Fortinet Security Fabric Extends Advanced Security for Oracle Public Cloud

Executive Summary

Oracle Cloud Infrastructure (OCI) offers a broad collection of cloud services from a single solution, delivered from the OCI bare metal stack to the OCI Classic (OCI-C) public cloud. These services provide basic security control for customer applications. However, cloud-native security doesn't offer enterprise-level functionality, which has become common practice for on-premises deployments. In addition, the operating system, software packages, network connections inbound/outbound traffic, and applications that are deployed by customers are the sole responsibility of the customer. Customers have the same responsibility to protect their cloud-based applications and enforce compliance as they do so for their onpremises applications. The Fortinet Security Fabric for OCI enables organizations to apply policies throughout their multi-cloud infrastructures for consistent enforcement and visibility.

Hybrid Cloud is a Reality

The use of hybrid cloud and hybrid IT with a combination of cloud services and on-premises assets is now a reality for most enterprises. According to Technology Business Research (TBR), 51% of enterprises have adopted at least one workload that leverages a hybrid cloud or hybrid IT deployment method.[1]

OCI helps capture the huge demand for hybrid cloud solutions worldwide with its incumbent positioning in mission-critical enterprise application deployments. With the introduction of OCI-C, customers can set the pace for their own cloud adoption when needed.

This joint solution from Oracle Cloud and Fortinet helps businesses address key challenges, including:

- Enterprise-class security for protection against advanced threats
- Consistent policies across the hybrid cloud infrastructure
- Continuous control and visibility through a single pane of policy management
- Greater business agility, from on-premises to the cloud
- Passing compliance audits for non-disruption of operations
- Easy contracts and licenses renewal across multi-cloud deploymentsimproved compliance
- Proven Protection from the OWASP Top 10 threats, DoS attacks, botnets, and more

FORTINET Fabric-Ready

Securing an Array of Public Cloud Use Cases

The Fortinet Security Fabric for public cloud extends consistent, best-in-class enterprise security to OCI. The Security Fabric protects business workloads across on-premises and cloud environments, including multi-layered protection for born-in-the-cloud applications. Fortinet Security Fabric for OCI supports a variety of common enterprise cloud usecases, including:

1. Hybrid Cloud

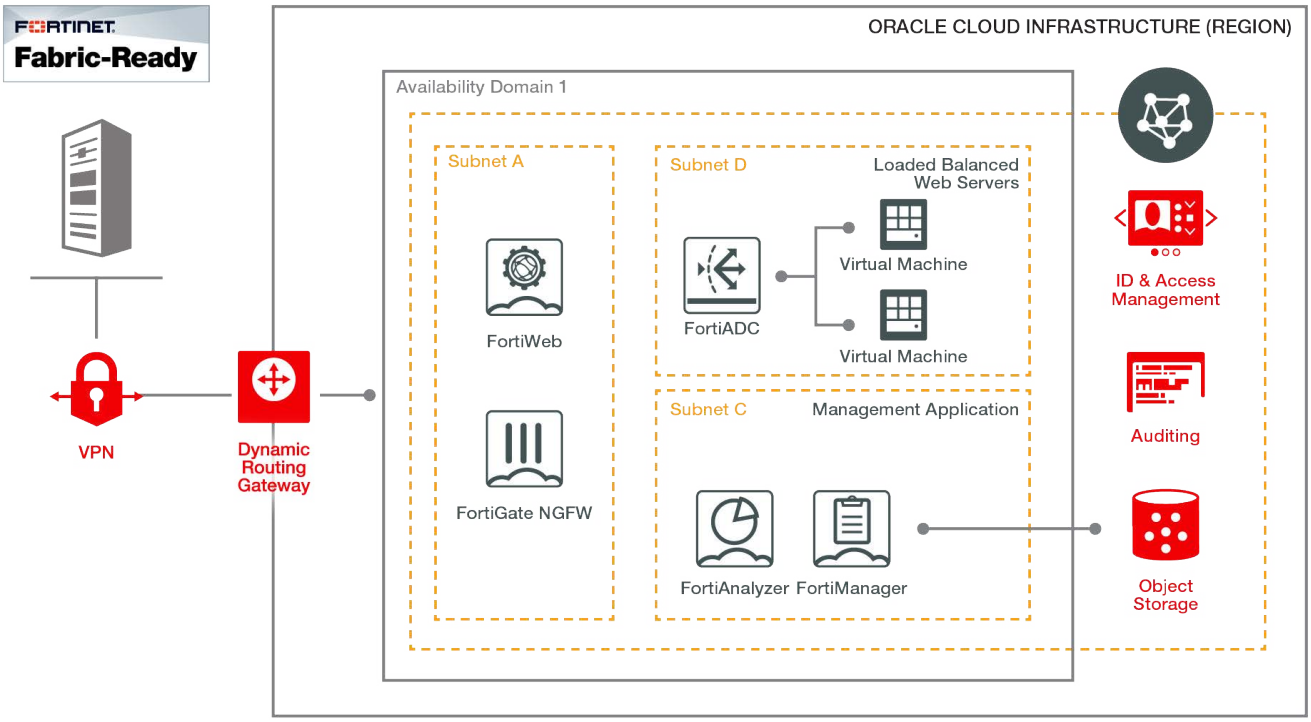
Businesses need seamless security orchestration that scales along with cloud workloads. The Fortinet Security Fabric includes next generation firewalls (NGFWs) that complement native public cloud security functions while supporting secured and encrypted connectivity across every flavor of cloud infrastructure. They can be managed from either a public cloud deployment or on-premises in a private data center.

2. 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 the public cloud for building remote access VPN in the cloud. Fortinet delivers access to both applications residing in the cloud as well as on-premises applications connecting to the cloud over IPSec VPN tunnels.

How the Security Fabric Complements Native OCI Security

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



FORTINET

Key Capabilities of Forti Net Security Fabric for OCI Include:

- **Single-Pane Control and Management**

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

- **Cloud-native Visibility and Control**

  Organizations gain indepth visibility into their cloud 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 tags, address groups, and logical naming of cloudbased 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. Fortinet Security Fabric offers IT departments better visibility into the use of public cloud infrastructures, and the ability to implement tighter control over usage patterns to protect the organization from risk.

Integrated Defenses that Span the Full Attack Spectrum

The different solutions that comprise the Fortinet Security Fabric for public cloud were designed to increase end-user confidence in cloud environments. All of the Fortinet cloud 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 the relevant public cloud platform while using the bring your own license (BYOL) model.

The following Products are part of the Fortinet Security Fabric for OCI:

- **FortiGate-VM**

  Next generation firewalls deliver 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 with 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 multilayer and correlated detection methods, FortiWeb defends applications from known vulnerabilities and 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 attacksas 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.

- **FortiADC**

  Optimizes the availability, user experience, and scalability of enterprise application delivery. It enables fast, secure, and intelligent acceleration and distribution of even the most demanding enterprise applications.

The different solutions that comprise the Fortinet Security Fabric for public cloud were designed to increase end-user confidence in cloud environments.

Multi-Layered Protection that Reduces Risk

The different solutions that comprise the Fortinet Security Fabric for public cloud were designed to increase end-user confidence in cloud environments. All of the Fortinet cloud 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 the relevant public cloud platform while using the bring your own license (BYOL) model.

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

[1]"Hybrid is driving cloud and the overall IT opportunity," Technology Business Research, April 2017.

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray