SOLUTION BRIEF

Fortinet Secures SAP on Alibaba Cloud

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.

Alibaba Cloud 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. For years, Alibaba Cloud has been a trusted global technology partner for SAP solutions. Since 2017, over 200 companies have deployed SAP systems including S/4HANA, NetWeaver, HANA, MaxDB, MSSQL, ASE, DB2, Business One, and Data Hub in Alibaba Cloud. The Fortinet/Alibaba Cloud partnership brings enterprise-class security to SAP deployments on Alibaba Cloud.

Fortinet's tested and validated solutions provide 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. Fortinet's security solutions are tied together into a comprehensive security fabric and are backed with world-class security research from Fortinet's renowned FortiGuard Labs.

Extend Cloud Security to SAP Workloads

Securing the cloud

Cloud security is maintained through a shared responsibility model, where Alibaba 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 its Fortinet Security Fabric into Alibaba Cloud, 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 in Alibaba Cloud—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.

The power of FortiGuard Labs

Fortinet's world-famous FortiGuard Labs provides near real-time threat intelligence across Fortinet's entire portfolio of security tools. FortiGuard Labs employs hundreds of skilled security researchers supported by machine intelligence and AI, all relying on data from millions of sensors around the world to stay ahead of the latest threats.

Enterprisewide security

Many firms elect to follow a hybrid cloud model where some applications or even parts of applications are hosted in the cloud while others remain on-premises. Hybrid and multi-cloud models may help protect data or improve performance, but they also add to complexity—and complexity is often at the root of security incidents. Such complexity is resolved through the Fortinet Security Fabric and by employing a 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 Alibaba Cloud.

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 Alibaba Cloud security solutions and protect data generated in SAP against common and emerging threats. All critical assets stay protected with Fortinet security on Alibaba Cloud as IT teams embark on their SAP projects.

By applying the Fortinet Security Fabric, organizations can have a consistent security framework for SAP. The Security Fabric, a broad, integrated, and automated cybersecurity framework, weaves together all operational and technical security facets, creating a consistent structure for the SAP security landscape.

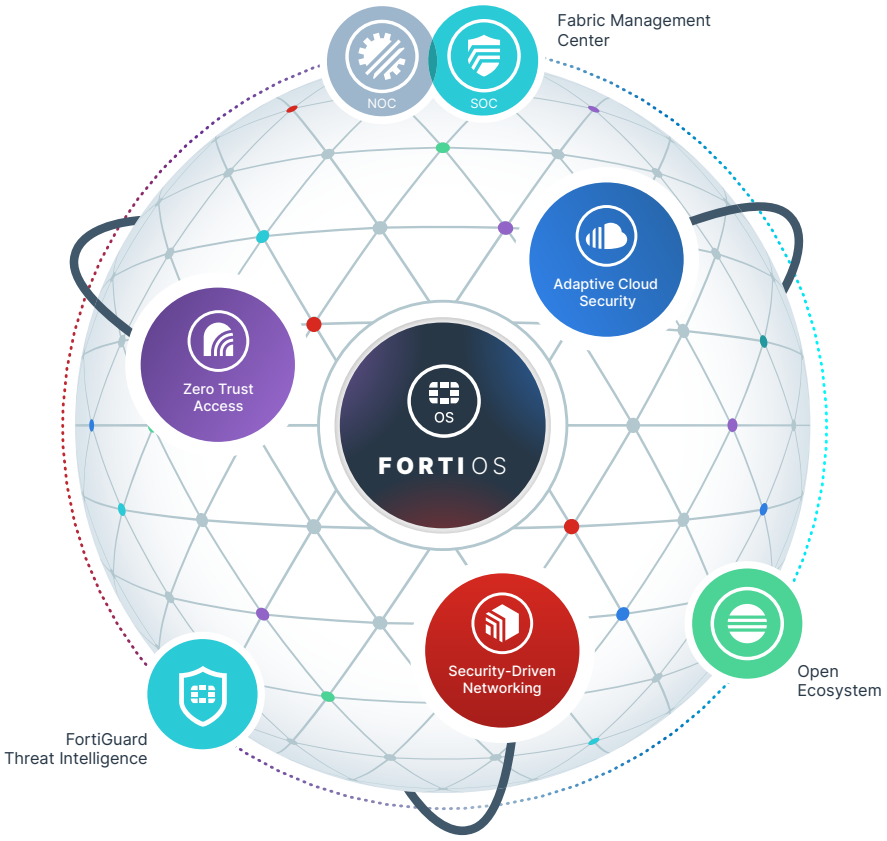

Figure 1: Fortinet Security Fabric diagram.

Fortinet Reference Architecture for SAP S/4HANA

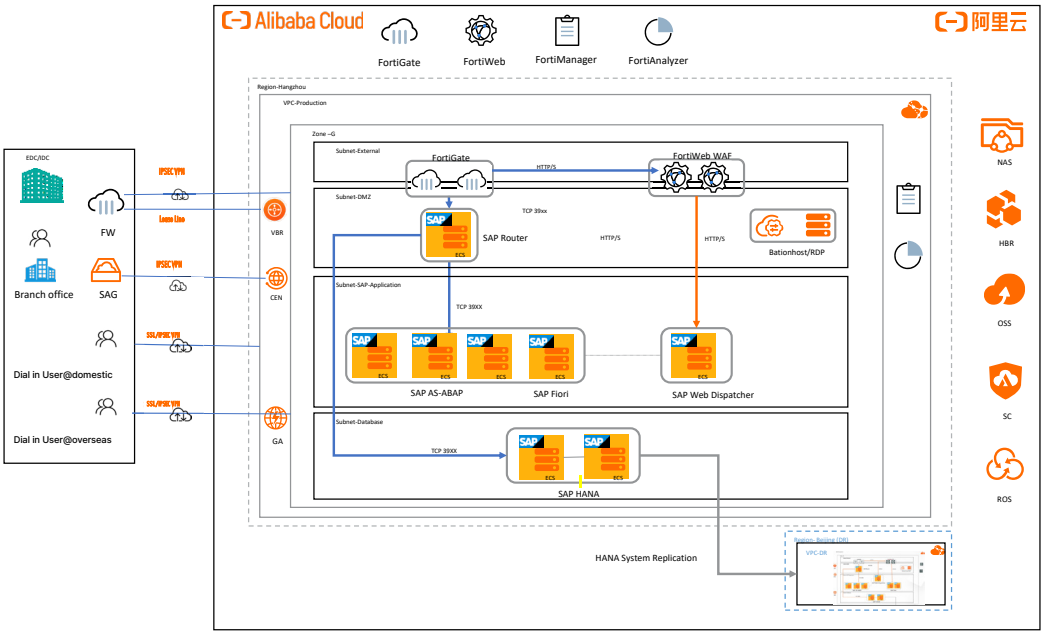

Figure 2: Fortinet reference architecture for SAP S/4HANA on Alibaba Cloud.

Fortinet Protects SAP Workloads Running on Alibaba Cloud

The Fortinet Security Fabric provides integrated defenses that span the full 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 Alibaba Cloud 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.

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.

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 machine learning 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.

March 27, 2021 2:29 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\March\Securing SAP on Alibaba Cloud\sb-FA-fortinet-secures-sap-on-alibaba-cloud-3272021\sb-FA-fortinet-secures-sap-on-alibaba-cloud-3272021

930202-A-0-EN