SOLUTION BRIEF

Fortinet Cloud Security Services Hub

Executive Summary

Cloud transformation is a C-level priority in most organizations. Application developers and development operations (DevOps) teams are moving at the speed of cloud. But unlike the network operations (NetOps) and security operations (SecOps) teams, the C-level priority is not security. Reducing security risks and ensuring compliance consistently across the different autonomously developed applications and environments controlled by 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. NetOps, SecOps, and DevOps teams can benefit from the Cloud Security Services Hub. It is easy to deploy and operate, and offers elastic scaling, consistent security policies, and effective compliance enforcement across different deployment topologies while allowing developers to continue rapidly iterating and introducing new applications to market.

DevOps Model and Associated Risks

Human error is often the culprit in cloud data breaches[1] (as opposed to malicious or criminal attacks). 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.

Centralize Visibility and Compliance

The answer is to build a central security services hub (also known as a "transit network") that is maintained by NetOps and SecOps teams. 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 to segment, inspect, and provide visibility into inbound and outbound traffic between the different connected networks and the internet, thereby reducing the burden on application developers from being overwhelmed by security and compliance requirements.

Unleash DevOps Agility With Cloud Security Services Hub

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

Risk #1: Not treating security as a first-class DevOps citizen

In 2020, average total cost of a data breach was $3.86 million. And 280 days was the average time to identify and contain a data breach.

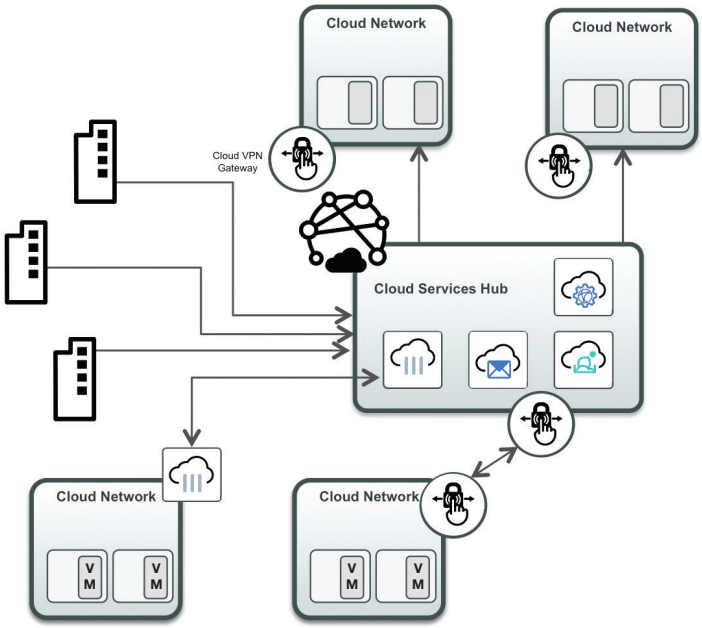

Figure 1: Unifying multi-cloud security. Organizations need a shared security services hub that can dynamically scale with fluctuating demands—one that tremendously simplifies the design and operation of security for large cloud infrastructures.

Cloud Security Services Hub Solution

The Fortinet Cloud Security Services Hub provides a complete security solution through the Fortinet Security Fabric that brings together next-generation firewall (NGFW), sandboxing, and web application and application programming interface (API) protection (WAAP). Organizations can start with centralizing network security and gradually add WAAP and other security capabilities to the Cloud Security Services Hub. 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 protection. The FortiGate VM NGFW is at the heart of the Cloud Security Services Hub solution. Using the FortiGate VM, the security services hub provides isolation between virtual networks and the internet. It filters out malicious IP addresses, implements segmentation policies, performs intrusion prevention (IPS) inspection, and uses deep packet inspection (DPI) to provide visibility into application layer traffic and threat vectors. FortiGate VM NGFWs are designed to scale up in performance or scale out for reliability. The VMs can range from a small 1 vCPU configuration to 96 vCPU configuration to match threat protection throughput requirements.

2. VPN connectivity. The security services hub uses FortiGate NGFWs to establish and maintain secure virtual private network (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 being limited by cloud service provider VPN gateways, which offer a fraction of the VPN performance.

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 solution that simplifies security rollout and brings forth centralized visibility and control, thereby reducing risk and improving compliance without slowing down the speed of DevOps-led cloud operations.

[1] James Rundle, "Human Error Often the Culprit in Cloud Data Breaches," The Wall Street Journal, August 27, 2019.

[2] Isaac Sacolick, "6 security risks in software development and how to address them," InfoWorld, March 8, 2021.

[3] "2020 Cost of a Data Breach Report," IBM Security, July 2020.

August 5, 2021 2:24 PM

356398-B-0-EN