

Fortinet Dynamic Cloud Security for Google Cloud Platform

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. Cloud computing expands digital attack surfaces across hybrid and multi-cloud infrastructures. The Fortinet Security Fabric offers organizations a comprehensive set of security solutions to address the expanding attack surface that spans hybrid cloud infrastructures. Doing so provides them with integrated network security, application security, and cloud platform security in one platform. Fortinet's approach natively integrates security with Google Cloud Platform (GCP), offering a broad set of security solutions and ultimately enabling streamlined management and automated security operations. This gives GCP customers the flexibility to run any application on GCP or on-premises, while maintaining consistent security everywhere.

Consistent Enterprise Security Protection—from On-premises Data Centers, to the Cloud, to the Branch

Fortinet Dynamic Cloud Security for GCP provides consistent, best-in-class enterprise security. The Fortinet Security Fabric protects business workloads across on-premises, data centers, and cloud environments—providing multilayered security for cloud-based applications. Fortinet Dynamic Cloud Security offers network, application, and cloud platform security capabilities in a variety of form factors, including virtual machine (VM), container, and Software-as-a-Service (SaaS) form factors. In each instance, Fortinet security functionality is natively integrated into GCP.

Google offers customers a variety of basic security tools to address GCP security needs-based compute infrastructure. However, as much as these tools offer good security capabilities for basic needs, they introduce a great deal of operational overhead for application development teams looking to rapidly build new capabilities and introduce products to market. Further, according to the shared security responsibility model, GCP is only responsible for protecting the cloud infrastructure, isolating tenants, and keeping their services running. Customers are responsible for securing applications they build in the cloud and the services they consume. Since securing cloud resources is complex and varies by cloud provider, cloud security failures are typically the fault of the customer. Fortinet Dynamic Cloud Security for GCP helps organizations maintain 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 overall security posture and reduce misconfiguration.

Expanding Threat Landscape

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-cloud infrastructure for flexibility in modernizing existing applications.¹ Google's Anthos extends Google compute services to on-premises data centers and edge locations. Anthos is built on open-source technology and enables application modernization consistently between on-premises and cloud environments. Google's leadership to open standards like Kubernetes container orchestration enables business innovation and pricing to optimize cloud spend, combining the best of on-premises and public cloud compute capabilities. Fortinet Dynamic Cloud Security provides continuous security from on-premises to multiple clouds to protect GCP users.

Enterprise Security for Google Cloud Platform

Continuous threat visibility within FortiCWP and Google Cloud Security Command Center

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

Advanced security and threat protection

Reduce risk from advanced threats by accessing the latest threat intelligence and sharing information in real time. Secure branch office access to GCP with FortiGate Secure SD-WAN.

Dynamic security from the edge to the cloud

Run applications anywhere using consistent security with a universal security management pane for flexible workload deployments.

How the Security Fabric Complements Google Cloud Security

The Fortinet Security Fabric offers multilayer protection and operational benefits for securing business workloads across on-premises, data center, and cloud environments. 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 GCP. This simplicity helps eliminate human errors while reducing the time burden on limited IT resources.

- **Cloud-native visibility and control**

Reduce misconfiguration using centrally managed security from within FortiCWP cloud workload protection (CWP). Minimize the time burden on limited IT resources by viewing threats and developing reports directly from within FortiCWP.

- **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 that is fully integrated into GCP.

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.

- **Compliance ready**

Obtain insights with actionable instant security reports on targeted attacks. Meet compliance regulations for industry standards such as Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), as well as data privacy laws such as the European Union's General Data Protection Regulation (GDPR).

Protect the Full Attack Spectrum

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

They are also available via flexible procurement options:

- **BYOL**

Licenses purchased from a Fortinet channel partner for different products are transferrable across platforms.

- **PAYG**

Fortinet solutions like FortiGate next-general firewall (NGFW) and FortiWeb Cloud WAF-as-a-Service can be consumed using a pay-as-you-go (PAYG) on-demand usage model from the Google Cloud Marketplace.

The following products are available as part of the Fortinet Security Fabric for Google Cloud:

- **FortiGate NGFW (BYOL, PAYG)**

Delivers the industry's best threat protection capability sets to defend against advanced known and unknown cyberattacks. Using APIs, FortiGate is infrastructure aware, enabling the configuration of high-availability (HA) environments automatically to create failover scenarios.

- **FortiWeb Cloud WAF-as-a-Service (SaaS PAYG)**

Delivers security using a SAS-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero-day threats, and other application layer attacks.

- **FortiWeb (BYOL)**

Protects web applications from attacks that target known and unknown vulnerabilities. FortiWeb is the first ML-enabled WAF that reduces false positives and implements an effective security posture.

- **FortiManager (BYOL)**

Fortinet 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 as well as 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. When combined with the FortiGuard Indicators of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to allow for rapid action.

- **FortiCWP (BYOL)**

FortiCWP offers a cloud-native cloud workload protection (CWP) service designed for mitigating cloud platform configuration-related risks, monitoring cloud account activity for suspicious behaviors, and helping organizations prevent threats and maintain compliance. It provides insights into infrastructure, user behavior, and data stored in the cloud with reporting tools.

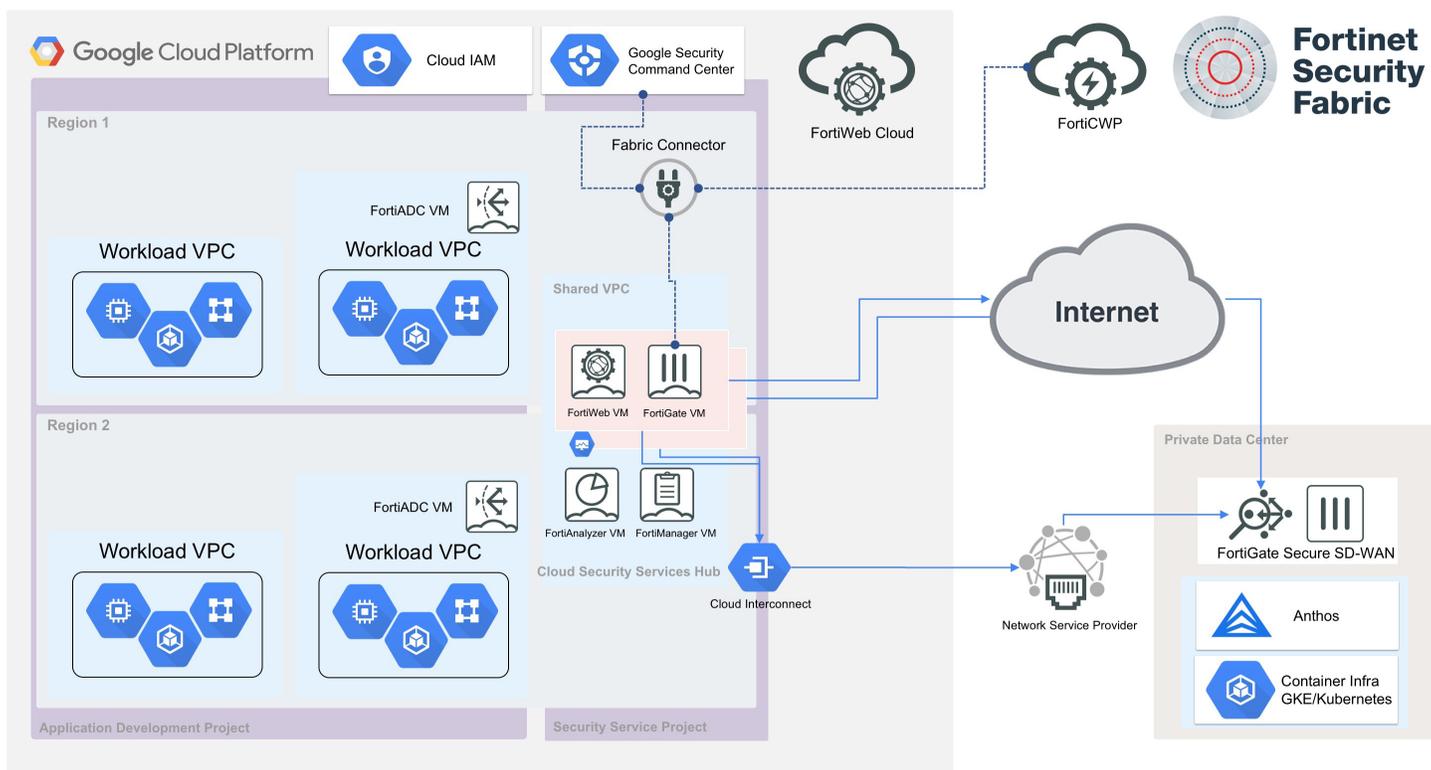
- **FortiADC (BYOL)**

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.

- **Fabric Connectors**

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

Reference Architecture



Use Cases for Extending the Fortinet Security Fabric to Google Cloud

The Fortinet Security Fabric for Google Cloud offers consistent, enterprise security. The Fortinet Security Fabric protects workloads across on-premises, data center, and cloud environments, including multilayered security for born-in-the-cloud applications. The Fortinet Security Fabric supports a spectrum of Google Cloud-based enterprise use cases:

1. Network Security

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

- Distributed enterprise/SD-WAN
- Hybrid cloud
- VPC-to-VPC segmentation
- Remote access

2. Application and Web Traffic Security

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

- FortiWeb Cloud WAF-as-a-Service
- FortiWeb VM

3. Cloud Workload Protection

Monitor activity in Google Cloud to apply best security practices, mitigate risk, and reduce misconfiguration.

- Configuration assessments
- Cloud account activity monitoring
- Cloud traffic monitoring
- Cloud data security scanning

Enterprise Protection to Reduce Risk

Fortinet Dynamic 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 GCP users. Continuous control and visibility through a single pane of policy management reduce security complexity. With Fortinet Dynamic Cloud Security, leaders can rest assured their security architecture covers the entirety of the network attack surface, and that their sensitive data is compliant and secure.

¹ ["2019 State of the Cloud Report,"](#) Flexera, March 2019.

