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. 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, 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. 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 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 Google Cloud.

Google offers customers a variety of basic security tools to address Google Cloud 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, Google Cloud 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 Cloud Security for Google Cloud 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

76% of organizations are utilizing two or more cloud providers in efforts to reduce exposure to single sourcing and overpayment. 39% of 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

Enterprise Security for Google Cloud

Continuous threat visibility within FortiCNP and real-time protection with FortiEDR 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 Google Cloud with FortiGate Secure SD-WAN and Network Connectivty 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.

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 Cloud Security provides 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 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 Google Cloud. This simplicity helps eliminate human errors while reducing the time burden on limited IT resources.

- **Cloud-native visibility and control**

  Simplify security by contextualizing security findings and prioritizing the most critical resources with actionable insights to help security teams effectively manage cloud risk with FortiCNP cloud network protection (CNP).

- **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 (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:

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

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

- **PAYG**

  Fortinet lists many solutions that 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. 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)**

  Deployed as a VM, protects web applications and APIs from attacks that target known and unknown vulnerabilities, including the OWASP To 10, zero-day threats, and other application layer attacks.

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

  Delivered as a SaaS service, 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.

- **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.

- **FortiCNP (BYOL and PAYG)**

  FortiCNP is a cloud-native protection (CNP) platform natively integrated with Cloud Service Providers' (CSP) security services and Fortinet's Security Fabric to deliver a comprehensive, full-stacked cloud security solution for securing cloud workloads.

- **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.

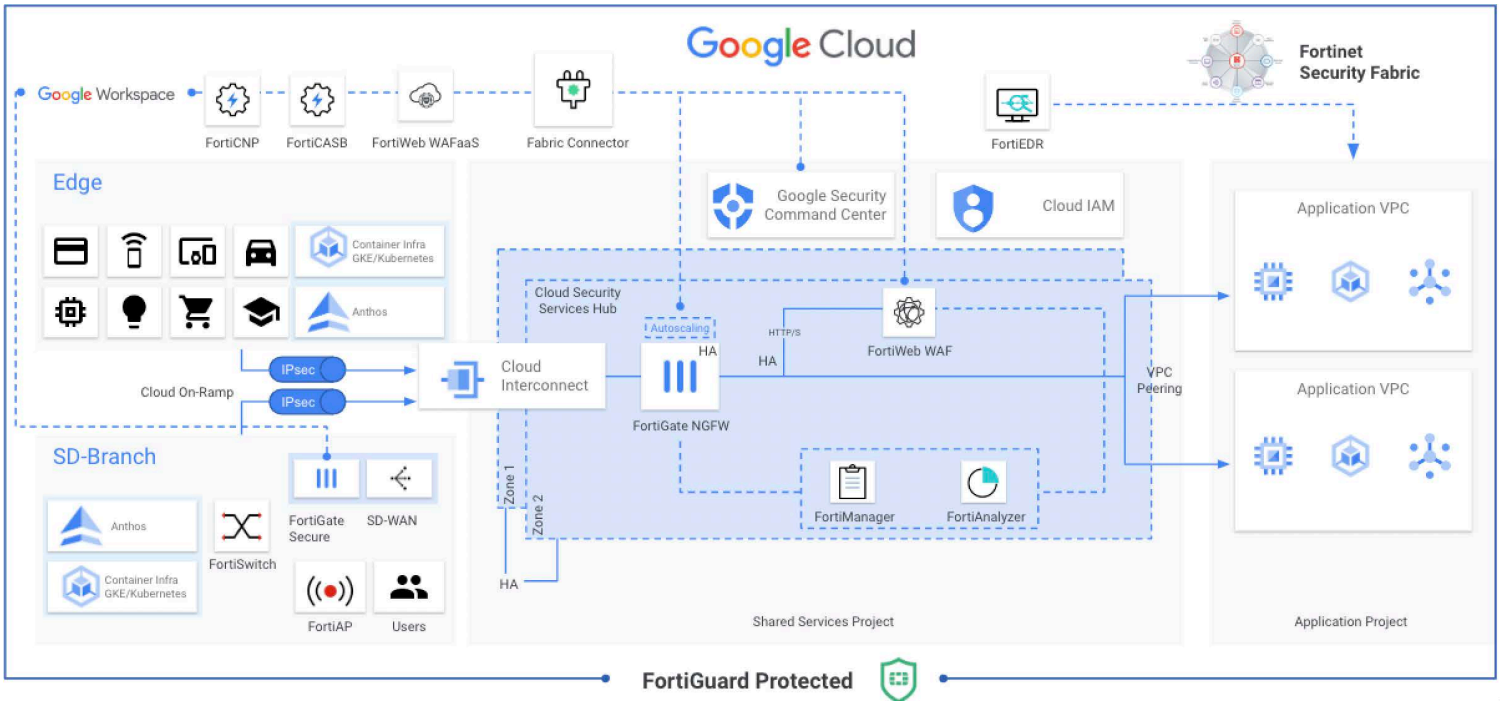
- **Fabric Connectors**

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

FortiEDR

FortiEDR brings MITRE ATT&CK-proven behavior-based endpoint detection and response (EDR) technology to protect Google Cloud workloads. Rest well knowing that 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.

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 Google Cloud infrastructure to build effective and low-friction security solutions.

   - Distrubuted 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 attacks, botnet attacks, 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. **Cloud Workload Protection**
   - Configuration assessments
   - Cloud account activity monitoring
   - Cloud traffic monitoring
   - Cloud data security scanning

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] "2022 Cloud Security Report," Fortinet, 2022.

July 29, 2021 8:51 AM
571283-C-0-EN