orca SECURITY

Cloud migration without compromising security

Empowering enterprises to modernize SAP in the cloud with full visibility and security

aws PARTNER

Introduction

Studies show that SAP on AWS customers experience

58%

less downtime, compared to on-premises SAP environments

SAP workloads are moving to the cloud to improve reliability and resilience. In fact, studies show that SAP on AWS customers experience 58% less downtime, compared to on-premises SAP environments.[1] But while many corporate leaders are determined to capture this operational stability, cloud migrations can also come with risks. A lack of security knowledge and system misconfigurations can be a weak point in SAP cloud migration initiatives.

The good news is that modernizing an SAP landscape is the perfect time to rethink security from the ground up. Integrated threat detection and response tools can help organizations stay ahead of threats throughout a cloud migration, while also safeguarding operations well into the future. The SAP migration can be the catalyst for positive business change.

AWS and AWS Partners like Orca Security enable security teams to gain deep visibility into cloud configurations, prioritize and remediate risks, and achieve ongoing compliance across SAP environments. The Orca Cloud Security Platform eliminates the blind spots created by legacy agent-based approaches.

This white paper explores how to protect mission-critical SAP workloads with integrated threat detection and response. It looks at how to enhance detection of risks, simplify investigations, and speed up remediation—all while significantly improving security outcomes.

Security challenges in SAP migrations

Around the world, organizations are under increasing pressure to modernize their SAP landscapes. And it's not just 2027 end-of-support deadlines that are driving SAP migration initiatives. By moving SAP workloads to the cloud, organizations can be more agile, scale effectively, and enable new levels of innovation. Plus, modernization gives teams the rare opportunity to address legacy vulnerabilities and future-proof their security posture.

In fact, a security-first mindset is essential for successful SAP migrations. Afterall, SAP systems power critical functions across finance, operations, and customer experiences—making security a shared priority. Security incidents involving SAP can lead to data loss, regulatory fines, and reputational damage. Recently, 79% of customers cited a lack of security and compliance as the reason why cloud migrations fail.[2]

Securing SAP workloads requires a layered approach that helps mitigate risks across the application, platform, and infrastructure levels. Key strategies include:

- **Strong identity and access management**—enforcing policies of "least privilege access" for SAP roles, as well as multi-factor authentication
- **Network security measures**—isolating SAP workloads in virtual private clouds and filtering traffic with firewalls
- **Data encryption**—protecting sensitive data in transit and at rest using encryption keys
- **Continuous monitoring**—enabling real-time detection of misconfigurations, suspicious behaviors, and policy violations to speed response

AWS works alongside leading security partners to deliver deeper protection for SAP workloads. The reality is that cybersecurity teams are often short-staffed and challenged by alert fatigue, tool sprawl, and lack of visibility across hybrid environments. AWS Partners expand on core AWS security to help teams strengthen their security posture without added complexity. Whether it's agentless scanning, zero trust enforcement, or telemetry tailored to SAP, they help safeguard critical workloads before, during, and after cloud migration.

The AWS culture of security

"Our customers trust us with their most critical assets, and that trust demands action. By delivering comprehensive visibility across SAP workloads in partnership with AWS, we're not just securing data—we're securing futures, ensuring every business can innovate without compromise."

—Gil Geron, CEO, Orca Security

The solution: Integrated threat detection and response

Speed is everything in cybersecurity, and AI-powered solutions can make all the difference in helping organizations respond to incidents faster, reduce risk, and strengthen their overall security posture. Integrated threat detection and response (TDR) solutions use AI models to monitor, detect, and mitigate any potential threats with minimal (or no) human intervention. The unified control spans across an SAP environment and underlying infrastructure (cloud services, identity systems, networking, and more).

Beyond traditional monitoring, TDR solutions can continuously analyze vast streams of data to identify anomalies that could signify novel risks. Responses can then be automated to stay ahead of evolving threats. The solutions also give teams deeper visibility and threat intelligence enriched with SAP insights, enhancing the protection of critical business data.

To safeguard each stage of an SAP migration, consider TDR solutions that include these key capabilities:

- **Real-time monitoring:** Continuous monitoring of the SAP landscape to identify potential issues, based on business risk
- **Threat intelligence:** Integration of external threat feeds to generate alerts about known threats and help accelerate response
- **Behavioral analysis:** Log data analysis and correlation to proactively detect threats in the SAP environment
- **Automated response:** Workflow automation of routine security tasks, such as updating firewall settings or isolating compromised systems
- **Incident reporting and forensics:** Post-incident root-cause analysis and reporting to track the ongoing health of SAP workloads

How it works: Security across the migration journey

Integrated TDR solutions combine signals from SAP logs, AWS-native tools, and cloud-native security tools to strengthen security across cloud and hybrid environments. AI-powered solutions reduce the time to response and remediation to a matter of minutes. The result is not just a stronger security posture—the security of your SAP landscape can be transformed into a competitive advantage.

AWS and AWS Partner solutions are designed from day one to bring intelligence-driven protection to the SAP migration lifecycle. Organizations can count on safeguards for each stage of cloud migration and continued security throughout ongoing cloud operations.

Pre-migration: Prepare for secure operations
Before migrating SAP workloads to the cloud, organizations can use TDR solutions to proactively detect and remediate potential vulnerabilities. This helps create a secure baseline for migration, rather than moving that technical debt to a new cloud footprint.

During migration: Manage risk in the transition
End-to-end security for workloads, users, and data is critical in the SAP migration phase. Using an event-driven architecture, TDR solutions can be automatically deployed as new AWS accounts are created, or cloud instances are launched. This helps ensure assets are monitored and protected in real-time, using AI-accelerated incident response. The latest tools also help enforce consistent guardrails for containerized workloads, serverless functions, and microservices, so teams can modernize with confidence.

After migration: Optimize and scale securely
With SAP-aware protection built into the environment, security teams can manage change and respond to new security incidents, even as the cloud footprint grows. TDR solutions can automate detection and remediation of cloud-native threats. AI-powered workflows enable analysts to quickly interpret alerts, take action, and improve decision-making. With integrated threat intelligence and continuous tuning, organizations can reduce response times and ensure cloud security keeps pace with business growth.

The benefits of strategic partners

From early assessments to long-term optimization, the right partners can strengthen SAP security across the migration journey. AWS and AWS Partners focus on securing infrastructure, data, and access to help you move faster, without compromise.

The Orca Cloud Security Platform addresses the critical challenge of fragmented visibility in cloud environments by delivering an agentless-first approach to comprehensive cloud security. Through its patented SideScanning™ technology, Orca provides deep visibility into cloud configurations, host operating systems, container images, Kubernetes clusters, and open-source components across cloud environments.

Orca transforms threat detection and response by prioritizing risks based on business impact through attack path analysis and its proprietary Unified Data Model, which correlates data from cloud resources, identity and access, external exposure, and threat intelligence sources. Rather than overwhelming security teams with alert fatigue, Orca identifies the most critical attack paths and enables teams to focus on remediating the highest-impact vulnerabilities first.

The Orca Platform accelerates cloud security outcomes through prioritized alerts, AI-driven remediation guidance, and robust bi-directional integrations with ticketing systems like Jira and ServiceNow. Security intelligence reaches the right teams at the right time for efficient remediation and continuous protection.

Command your cloud with Orca Security

By integrating with 100+ AWS services like Amazon GuardDuty and AWS Security Hub, while providing 185+ customizable compliance frameworks, Orca enables security teams to establish a unified platform that identifies assets, detects and prioritizes risks, and monitors compliance gaps. This eliminates the blind spots created by legacy agent-based approaches.

Start your secure migration here

SAP workloads are at the heart of all kinds of essential business operations, and their security is paramount for the business. AWS and AWS Partners can help organizations infuse AI-powered security into SAP migrations, so they can protect user access while reducing attack surfaces and improving visibility. Ultimately, organizations get the peace of mind to operate securely, and stay ready for the path ahead.

Ready for the next steps in your migration journey? Learn how AWS and Orca can help you reduce risk and modernize your SAP landscape today.

[1] Rutten, Peter & Marden, Matthew, "The Business Value of SAP S/4HANA on AWS," IDC, sponsored by Amazon Web Services, August 2023. https://pages.awscloud.com/rs/112-TZM-766/images/PTNR_SAP_IDC_Whitepaper_Aug-23.pdf

[2] Belford, Christopher, "Why Over 75% of Cloud Migrations Fail," EPI-USE Blog, November 25, 2024. https://www.epiuse.com/aws-services/blogs/why-over-75-of-cloud-migrations-fail