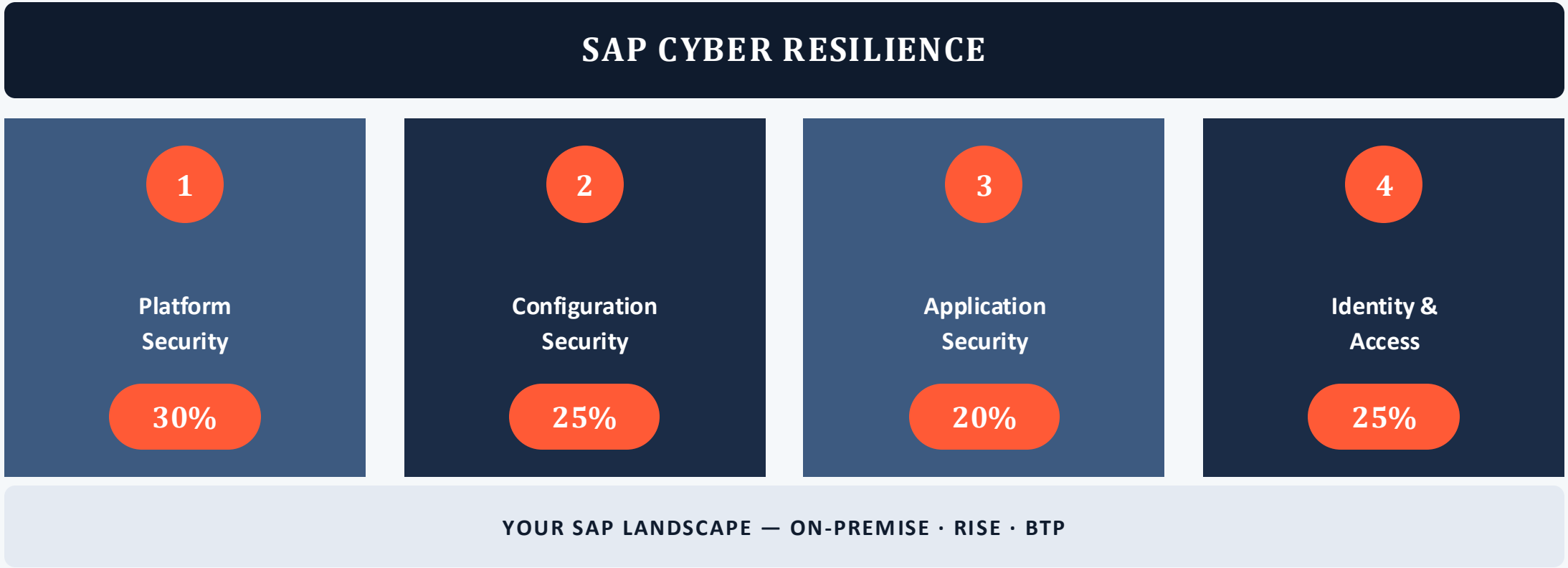
SAP security spans multiple domains. Managing them in isolation creates operational gaps that increase cyber risk.

Infrastructure, configuration, application code, and identity all contribute to resilience. A weakness in any one area can undermine the rest.

Today, we introduce a practical framework for evaluating all four — together.

THE FRAMEWORK

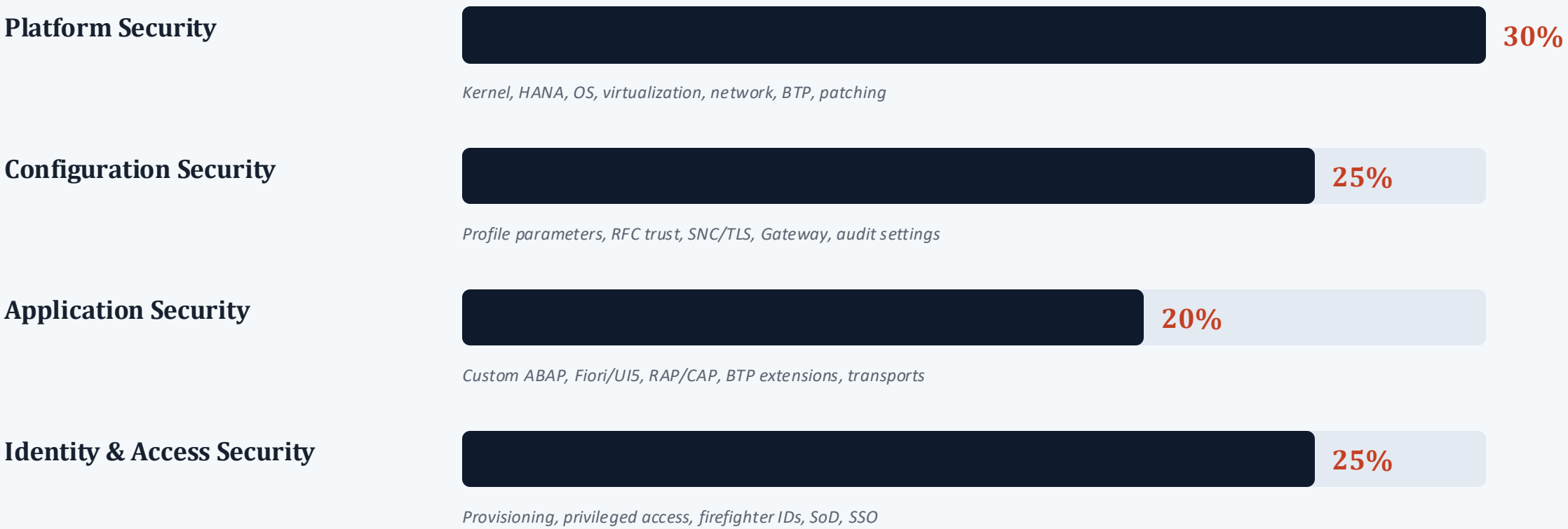
The Four Pillars of SAP Cyber Resilience



Estimated share of SAP cybersecurity risk, shown on each pillar

BY THE NUMBERS

Estimated share of SAP cybersecurity risk



This weighting forms the foundation of the SACO resiliency scoring model.

WHY THE NUMBERS LOOK DIFFERENT

Identity isn't the biggest risk here — and that's unusual

For most enterprise applications, identity represents 40–50% of cyber risk, because users are the primary attack surface.

SAP is different. It's both an application platform and an operating platform for business-critical processes.

A compromise can occur through many non-user vectors:

- Outdated SAP kernel
- Vulnerable ICM / Web Dispatcher
- Insecure RFC destinations
- Weak profile parameters
- Exposed SAPRouter
- HANA vulnerabilities
- Misconfigured trust relationships

As a result, Platform and Configuration Security together account for over half of SAP cyber risk.

PILLAR 1 OF 4

Platform Security

30%

of SAP cyber risk

The infrastructure layer everything else depends on

WHAT IT COVERS

- SAP kernel & HANA patching
- Web Dispatcher & SAP Host Agent
- OS & virtualization
- SAPRouter & Cloud Connector
- Kubernetes & cloud infrastructure
- BTP platform security

TYPICAL TEAMS SAP Basis · Infrastructure · Cloud · Security Operations

WHY IT MATTERS

Unpatched kernel and OS-level vulnerabilities give attackers a way in before any application-level control even applies.

PILLAR 2 OF 4

Configuration Security

25%

of SAP cyber risk

The settings that determine how securely SAP actually runs — often the most overlooked area

WHAT IT COVERS

- Secure profile parameters
- SNC & TLS
- RFC trusted systems
- Gateway ACLs & ICM settings
- Audit logging
- HANA & transport settings

TYPICAL TOOLS EWA · Security Optimization Service · IT-Conductor SecureOps

WHY IT MATTERS

The most common SAP breaches trace back to defaults left unchanged — not exotic exploits.

PILLAR 3 OF 4

Application Security

20%

of SAP cyber risk

Where SAP-specific vulnerabilities live in code and services

WHAT IT COVERS

- Custom ABAP code & custom RFCs
- SQL injection & authorization bypass
- Fiori & OData services
- RAP/CAP & BTP extensions
- Transport governance
- CI/CD security

RESPONSIBLE TEAMS ABAP Developers · DevSecOps · Quality Assurance

WHY IT MATTERS

Generic application security tools don't understand SAP's authorization model or custom code — SecureOps does.

PILLAR 4 OF 4

Identity & Access

25%

of SAP cyber risk

Who can do what — and whether that's still correct

WHAT IT COVERS

- SAP_ALL users & emergency IDs
- Dialog users & service accounts
- RFC users & privileged access
- IAM integration & Entra ID
- GRC Access Control
- SAML & MFA

RESPONSIBLE TEAMS IAM · SAP Security · GRC

WHY IT MATTERS

Over-provisioned access turns a minor compromise into a business-critical incident.

WHY THE FRAMEWORK MATTERS

A gap in one pillar undermines the others

- Strong identity controls don’t help if the kernel is unpatched.
- A hardened OS doesn’t help if authorizations are over-provisioned.
- Clean configuration doesn’t help if custom code has an unchecked vulnerability.

Complete SAP security requires visibility across all four pillars — together, not as four separate tools.

PUTTING THE NUMBERS TO WORK

Mapping to common SAP attack vectors

ATTACK VECTOR	PRIMARY PILLAR
Missing SAP Security Notes	Platform
HANA exploit	Platform
Exposed SAPRouter	Platform
Weak profile parameters	Configuration
Weak SNC/TLS	Configuration
RFC trust abuse	Configuration / Identity
Insecure Integration Suite API	Application / Configuration
Vulnerable ABAP custom code	Application
Malicious transport	Application
Stolen SAP_ALL account	Identity
Privilege escalation	Identity

HOW SECUREOPS RESPONDS

One platform, every pillar

1

Monitor

Continuous visibility into platform, configuration, application, and identity risk across the landscape.

2

Assess

AI-assisted analysis evaluates risk and priority within and across all four pillars.

3

Automate

Governed remediation executes approved fixes, with approval gates and evidence at every step.

PUTTING IT TOGETHER

SecureOps across all four pillars

	MONITOR	ASSESS	AUTOMATE
Platform Security	Continuous vulnerability detection & infrastructure monitoring	Patch-level risk scoring (Patch Tuesday analysis)	Kernel/HANA lifecycle orchestration & automated remediation
Configuration Security	Configuration drift detection	SAP benchmark validation & hardening recommendations	Policy enforcement & continuous compliance
Application Security	Transport governance tracking	Custom code risk assessment	AI-assisted remediation & DevSecOps integration
Identity & Access	Privileged access & anomalous behavior monitoring	SoD integration & emergency access governance	Automated identity risk response

THE TAKEAWAY

“A complete SAP security strategy needs visibility across all four pillars — not four separate tools.”

Whether you’re building a new SAP cyber operations program or maturing an existing one, the framework is the same: Platform (30%), Configuration (25%), Application (20%), Identity & Access (25%) — together.

COMING UP

This is session 4 of the series

SAP AUTONOMOUS CYBER OPERATIONS

More sessions are on the way

We’re continuing to build out SAP Autonomous Cyber Operations as a series — stay registered for details on what’s next.

Watch your inbox for the next session announcement.

TAKE THE NEXT STEP

Begin your SAP Autonomous Cyber Operations journey

Start with an assessment to identify:

- Operational gaps
- Remediation bottlenecks
- Automation opportunities

Request a SAP Security Operations Assessment

Questions?