FORTINET SECURITY FABRIC EXTENDS ADVANCED SECURITY TO THE GOOGLE CLOUD PLATFORM

EXECUTIVE SUMMARY

Google Cloud Platform (GCP) was designed with security at its core. Google uses a variety of technologies and processes to secure information stored on Google servers. And like other public cloud platforms, Google offers customers a great deal of basic security control over their instances running on its infrastructure. However, cloud Infrastructure-as-a-Service (IaaS) does not control security on the operating system, software packages, network connections, inbound and outbound traffic, or applications that are deployed by customers. Customers are required to protect their cloud-based applications and adhere to compliance similar to how they do for on-premises applications. The Fortinet Security Fabric for GCP enables organizations to apply consistent policies throughout their multi-cloud infrastructures, resulting in consistent enforcement and visibility.

SECURING AN ARRAY OF GOOGLE PUBLIC CLOUD USE CASES

The Fortinet Security Fabric for GCP extends consistent, best-in-class enterprise security to GCP. The Security Fabric protects business workloads across on-premises data-center and cloud environments, including multi-layered security for born-in-the-cloud applications. The Security Fabric supports a variety of common GCP-based enterprise cloud use cases, including:

1. **Hybrid Cloud.** Businesses need seamless security orchestration that scales along with cloud workloads. The Fortinet Security Fabric includes next-generation firewalls (NGFWs) that complement native GCP security functions while supporting secured and encrypted connectivity across every flavor of cloud infrastructure. They can be managed from either a public cloud deployment or on-premises in a private data center.
2. **Web Application Security.** An increasingly essential part of modern business, web applications are commonly deployed over public cloud infrastructures. At the same time, web applications are responsible for the highest number of breaches per pattern.[1] The Fortinet Security Fabric for GCP includes solutions designed to protect business-critical web applications while relieving the need to constantly apply patches to web servers. This helps organizations comply with regulatory and security standard requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA).
3. **Secure Access VPN.** As organizations increasingly adopt a "cloud-first" approach, they're building out large, cloud-heavy infrastructures to support future IT growth and instant services to internal line-of-business customers. But they still require secure remote access to these new IT infrastructures, including all internal applications and work-related tools. Fortinet delivers best-in-class performance for securing VPN traffic and enables organizations to leverage Google's global presence by building remote access VPN in GCP. Fortinet delivers access to both applications residing in the cloud as well as on-premises to the cloud over IPsec VPN tunnels.
4. **Cloud Services Hub (VPC).** Cloud provider connectivity far outperforms that of a typical midsize enterprise. A GCP-based virtual private cloud (VPC) can provide a shared set of services to multiple networks worldwide. By leveraging the extent of network visibility, VPN connectivity, NGFW, and advanced web application firewall capabilities, the Security Fabric offers far more services while leveraging cloud elasticity and on-demand scalability for optimized price/performance.
5. **SD-WAN in the Cloud.** Many enterprise customers say their existing wide-area network (WAN) is cost prohibitive and lacks the agility to accommodate cloud adoption. Similar to the Cloud Services Hub, the Security Fabric's secure software-defined wide-area network (SD-WAN) services can be provided to multiple remote branches, where they all connect to Internet services through an SD-WAN hub built on GCP. Customers can build out cloud-based SD-WAN solutions where management and reporting of the security infrastructure are performed in the cloud, while managing on-premises and in-the-cloud gateways. The benefits of doing so include scalability, localization, and availability.

HOW THE SECURITY FABRIC COMPLEMENTS GCP SECURITY

Fortinet Security Fabric provides GCP users with the ability to apply consistent policies throughout their multi-cloud infrastructures, resulting in consistent enforcement and visibility. The Security Fabric offers deep, multi-layer protection and operational benefits for securing web applications over GCP and for managing global security infrastructures from the cloud.

Key capabilities of the Security Fabric for GCP include:

Single-Pane Control and Management. Both cloud and on-premises 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. Organizations gain in-depth visibility into their GCP application deployments. They no longer need to care for specific deployment configuration details, but rather get closer to an intent-based policy description. By using dynamic address groups and logical naming of cloud-based resources, security policies can follow while underlying resources scale-out or move throughout the cloud infrastructure.

Shadow IT Control. With organizations streamlining IT operations and consolidating security controls, many lines of business

now directly source their own cloud-based services. The Security Fabric offers IT departments better visibility into the use of GCP infrastructures and the ability to implement tighter control over usage patterns to protect the organization from risk.

PCI Compliance-Ready. Security Fabric solutions offer best-in-class protection to help you comply with the current PCI DSS standard (6.6).

INTEGRATED DEFENSES THAT SPAN THE FULL ATTACK SPECTRUM

The different solutions that comprise the Fortinet Security Fabric for GCP were designed to increase end-user confidence in Google cloud environments. All Fortinet GCP products are based on Fortinet Virtual Machine (VM) form factors. Licenses purchased from a Fortinet channel partner for VMs are transferrable across platforms. For instance, the same VM license for FortiGate-VM on VMware will work for the FortiGate for GCP platform while using the **bring-your-own-license (BYOL)** model. In this case, BYOL products can be purchased directly through GCP and are billed by the hour. Beyond the above, FortiGate can also be consumed using **pay-as-you-go (PAYG)**.

The following products are part of the Fortinet Security Fabric for GCP:

- **FortiGate-VM** NGFW delivers one of the industry's best threat-protection capability sets to defend against the most advanced known and unknown cyberattacks. FortiGate-VM scales up and down as per customer requirements and is offered at various sizes to align with the variety of supported use cases.
- **FortiWeb** web application firewalls (WAFs) protect hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and from zero-day threats.
- **FortiManager** provides single-pane-of-glass controls across the extended enterprise—offering insights into traffic and threats while overseeing policies. It includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices.
- **FortiAnalyzer** 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.
- **FortiCASB** offers a cloud-native Cloud Access Security Broker (CASB) subscription service that is designed for visibility, compliance, data security, and threat protection. It provides insights into users, behaviors, and data stored in the cloud with comprehensive reporting tools.

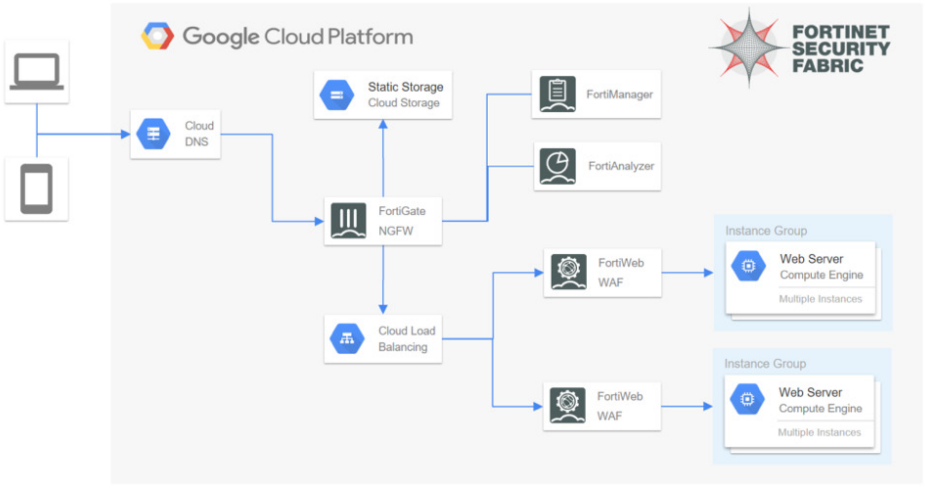

FIGURE 1: FORTINET SECURITY FABRIC SOLUTIONS FOR GOOGLE CLOUD PLATFORM

- **Fabric Connectors** enable open integration of the Fortinet Security Fabric to automate firewall and network security into dynamic network flows with multiple components in a customer's ecosystem.

MULTI-LAYERED PROTECTION THAT REDUCES RISK

Fortinet breaks down the walls that inhibit security visibility and management between and across private, public, and hybrid cloud platforms—enabling security leaders to ensure their security networks cover the entirety of the attack surface.

Core benefits of the Fortinet Security Fabric for GCP include:

- Consistent security posture in a shared responsibility model, from on-premises to the cloud
- Comprehensive advanced security and threat prevention for GCP users
- Continuous control and visibility through a single pane of policy management

[1] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

August 8, 2018 8:42 AM

252156-A-0-EN