SOLUTION BRIEF

Fortinet Provides Advanced Security for SAP Solutions on Google Cloud

Executive Summary

SAP S/4HANA gives you the business agility you need today, with smart automated processes and insight into every corner of your business, so you can move from crisis to opportunity. Business leaders look to SAP to transform business processes for intelligent enterprise. SAP enables organizations to adopt best practices while attaining operational excellence. As organizations upgrade their existing SAP system or convert to SAP S/4HANA, many leverage Google Cloud for reliability and innovation and Fortinet for a holistic approach to security.

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. The Google Cloud infrastructure is certified by SAP to ensure high performance to power SAP workloads. Google Cloud drives agility and efficiency while using modern approaches to incorporate business innovation for SAP workloads. 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.

A focused SAP security practice is necessary to protect all the data generated by SAP, and Fortinet secures the entire SAP landscape whether on-premises, hybrid or multi-cloud. As more organizations embrace a hybrid or multi-cloud strategy, Fortinet provides the security layer across the entire ecosystem. 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.

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 Google Cloud

- 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 Solutions

Securing the cloud

Google offers customers a great deal of 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**.

Flexibility for SAP solutions

Google Cloud and Fortinet have partnered to deliver extensive security orchestration that scales along with cloud workloads. The Fortinet Security solutions complement native Google security functions while supporting secured and encrypted connectivity across public, hybrid and private cloud infrastructure. The Fortinet Security Fabric for Google Cloud protects attack surfaces that span hybrid- & multi-cloud infrastructures providing flexibility for SAP projects.

The SAP threat landscape is shifting

As organizations upgrade their existing SAP system or convert to SAP 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

Cyber threats use 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 SAP 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 powered by FortiGuard Labs, Fortinet's industry-leading cybersecurity research and intelligence organization, to expedite threat prevention, detection, and response.

Application security and edge

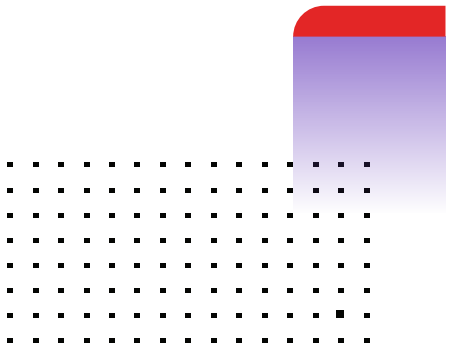
Fortinet enables Zero Trust Security that move defenses from static, network-based perimeters to focus on users, assets, and resources.

Enterprise wide security

The single-pane-of-glass management enabled by the Fortinet Security Fabric portfolio and cybersecurity platform 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 network wide 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 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.



How your SAP workloads are safer with Google Cloud and Fortinet

Together, Google Cloud and Fortinet provide customers with consistent enterprise security protection. Leverage a broad, integrated, automated cybersecurity platform across Google Cloud, multi-cloud, and hybrid environments. Fortinet secures the Intelligent Enterprise running SAP – by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, 3rd party systems in multi-cloud environments, and on-premises.

End to end security from within Google Cloud

- Conceived and built to be natively integrated with Google Cloud
- Complete suite of integrated Firewall, Load Balancing, Threat Analytics and Security Management solutions
- Threat Intelligence, AI-based Threat Detection, Layer 7 Application Inspection, High Performance and Multi-Layer Advanced Security

Consolidation and simplification

- Provides new and existing Google Cloud customers with greater visibility, protection, and control of their entire IT environment through a “single pane of glass”
- Enhances Google Cloud so organizations can manage their portion of the Shared Responsibility Model
- Lowers total cost of ownership (TCO)

Fortinet Security Fabric helps SAP customers to:

- Meet best practice security standards
- Gain visibility and monitor enterprise IT environment
- Comply with ever changing regulatory landscape
- Reduce risk and security complexities
- Simplify and automate operations
- Extend security policies from on-premises to the cloud

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 platform, it weaves together all operational and technical security facets, creating a consistent structure for the SAP security landscape.

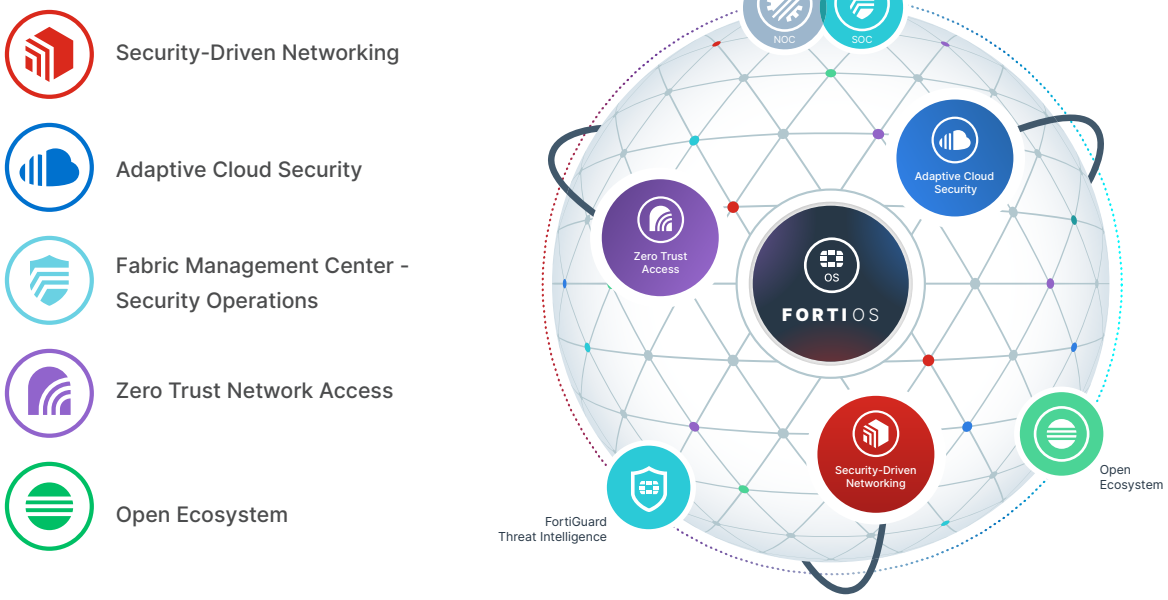


Figure 1: Fortinet Security Fabric diagram.

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.

Integration with Google Cloud's Security Command Center

Fortinet's FortiCWP integrates with Google Cloud's Cloud Security Command Center to improve IT efficiency using familiar tools to manage workloads and view security threats.

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**.

Enterprise Security for Google Cloud

- Simplify security management with single-pane control across Google Cloud and on-premises data centers
- Gain cloud-native visibility and control into your Google Cloud workloads and applications
- Leverage Fortinet Cloud Security Services Hub for scalable and multi-layer secure connectivity
- Security offerings in VM, and SaaS form factors

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.

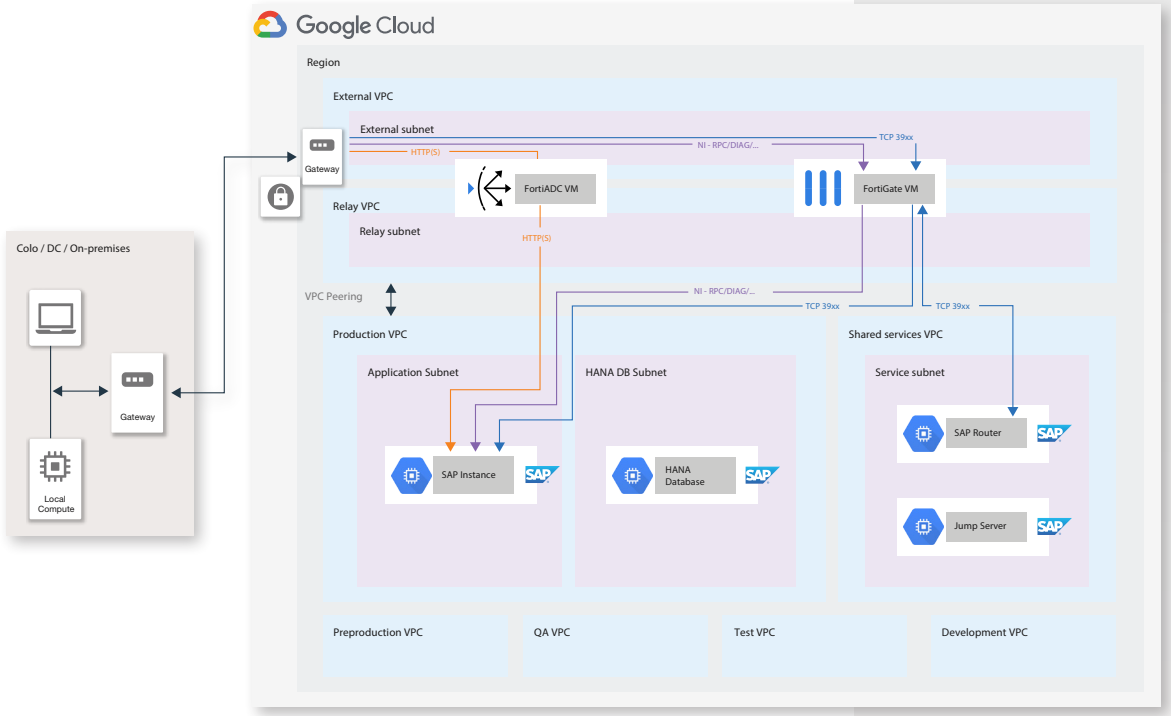
Support for Anthos

Fortinet and Google Cloud provide organizations a flexible deployment model to SAP S/4HANA using a hybrid cloud deployment model with Anthos. Customers who are transforming their business can use SD-WAN as an onramp with Google Cloud. The Fortinet Security Fabric provides multi-layer protection and operational benefits for securing SAP workloads across hybrid environments for the cloud journey to SAP S/4HANA on Google Cloud.

A secure path to Google Cloud

As organizations plan for SAP S/4HANA migrations they often identify additional workloads to migrate to the cloud. The Fortinet and Google Cloud partnership provide customers with a secure path to Google Cloud to support all workload migrations. The Security Fabric offers Network, Application, and Cloud platform security capabilities provided in a variety of form factors including VM-, container-, and SaaS delivered protection that natively integrates Fortinet security functionality into Google Cloud.

Fortinet Reference Architecture for SAP S/4HANA



Fortinet on Google Cloud 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. **FortiGate NGFW** leverages AI/ML & Google data analytics for better business agility - Google core data analytics assets: Dataflow, Datalab, BigQuery.

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. Common exploits such as relay attacks, remote command execution, SQL injections in SAP NetWeaver ABAP and Java and other services are mitigated with microsecond latency. Configuration errors are minimized as SAP heuristics, and signatures are enabled in the default IPS policy.

IPS Signatures for SAP

Year after year, Fortinet has been reported as a standout leader in next-generation IPS through independent studies such as those by NSS Labs and Virus Bulletin. Fortinet's catch rate for exploit and exploit evasion attempts is among the highest in the industry.

Fortinet Key Facts

Fortinet, Inc. provides cyber security solutions to a range of enterprises, service providers and government organizations across the world. **Its "Fabric Ready" network security solutions consist of cloud, virtual and physical platforms, which provide integrated security and networking functions** to protect data, applications and users from network-and content-level security threats

The data below is based on 2020 facts.

- 4 Gartner Magic Quadrants as Leader/Visionary
- #1 Units Shipped, Security Appliances
- Over 500,000 Customers
- HQ Location: Sunnyvale, CA USA
- Employees: >9,700
- Revenue: >$2.5B Growing
- Website URL: www.fortinet.com
- Google Cloud Premier and Co-Sell Partner

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 Fortinet Application Delivery Controller (ADC) is a dedicated load balancing platform providing HTTP(s) protection that not only protects against Open Web Application Security Project (OWASP) threats but also provides virtual patching and auto tuning. It can replace the SAP Web Dispatcher.

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.

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.

Evaluate SAP compliance

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

Protects web applications

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

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.

A secure path to Google Cloud

Reduce your security risk and protect your workloads as you migrate to Google Cloud. The Fortinet cloud security for Google Cloud provides consistent, enterprise security to Google Cloud-based environments.

- FortiCWP provides comprehensive security through integrations with Google Security Command Center
- Improve IT efficiency using familiar tools to manage workloads and view security threats
- Advanced security and threat protection with SD-WAN Cloud onramp for branch office
- Reduce risk from advanced threats by accessing the latest threat intelligence and sharing information in real-time
- Secure branch office access to Google cloud with Fortinet SD-WAN
- Dynamic security from the edge to the cloud
- Run your applications anywhere using consistent security with universal security management pane for flexible workload deployments
- Google SaaS web protection with FortiWeb Cloud WAFaaS
- A SaaS implementation of WAF protects Google Cloud workloads against sophisticated attacks

Security for the Intelligent Enterprise

As organizations move their SAP solutions to Google Cloud, protecting SAP systems that contain data from finance, human resources, and other sensitive data is paramount. The attack surface shifts as organizations use hybrid, multi-cloud, Fiori, and smart devices and it becomes incredibly difficult to secure the SAP landscape.

Organizations can rest assured running Fortinet on Google Cloud will provide the security protection they need to maintain operationally viable, consistent security protection in a shared responsibility model, whether on-premises, hybrid or in 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 SAP 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.

FORTINET

www.fortinet.com

December 13, 2021 10:46 AM
123456-0-0-EN