SOLUTION BRIEF

Fortinet Cloud Security Services Hub

Executive Summary

Cloud environments enable developers to independently develop new applications in networks that are outside of corporate network security protection and the realm of IT control. Applying security policies consistently across the different autonomously developed applications and environments controlled by development operations (DevOps) teams is a challenging task. This problem is compounded by a lack of qualified security personnel and other resource constraints. The Fortinet Security Fabric helps address these challenges by leveraging public cloud network characteristics. It provides consistent security by building a centralized security services hub—delivering visibility and consistent security policy enforcement across all environments while allowing developers to continue rapidly iterating and introducing new applications to market.

Unleash DevOps Agility While Maintaining Centralized Security:

- Provides consistent security enforcement across infrastructures and applications
- Offers a highly available and scalable security infrastructure
- Separates security from application life cycles without compromise
- Secures VPN cloud connectivity
- Delivers native integration with leading public cloud security tools

Addressing Inconsistent Security Across Development Efforts

Last year, more than half of all breaches were caused by either human errors or system glitches (as opposed to malicious or criminal attacks).[1] Misconfiguration of cloud-based applications directly contributes to risk within cloud-based infrastructures. As developers focus on rapidly producing the most efficient and valuable applications, they often neglect which security controls are best suited to protecting their applications.

Developing secure applications always presents challenges—and these become even more pronounced when DevOps teams work in separate virtual networks and clouds without centralized security standards and controls. Limited visibility and control make it especially difficult to ensure consistent, effective security standards for applications in development.

A recent survey shows that 52% of companies scaled back security measures to meet a business deadline or objective.[2]

"An immature DevOps organization is focused on accelerating and optimizing their own domains with various technologies, instead of establishing an effective feedback loop, end-to-end visibility, and most importantly common situational awareness."[3]

A Security Services Hub, Separate from Development

The answer is to build a central security services hub (also known as a "transit network") that is maintained by security professionals. This solution splits security management and operation from application development by providing security in a centralized, shared, logical network that is managed by the security team. It allows different application environments, typically built using different cloud virtual networks, to connect through the cloud security services hub to each other and to the internet. This approach can also securely connect other physical networks, offices, clouds, and data centers—all leveraging a central security infrastructure.

A security services hub enforces security policies and provides visibility into inbound and outbound traffic between the different connected networks and the internet, while relieving developers of the burden of maintaining security for their applications.

A Cloud Security Services Hub Built on the Fortinet Security Fabric

By leveraging different solutions within the Fortinet Security Fabric, the cloud security services hub can extend protection beyond that of a next-generation firewall (NGFW). It offers web application and API protection (WAAP) capabilities, sandboxing to detect unknown threats, and mail gateway protection—all as needed by organizational applications. As an extension of the Fortinet Security Fabric, customers have integrated protection that simplifies the management and automation of security for cloud-based infrastructure.

1. NGFW access control. The FortiGate VM NGFW is at the heart of the cloud security services hub solution. Using the FortiGate VM, the security services hub provides defenses between virtual networks and out to the internet. It repels malicious IP addresses, implements segmentation policies, performs intrusion prevention (IPS) inspection, and leverages application control capabilities for securing egress communications.

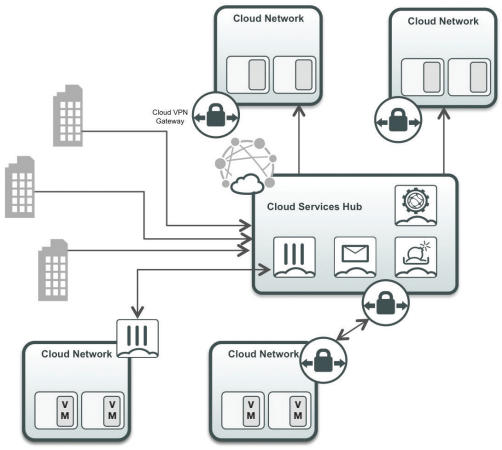

Figure 1: **Unifying multi-cloud security.** Organizations need a shared security services hub that can dynamically scale with fluctuating demands—one that tremendously simplifies the design and operation of security for large cloud infrastructures.

FortiGate VM NGFWs are designed to inspect high-speed traffic for threats. They notably offer the most scalable NGFW solution for cloud environments—all the way from very minimal footprints up to over 96 vCPU-based virtual NGFWs.

2. VPN connectivity. The security services hub uses FortiGate NGFWs to establish and maintain secure VPN cloud connectivity across virtual networks and from other data centers, office locations, and remote users. The scalability of FortiGate VM NGFWs allows organizations to maintain high-speed VPN connections without the need to go through endless engineering challenges (as is often experienced when building high-speed VPNs in the cloud).

3. Secure web gateway. FortiGate VM NGFWs implemented in the cloud security services hub as a secure web gateway can be used as an exit point out to the internet for end-users as well as servers, organizational offices, branches, or even backhauled remote users. In this configuration, the security services hub enforces acceptable internet usage policies and mitigates the risk from malicious or suspicious websites or internet resources.

4. Web application security. As the use of Software-as-a-Service (SaaS) applications grows to the point where almost all cloud-based applications use the HTTP protocol and can be considered either front-end web applications, back-end web applications (for mobile apps), or middleware APIs, the need for an effective and easy-to-use WAAP increases.

A FortiWeb web application firewall (WAF/WAAP) can be part of the security services hub and used as the shared web application security entry point for internet traffic accessing web-based applications in different virtual networks that are used to build business applications. This allows for a central set of web security policies to protect applications, including those in development and across a large set of organizational applications. It offers security against sophisticated attacks while ensuring compliance with regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). FortiWeb addresses the key challenges of false positives and long policy tuning cycles associated with web application security through the use of machine learning. These advantages make web security available for more applications and can help increase the secure adoption of cloud technology.

5. Sandboxing. Protecting against unknown and zero-day attacks is critical for organizations that handle large amounts of unsolicited content and files. Placed in the cloud security services hub, a FortiSandbox can be integrated with FortiGate VM NGFWs to scan relevant in-line traffic for unknown threats. This protection can also be integrated into the cloud application as a service by leveraging the FortiSandbox JSON API. In addition, FortiSandbox can be directly attached to cloud storage buckets leveraging native integration functionality in order to scan files that are placed in publicly accessible storage services without going through the in-line protections of the cloud security services hub.

Security to Empower Developers

Developers and security teams both benefit from a security architecture that consistently enforces policies across all application environments while allowing developers to continue iterating on their applications without needing to slow down for security controls. The Fortinet Security Fabric-based cloud security services hub enables teams to leverage different cloud environments to develop applications autonomously without struggling with the implementation of independent security policies for each environment. And with the security services hub, developers and organizations alike benefit from a central location for security policy management and enforcement.

[1] "2018 Cost of a Data Breach Study," Ponemon, July 2018.
[2] "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.
[3] Michael Segal, "Visibility is key for devops and the hybrid cloud," Network World, September 7, 2018.

FORTINET®

www.fortinet.com

July 22, 2019 9:23 AM

356398-A-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:SB-Fortinet-Cloud-Security-Service-Hub:sb-fortinet-cloud-security-service-hub Folder-2:sb-fortinet-cloud-security-service-hub