SOLUTION BRIEF

Fortinet Cloud Security for Google Cloud

Executive Summary

Organizations are modernizing their IT operations to develop applications faster and accelerate time to innovate to maintain their competitive position in the digital innovation era. Google Cloud provides customers with modern tools to enable business innovation. However, cloud computing expands the digital attack surface across hybrid and multi-cloud infrastructures. The Fortinet Security Fabric offers organizations comprehensive security solutions to address the expanding attack surface with integrated network, application, and cloud security in one platform.

Fortinet's approach natively integrates security with Google Cloud, offering a broad set of security solutions and ultimately enabling streamlined management and automated security operations. This gives Google Cloud customers the flexibility to run any application on Google Cloud or on-premises, while maintaining consistent security everywhere.

Advanced Security for Google Cloud

Fortinet Cloud Security for Google Cloud provides consistent, best-in-class enterprise security across on-premises, data centers, and cloud environments. Fortinet Cloud Security offers network, application, and cloud-native security capabilities in various form factors, including virtual machine (VM) and Software-as-a-Service (SaaS). In each instance, Fortinet security functionality is natively integrated into Google Cloud.

Google offers customers various essential security tools to address the security of the Google Cloud infrastructure. However, as much as these tools provide effective security capabilities for basic needs, they introduce a great deal of operational overhead for application development teams looking to build new capabilities and introduce products to market rapidly. Further, according to the shared security responsibility model, Google Cloud is only responsible for protecting the cloud's physical infrastructure, isolating tenants, and keeping their services running.

Customers are responsible for securing applications they build in the cloud and the services they consume. Because securing cloud resources is complex and varies by cloud provider, cloud security failures are typically the customer's fault.

Fortinet Cloud Security for Google Cloud helps organizations maintain a consistent security posture in a shared responsibility model, from on-premises to the cloud. It delivers comprehensive, multilevel security and threat protection to improve an organization's security posture and reduce misconfiguration.

Challenges

The 2025 Fortinet Cloud Security Report reveals that cloud security remains a high concern despite increasing cloud adoption. Ninety-two percent of organizations stated that they have moderate to extreme levels of concern about their public cloud environment security posture.[1]

Enterprise security for Google Cloud

Enable performance and agility with comprehensive, advanced security and threat prevention from on-premises to the cloud.

Secure everything from code to cloud

Manage risk, rapidly detect and respond to active threats, boost developer productivity, and increase security effectiveness with Lacework FortiCNAPP.

Continuous visibility and real-time malware protection with FortiEDR and Google CloudSecurity Command Center

Improve IT efficiency using familiar tools to manage workloads and view security threats.

Advanced network security and threat protection

Reduce risk from advanced threats by accessing the latest threat intelligence from FortiGuard Labs. Secure branch office access to Google Cloud with FortiGate Secure SD-WAN and Network Connectivity Center (NCC) Integration.

Key considerations include data security and privacy, configuration management, access control and identity management, and threat detection and mitigation. As more organizations use two or more cloud providers or a hybrid cloud infrastructure, the complexity of these challenges compounds. Accordingly, it's understandable why 97% of organizations say it would be helpful to have a single cloud security platform to configure and manage security policies consistently and comprehensively across their cloud environments.[2]

The Fortinet Security Fabric answers this need, providing continuous security from on-premises to multiple clouds to protect Google Cloud users.

How the Security Fabric Complements Google Cloud Security

Key capabilities of the Fortinet Security Fabric for Google Cloud include:

- **Single-pane control and management**

  Both cloud and on-premises Fortinet Security Fabric resources can be managed from Google Cloud. This simplicity helps eliminate human errors while reducing the time burden on limited IT resources.

- **Security from code to cloud**

  Lacework FortiCNAPP unifies fragmented tools into a single platform to simplify and strengthen cloud security. It empowers teams to maximize their impact on security with minimal time and effort by automatically connecting risk insights with runtime threat data, ensuring they prioritize and address the most critical security risks and active threats.

- **Single-vendor SASE**

  FortiSASE is a single-vendor SASE solution. It integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge (SSE) to extend the convergence of networking and security from the network edge to the remote workforce. FortiSASE enables secure access from anywhere to the web, cloud, and applications everywhere.

- **Protection from zero-day attacks**

  Secure applications from the edge to the cloud with access to the latest threat intelligence to provide highly scalable zero-day attack protection fully integrated into Google Cloud. The FortiGuard Labs global security research team has over 215 dedicated experts. Artificial intelligence (AI) and machine learning (ML) systems gather and analyze over 100 billion security events daily.

Google Cloud
INFRASTRUCTURE MODERNIZATION
Partner of the Year
Networking
2025

Google Cloud
TECHNOLOGY
Partner of the Year
Security — Infrastructure
2024

Google Cloud
TECHNOLOGY
Partner of the Year
Security — Application
2024

- **Fabric Connectors**

  Fabric Connectors enable open integration of the Fortinet Security Fabric to automate firewall and network security insertion into Google Cloud with multiple existing components within a customer's ecosystem. It also allows for the integration of security intelligence services from Google Cloud.

Protect the Full Attack Spectrum

Fortinet breaks down the walls that inhibit security visibility and management between and across on-premises and cloud environments. These solutions are designed to improve an organization's security posture and increase end-user confidence in Google Cloud environments.

Product	Description
Bring your license (BYOL)	Licenses purchased from a Fortinet channel partner for different products are transferable across platforms.
Pay-as-you-go (PAYG)	Fortinet lists many solutions that can be consumed using a PAYG on-demand usage model from the Google Cloud Marketplace. Additionally, many products with free trials can easily be continued with PAYG pricing.
Private offer	With private offers, you can simplify the procurement cycle and unlock discounts for SaaS products and VM images directly from Google Marketplace.
Available on the Google Cloud Marketplace as part of the Fortinet Security Fabric for Google Cloud	
FortiGate Next-Generation Firewalls (NGFWs) and SD-WAN (BYOL, PAYG)	FortiGate provides flawless convergence that can scale to any location: remote office, branch, campus, data center, and cloud. Using APIs, FortiGate is infrastructure-aware, enabling the configuration of high-availability environments automatically to create failover scenarios. FortiGate VM delivers integration with Google Cloud's Network Connectivity Center (NCC). NCC bridges a first-party native-cloud underlay from Google Cloud with secure SD-WAN and cloud on-ramp service from Fortinet across hybrid and multi-clouds.
FortiWeb (BYOL, PAYG)	Deployed as a VM, FortiWeb protects web applications and APIs from attacks that target known and unknown vulnerabilities, including the OWASP Top 10, zero-day threats, and other application-layer attacks.
FortiAppSec Cloud WAF-as-a-Service (SaaS)	Delivered as SaaS, FortiAppSec Cloud includes bot mitigation and API discovery and protects public cloud–hosted web applications from the OWASP Top 10, zero-day threats, and other application-layer attacks.
Lacework FortiCNAPP (SaaS)	Lacework FortiCNAPP offers cloud and security operations teams reduced complexity, greater visibility, and enhanced security effectiveness all through a unified, AI-driven platform.
FortiFlex (private offer)	FortiFlex is a points-based cybersecurity licensing program that allows organizations to provision the services and solutions they need on-demand easily. With FortiFlex, organizations are freed from having to preplan and presize their deployment purchases and risk under-sizing or over-sizing their solutions. Instead, organizations simply purchase packages of FortiFlex points that can then be used to deploy any solution size, in any quantity, and with any service.
FortiSASE (private offer)	FortiSASE offers a comprehensive set of security capabilities, including secure web gateway (SWG), universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), and Firewall-as-a-Service (FWaaS).
FortiManager (BYOL)	FortiManager provides single-pane-of-glass management and policy controls across the extended enterprise for insight into networkwide, traffic-based threats. This includes features to contain advanced attacks and scalability to manage up to 10,000 Fortinet devices.
FortiAnalyzer (BYOL)	This solution collects, analyzes, and correlates data from Fortinet products for increased visibility and robust security alert information. Combined with the FortiGuard Indicators of Compromise Service, it also provides a prioritized list of compromised hosts to allow rapid action.
FortiADC (BYOL, PAYG)	FortiADC optimizes application performance using unmatched load balancing and web security. It provides global server load balancing, link load balancing, and user authentication to deliver availability, performance, and security for enterprise applications.
FortiEDR (PAYG)	FortiEDR brings MITRE ATT&CK–proven behavior-based endpoint detection and response (EDR) technology to protect Google Cloud workloads. FortiEDR reduces the attack surface, detects and defuses attacks in real time, and supports various customizable automation steps to remediate policy violations.
FortiDevSec (PAYG)	FortiDevSec is an application security testing product that offers comprehensive SaaS-based continuous application testing for software developers and DevOps without any security expertise. Comprehensive testing is included for SAST, SCA, containers, IaC, Secrets, DAST, and more.
FortiSandbox (BYOL)	FortiSandbox for Google Cloud Platform enables organizations to defend against zero-day threats natively in the cloud, working alongside network, application, email, endpoint security, and other third-party security solutions or as an extension to their on-premises security architectures to leverage cloud elasticity and scale.
FortiMail (BYOL)	FortiMail VM is a complete secure email solution that protects against inbound attacks, including advanced malware, outbound threats, and data loss, with a wide range of top-rated security capabilities. It includes powerful, built-in spam, phishing, malware, and ransomware protection capabilities.

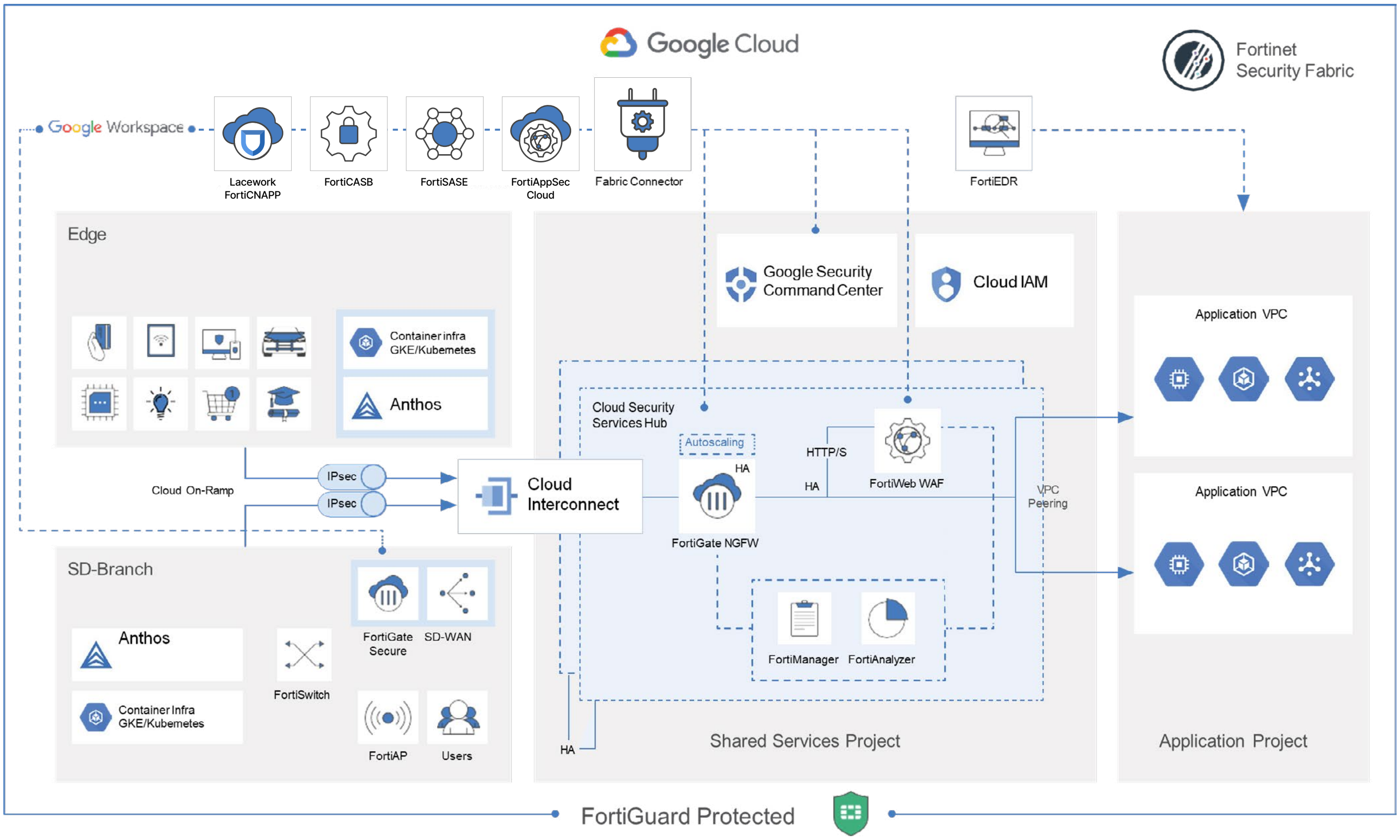

Figure 1: Google Cloud reference architecture

Use Cases for Extending the Fortinet Security Fabric to Google Cloud

The Fortinet Security Fabric supports a spectrum of Google Cloud–based enterprise use cases, such as:

1. Network security

Implement scalable and multilayer security using a cloud security services hub. Leverage the scale and flexibility of the Google Cloud infrastructure to build effective and low-friction security solutions.

- Distributed enterprise/SD-WAN
- Hybrid cloud
- VPC-to-VPC segmentation
- Remote access
- Perimeter security for GKE clusters

2. Application and web traffic security

Protect business-critical applications from known and unknown threats, including zero-day, botnet, and API attacks. Also, mitigate the risk from server vulnerabilities and support compliance with the latest laws, regulations, and standards.

- Cloud-native application protection
- API security for Apigee
- Web application security
- Regulatory compliance
- Risk management
- Bot defense

3. Endpoint protection

- Google Cloud workload protection
- Risk mitigation policy control
- Next-generation antivirus capabilities
- Real-time, automated breach protection
- Incident response orchestration
- Global 24×7 managed EDR and managed detection and response

Enterprise Protection to Reduce Risk

Fortinet Cloud Security for Google Cloud helps organizations maintain operationally viable, consistent security protection in a shared responsibility model, from on-premises to the cloud. It delivers comprehensive, advanced security and threat prevention capabilities for Google Cloud users. Continuous control and visibility through a single pane of policy management reduce security complexity. With Fortinet Cloud Security, leaders can rest assured that their security architectures cover the entirety of the network attack surface and that their sensitive data is compliant and secure.

[1] 2025 State of Cloud Security Report.