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.

Enterprise security for Google Cloud

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

Continuous visibility and real-time malware protection with FortiEDR and Google Cloud Security 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.

Security from the edge to the cloud

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

Advanced Security for Google Cloud

Fortinet Cloud Security for Google Cloud 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 Cloud Security offers network, application, and cloud platform security capabilities in various form factors, including virtual machine (VM), container, 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 offer effective 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, 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 overall security posture and reduce misconfiguration.

Expanding Threat Landscape

As outlined in the 2023 Fortinet Cloud Security Report, security remains a top concern among organizations using the cloud. In fact, 95% of surveyed organizations are concerned about their security posture in public cloud environments.[1] Key concerns include preventing cloud misconfigurations, securing applications already in production, and defending against malware. With a growing number of organizations using two or more cloud providers or a hybrid-cloud infrastructure, the complexity of these challenges is compounded. Accordingly, it's understandable why 90% 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

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

- **Single-vendor SASE**

FortiSASE is a single-vendor SASE solution. It integrates cloud-delivered SD-WAN connectivity with a cloud-delivered security service edge to extend the convergence of networking and security from the network edge to work-from-anywhere users. 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 that is fully integrated into Google Cloud. 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, Health Insurance Portability and Accountability Act, and data privacy laws such as the European Union's General Data Protection Regulation.

- **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. The Fortinet Security Fabric for Google Cloud solutions 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:

- **Bring your own license (BYOL)**

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

- **Pay-as-you-go**

Fortinet lists many solutions that can be consumed using a pay-as-you-go (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.

The following products are 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.

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

Delivered as SaaS, FortiWeb 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.

- **FortiFlex (private offer)**

FortiFlex is a points-based cybersecurity licensing program that allows organizations to easily provision the services and solutions they need on-demand. 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.

- **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 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. 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 a wide range of 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 the need for 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, and outbound threats and data loss with a wide range of top-rated security capabilities. It includes powerful, built-in capabilities for spam, phishing, malware, and ransomware protection.

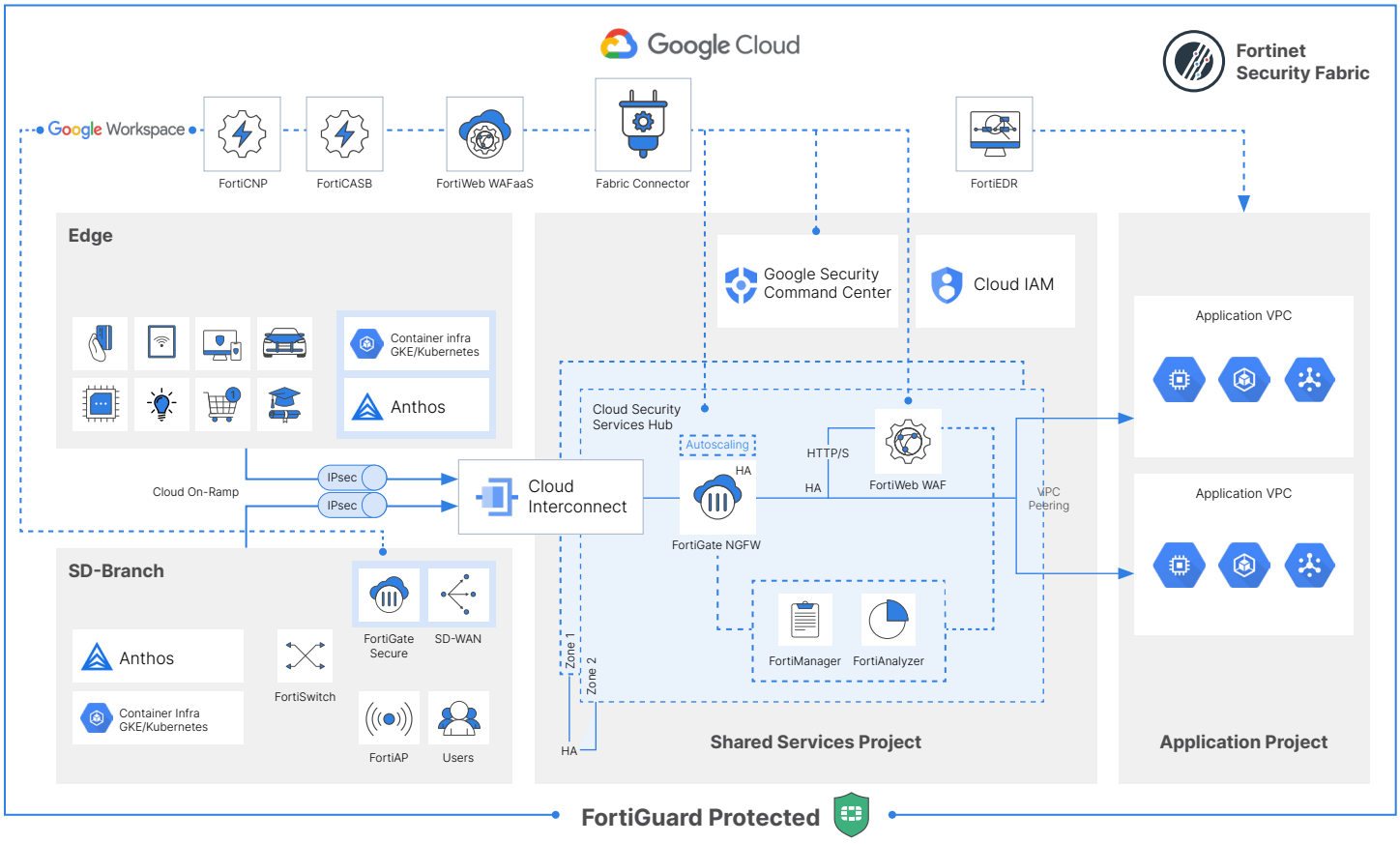

Figure 1: Google Cloud reference architecture

Use Cases for Extending the Fortinet Security Fabric to Google Cloud

The Fortinet Security Fabric offers consistent enterprise security and 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 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.

- 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 their security architecture covers the entirety of the network attack surface and that their sensitive data is compliant and secure.

[1] "2023 Cloud Security Report," Fortinet.

January 3, 2024 4:22 PM

571283-D-0-EN