SOLUTION BRIEF

Fortinet Secures SAP on AWS

Executive Summary

Many enterprises turn to SAP to improve decision-making and integrate information from customers, supply chains, and vendors to transform business processes with intelligent automation. SAP is a future-ready enterprise resource planning (ERP) system with built-in intelligent technologies, including artificial intelligence (AI), machine learning (ML), and advanced analytics.

AWS provides SAP-certified, cloud-native instance types to give SAP customers the flexibility to lift and shift their SAP landscape to reduce costs or modernize on SAP S/4HANA. AWS became the first cloud to run SAP workloads, and the AWS Migration Acceleration Program (MAP) helps customers accelerate their SAP transformation. A focused SAP security practice provides AWS customers with the confidence to deploy SAP while maintaining a consistent operational model and managing risks. To protect all the data generated by SAP, Fortinet utilizes a holistic approach to secure the entire SAP landscape and strengthen an organization's SAP security posture.

Protecting SAP landscapes is top of mind

Threat actors target SAP systems. With cybercrime expected to cost $10.5 Trillion by 2025 and SAP security updates unable to provide sufficient protection, protected SAP is crucial.[1]

Fortinet protects SAP workloads on AWS

- FortiGate adds Application Control, Intrusion Prevention and segmentation
- FortiADC protects SAP web applications and SAP APIs from malicious web attacks
- FortiWeb WAF protects the SAP Web Dispatcher and adds ML and AI to increase security of SAP landscapes

Support for older versions of SAP

SAP ECC, SAP NetWeaver, SAP Business Suite, ERP, CRM, SCM, Solution Manager and SRM.

Extend Cloud Security to SAP Workloads

Securing the cloud

Cloud security is maintained through a shared responsibility model, and AWS is responsible for protecting the cloud infrastructure that runs the services offered—**security of the cloud**. Customers are responsible for all the services, SAP workloads, applications, and data they use—**security in the cloud**.

The SAP threat landscape is shifting

As organizations upgrade their existing SAP system or convert to S/4HANA, many leverage the cloud for agility and scale on-demand. Enterprises shift their attack surface by adding more cloud services or by managing hybrid environments. SAP Fiori, the web interface, and smart devices connected to SAP are targets for security attacks.

SAP security risks

Cybersecurity uses infrastructure as an entry point to access sensitive data that resides within SAP. Currently, SAP does not provide guidance on infrastructure security, and SAP's Security Baseline Template leaves these problems to the customer to solve.

Secure SAP with holistic coverage

Fortinet natively integrates into AWS, enabling customers to deploy SAP workloads with full security visibility while maintaining centralized management and security automation. By protecting all the data generated within the SAP ecosystem regardless of its location—whether on-premises or AWS, Fortinet centralizes and automates security controls and analytics—making it easier to manage, respond, and automate security for SAP workloads. An organization's SAP security posture is strengthened using Fortinet's extensive threat intelligence, a comprehensive portfolio, and AI/ML security to provide a seamless security experience across the entire SAP landscape.

Focused SAP security practice

A consistent security framework protects all SAP workloads. Fortinet applies AI for faster threat prevention, detection, and response. It protects all SAP data generated by edge devices, endpoint systems, users, applications, databases, and third-party systems on AWS.

Accelerate SAP deployments

Fortinet reduces the time to securely deploy S/4HANA with prepackaged Infrastructure-as-Code templates, enabling the organization to be more agile, to adopt DevOps best practices, and to provide broad protection to your entire SAP deployment.

Built-in technologies

Combat modern threats using AI, ML, and advanced analytics with Fortinet to expedite threat prevention, detection, and response.

Enterprisewide security

Hybrid cloud footprints bring additional complexity and increase the level of effort to manage an extended security domain. Such complexity is resolved through the Fortinet single-pane-of-glass and consistent operating system approach to managing infrastructure regardless of where and on what platform it is deployed. Simplify operations and provide comprehensive security, visibility, and analytics with Fortinet to centralize operations and deliver scale, performance, and resilience for SAP on AWS.

Public cloud deployment flexibility

Organizations use multiple cloud providers to use cloud services best fit for their workload requirements and avoid vendor lock-in. Using a multi-cloud approach protects organizations from potential constraints or substantial costs if they switch cloud providers. 74% of companies are moving apps back and forth between the cloud and on-premises—thus, consistent security across locations is critical for ensuring SAP workloads are protected.

How Fortinet Secures the Intelligent Enterprise

The Fortinet Security Fabric was designed to complement AWS security solutions and protect data generated in SAP against common and emerging threats. All critical assets stay protected with Fortinet security on AWS as IT teams embark on their SAP projects.

By applying the Fortinet Security Fabric, organizations can have a consistent security framework for SAP. The Fortinet Security Fabric, a broad, integrated, and automated cybersecurity framework, extends security policies from on-premises to the cloud and weaves together all operational and technical security facets, creating a consistent structure for the needs of the SAP security landscape.

- **Zero Trust Access**
- **Security-Driven Networking**
- **Adaptive Cloud Security**
- **FortiGuard Threat Intelligence**
- **Fabric Management Center—SOC**
- **Fabric Management Center—NOC**
- **Open Ecosystem**

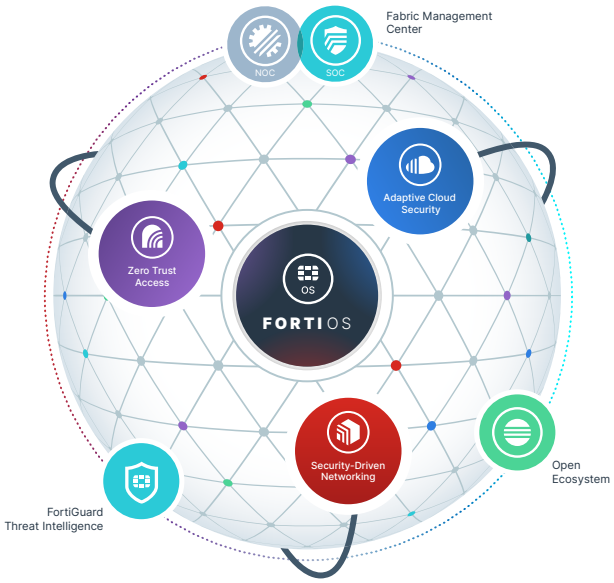

Figure 1: Fortinet Security Fabric diagram.

Fortinet Protects SAP Workloads Running on AWS

The Fortinet Security Fabric provides integrated defenses that span the full SAP attack spectrum to protect all SAP data generated by edge devices, endpoint systems, and SAP workloads. Breaking down the barriers that inhibit security visibility and management allows Fortinet to provide holistic security for SAP workloads. The native integration with Fortinet and AWS enables seamless, automated, and centralized management to support SAP transformation, from lift and shift to modernize on SAP S/4HANA. Organizations can achieve a consolidated view of their security posture across SAP workloads, a single console for policy management and governance reporting, and event monitoring regardless of physical, virtual, or cloud infrastructure.

How FortiADC provides advanced services for SAP

FortiADC is an advanced application delivery controller that enhances SAP applications' security, scalability, and performance. **FortiADC** provides WAF, intrusion prevention system (IPS), SSLi, link load balancing, and user authentication in one solution, whether SAP applications are hosted on-premises or in the cloud.

Dynamic SAP integration

FortiADC secures SAP both with **SAP connector** and by integrating application delivery into the Fortinet Security Fabric. The **SAP connector** gets changes from the SAP Message Server. All SAP web traffic to the SAP Application Servers is protected with end-to-end encryption using the FortiADC.

Simplify setup and management

An intuitive user interface streamlines the configuration of CLI and APIs. Automated configuration gathers information from the SAP ICM configuration (HTTP/HTTPs Ports, virtual hosts, etc.) and additional application server instances. The **SAP connector** provides a topology view of the SAP landscape within the network for easier management and unified visibility for multi-cloud or on-premises SAP deployments.

Advance Security

Policy-based insights into users, behaviors, and data stored in major SaaS applications

FortiCASB is a Fortinet-developed cloud-native Cloud Access Security Broker (CASB) solution designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization. For organizations that comply with regulatory requirements and industry mandates, **FortiCASB** has predefined policies for common regulatory standards to detect violations with actionable recommendations to remediate, along with reports for auditing and tracking. **FortiCASB** monitors malicious traffic, malware and sensitive data, suspicious user activity, and compliance violation with predefined out-of-the-box security policies.

Monitor and track user activity

FortiCASB uses RESTful APIs to integrate directly with SAP Identity Authentication Service (IAS) to monitor and track SAP IAS user activities such as logins, user assignments, updates, etc. **FortiCASB** also integrates with SAP Success Factors using an API-based approach, pulling data directly from SAP Success Factors via RESTful API. Documents are uploaded to determine if malicious and log files reviewed to verify the traffic is valid.

Traffic Analysis and Investigation

FortiCWP uses User Entity Behavior Analytics (UEBA) to look for suspicious or irregular user behavior and sends alerts for malicious behavior. A centralized dashboard displays security events and user activity in real-time to shorten the time to insight.

Fortinet Reference Architecture for SAP S/4HANA

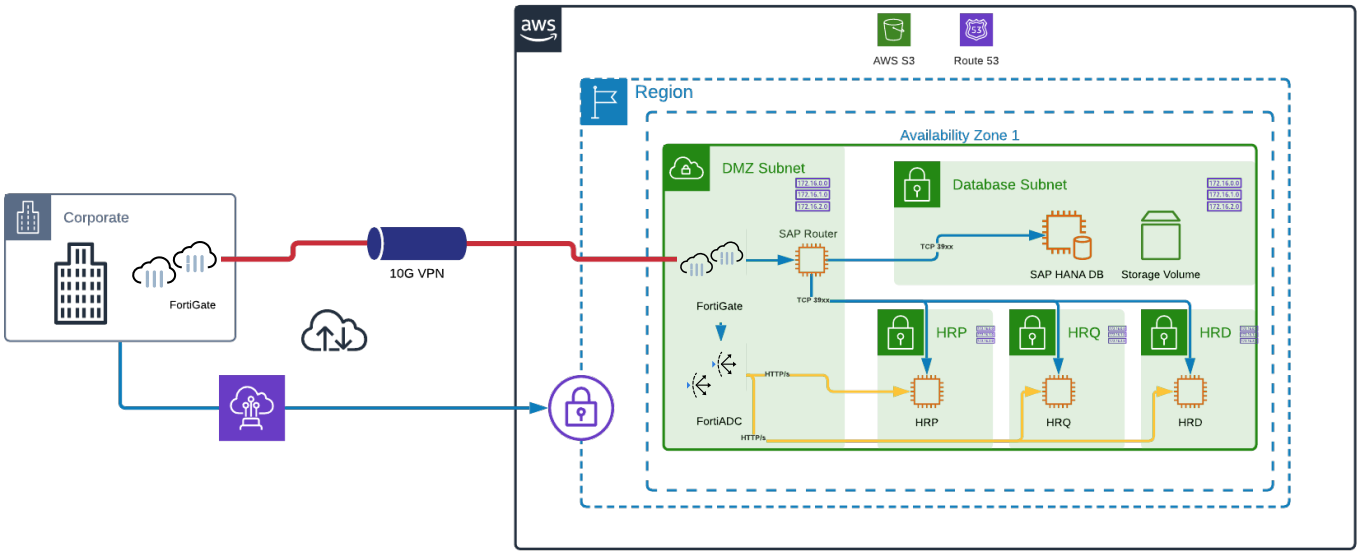

Figure 2: Fortinet reference architecture for SAP S/4HANA on AWS.

Fortinet Use Cases for SAP

Segment SAP workloads with low latency

FortiGate delivers high-performance, low-latency SAP security through the deep packet and content inspection specific to SAP services.

Protect threats targeting SAP with intrusion prevention system (IPS) and content inspection

The **FortiGate**, combined with **FortiGuard Threat Intelligence**, delivers validated industry-leading IPS technology. FortiGuard Labs provides SAP threat intelligence to the FortiGate's IPS engine to protect from well-known and emerging threats.

Provide high-performance SSL inspection

Physical **FortiGate NGFWs** use proprietary hardware acceleration that offloads encryption functions to a security processing unit. This Fortinet-only capability boasts performance advantages of up to 20x that of competitors in the latest-generation devices.

Protect SAP Web Dispatchers

The FortiWeb web application firewall (WAF) is a dedicated HTTP(s) protection platform that not only protects against Open Web Application Security Project (OWASP) threats but also provides virtual patching and auto tuning, and uses AI and ML to detect threats faster.

Evaluate SAP compliance

FortiCWP assesses cloud configuration security posture, detects potential threats originating from misconfiguration of cloud resources, monitors cloud network traffic, and provides comprehensive compliance reports.

Protects web applications

FortiWeb Cloud WAFaaS natively integrates into AWS to protect your hosted web applications without deploying and managing infrastructure.

Enterprise protection for SAP

As organizations embark on their SAP projects, protecting critical systems that contain data from finance, human resources, and other sensitive data is paramount. It becomes incredibly difficult to secure the SAP landscape while the attack surface shifts as organizations use the hybrid, cloud, Fiori, and smart devices.

Fortinet products offer comprehensive security for SAP and help organizations maintain operationally viable and consistent security in a shared responsibility model. Fortinet eases skills gaps and correlates events through ML and workflow automation, multiplying the scale of basis, network, and security administrators. Using Fortinet, organizations can accelerate their SAP projects while providing multilayer security and threat prevention across their entire IT environment.

[1] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime magazine, November 13, 2020.

December 14, 2021 12:59 PM
1150209-A-0-EN