SOLUTION BRIEF

# Fortinet Provides Advanced Security for SAP Workloads on Google Cloud

## Executive Summary

SAP drives improved business outcomes by organizing, correlating, and monetizing data. Whatever the desired outcome, SAP on Google Cloud increases the value of your data through intelligent process, workflow, and analytics. Whether your priority is redefining the customer experience, attaining operational excellence, or optimizing your supply chain, running SAP on Google Cloud delivers intelligence across the business.

The Google Cloud infrastructure is certified by SAP to ensure high performance and reliability to power SAP workloads. Google Cloud drives agility and efficiency while using modern approaches to incorporate business innovation for SAP workloads. A focused SAP security practice is necessary to protect all the data generated by SAP, and Fortinet utilizes a holistic approach to secure the entire SAP landscape. By leveraging its extensive threat intelligence, a comprehensive portfolio, and state-of-the-art artificial intelligence (AI)/machine learning (ML) security, Fortinet strengthens an organization's SAP security posture.

## Extend Cloud Security to SAP Workloads

### Securing the cloud

Google offers customers a great deal of basic security over their instances, running on its infrastructure. However, according to the shared security responsibility model, Google Cloud is only responsible for protecting the cloud infrastructure that runs all the services offered—basically, the **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 that connect to SAP are targets for security attacks.

### SAP security risks

Cybersecurity uses infrastructure as an entry 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.

## Consistent Enterprise Security for SAP

Fortinet natively integrates into Google Cloud to provide full visibility of SAP workloads. Google Cloud customers can confidently deploy SAP workloads while maintaining centralized management, security automation, and managing risks using Fortinet to secure the Intelligent Enterprise running SAP. By protecting all the data generated within the SAP ecosystem regardless of its location—whether on-premises data center, Anthos, or multiple cloud providers, Fortinet centralizes and automates security controls and analytics—making it easier to manage, respond, and automate security for SAP workloads.

### Focused SAP security practice

A consistent security framework protects all SAP workloads, and Fortinet applies AI for faster threat prevention, detection, and response. It protects all SAP data generated by edge devices, endpoint systems, users, applications, databases, third-party systems on Google Cloud, Anthos, or across multi-cloud environments.

### Accelerate SAP deployments

Fortinet reduces the time to securely deploy S/4HANA with pre-packaged 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 intelligent technologies

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

### Enterprisewide security

The single-pane-of-glass management enabled by the Fortinet portfolio provides a complete and consolidated view of security events for SAP workloads. Fortinet employs built-in intelligent technologies, including AI, ML, and advanced analytics to expedite threat prevention, detection, and response. Simplify operations and provide networkwide security, visibility, and analytics with Fortinet to centralize operations across complex computing landscapes such as SAP.

### Public cloud deployment flexibility

A multi-cloud strategy is being adopted by 84% of enterprises[1] in efforts to reduce exposure to single sourcing and overpayment. Organizations are using hybrid clouds for flexibility in modernizing existing applications. Google's Anthos was built on open-source technology and enables application modernization consistency between on-premises and cloud environments—thus, consistent security across locations is critical for ensuring SAP workloads are protected.

[1] "RightScale 2019 State of the Cloud Report," Flexera, March 2019.

## How Fortinet Secures the Intelligent Enterprise

The different solutions that comprise the Fortinet Security Fabric protect data generated in SAP against common and emerging threats. Fortinet ensures all critical assets stay protected as IT teams embark on their SAP projects. The Fortinet Security Fabric protects all SAP-generated data across multiple locations and regions.

By applying the Fortinet unified portfolio, organizations can have a consistent security framework for SAP across multiple locations and regions. Leveraging the Fortinet Security Fabric, a broad, integrated, and automated cybersecurity framework, it weaves together all operational and technical security facets, creating a consistent structure for the SAP security landscape.

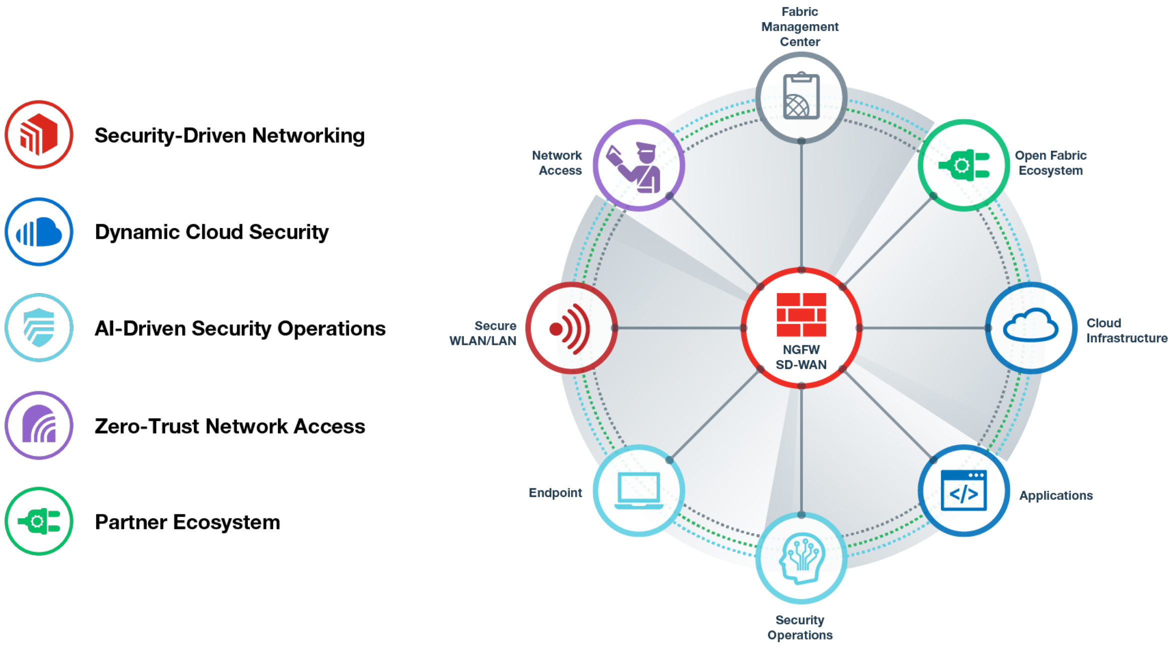

Figure 1: Fortinet Security Fabric diagram.

## Fortinet Protects SAP Workloads Running on Google Cloud

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. Fortinet breaks down the barriers that inhibit security visibility and management across private, public, and hybrid cloud platforms. Native integration with Google Cloud and Anthos enables Fortinet to provide seamless, automated, and centralized management to support SAP deployments.

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 Reference Architecture for SAP S/4HANA

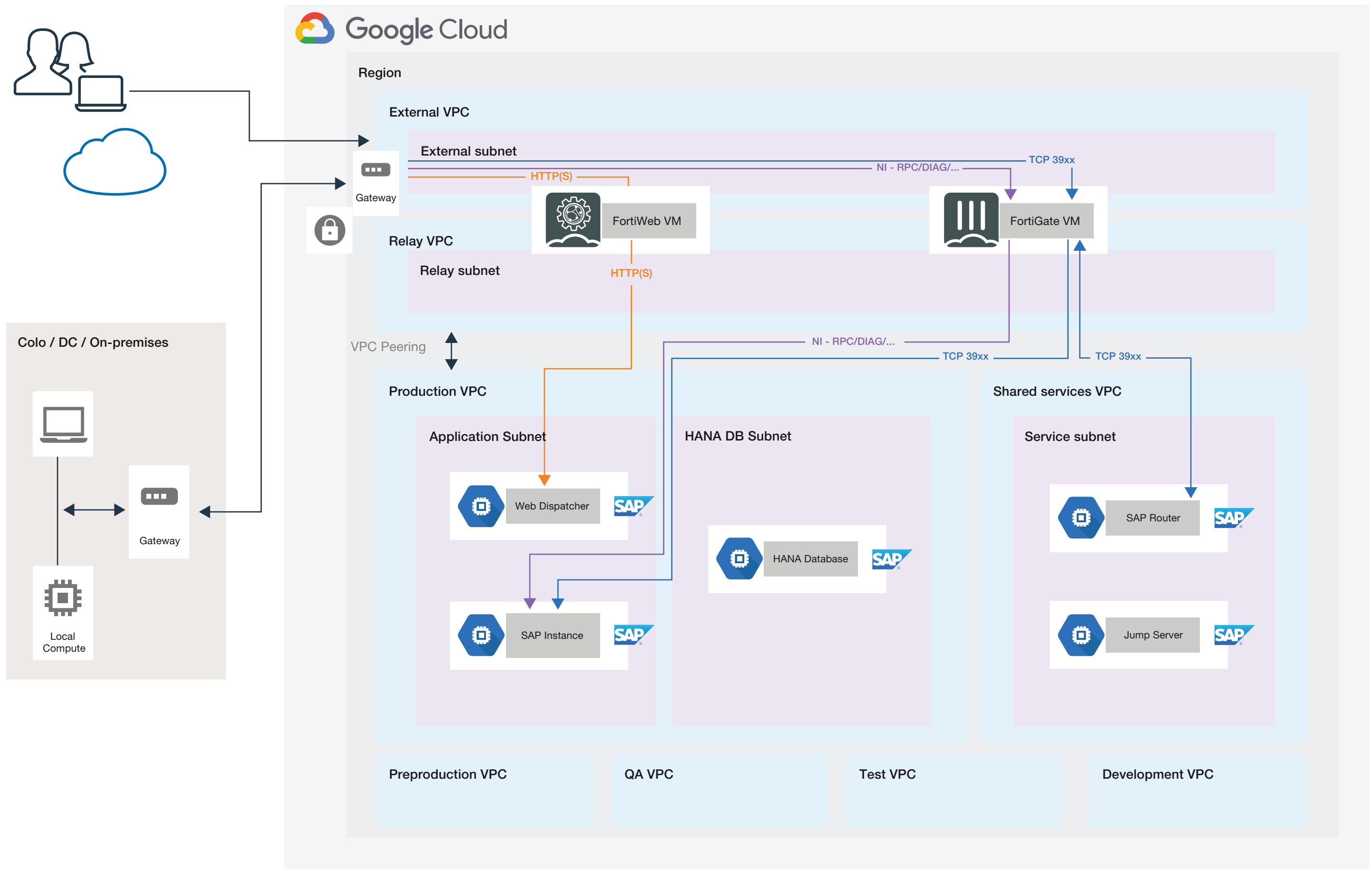

Figure 2: Fortinet Reference Architecture for SAP S/4HANA on Google Cloud.

## 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

Zero-touch deployment with **FortiGate Cloud** simplifies setup and ongoing management while providing centralized configuration and device management. Customizable dashboards and actionable reports display all threats so you can remediate fast. FortiGate delivers broad protection and automated management for consistent enforcement and visibility to protect SAP workloads.

### 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.

## Security for the Intelligent Enterprise

As organizations embark on their SAP projects, protecting SAP 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.

Organizations are using Fortinet to maintain operationally viable, consistent security protection in a shared responsibility model, from on-premises to the cloud. SAP workloads gain comprehensive, advanced security and threat prevention. 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.