SOLUTION BRIEF

Fortinet Security Fabric Automation for AWS

Executive Summary

Amazon Web Services (AWS) is the largest provider of cloud computing services worldwide. AWS pioneered Infrastructure-as-a-Service (IaaS) and is rapidly enhancing their Platform-as-a-Service (PaaS)—enabling customers to accelerate software development and streamline operations. While AWS offers security functionality, enterprise customers that use both on-premises and cloud-based environments need the ability to implement consistent security policies across all locations. The Fortinet Security Fabric natively integrates into AWS to provide full visibility and control of applications, centralized management, and security automation across hybrid environments.

The Fortinet Security Fabric includes FortiGate next-generation firewalls (NGFWs) that complement native AWS security groups while supporting secured and encrypted VPN connectivity across every flavor of cloud infrastructure.

Establishing Consistent Security Across Data Centers and the Cloud

By the end of 2018, 50% of global enterprises will rely on at least one public cloud platform to drive digital transformation (DX).[1] Increased adoption of cloud services like AWS is just one of the trends driving the DX era, along with the explosion of the Internet of Things (IoT) and mobile devices. While these technologies make businesses nimbler and offer new capabilities at an infrastructural level, they've also changed the nature of networks themselves—and how they are protected from outside threats.

Because of built-in security features, it's often assumed that cloud solutions like AWS are safe and that everything is automatically protected. But AWS is only responsible for protecting the cloud infrastructure that runs all of the services offered—namely, *security of the cloud.* Thus, cloud customers should carefully consider the services they choose, as that dictates their own responsibility for *security in the cloud*. Indeed, the vast majority of cloud security failures end up being the customer's fault. This often comes from a lack of understanding of the shared responsibility model and how the details of that model vary from cloud to cloud. Generally, cloud customers are responsible for securing the remaining upper elements—network, applications, and data.

Securing an Array of AWS Public Cloud Use Cases

The Fortinet Security Fabric extends consistent, best-in-class enterprise security to AWS-based cloud environments. The Security Fabric protects business workloads across on-premises data centers and cloud environments—including multilayer security for cloud-based applications. The solution offers VM-, container-, and API-based protection that delivers natively integrated security functionality powered by Fortinet and enforced by AWS.

The Security Fabric supports a wide variety of public cloud use cases, including:

1. **Hybrid cloud.** Businesses need seamless security protection that scales along with cloud workloads. The Fortinet Security Fabric includes FortiGate next-generation firewalls (NGFWs) that complement native AWS security groups while supporting secured and encrypted virtual private network (VPN) connectivity across every flavor of cloud infrastructure. FortiGate NGFWs can be managed from either a public cloud deployment or on-premises in a private data center.

2. **Advanced threat prevention.** An increasingly essential percentage of modern business applications are deployed over public cloud infrastructures in general and AWS in particular. At the same time, web and mail applications are responsible for the highest number of breaches per pattern.[2] The Fortinet Security Fabric for AWS includes solutions designed to protect these kinds of business-critical applications from known and unknown threats, including zero-day attacks, by integrating Fortinet solutions such as FortiWeb web application firewalls (WAFs), FortiMail secure email gateways (SEGs), and FortiSandbox sandboxing. This mitigates the risk from server vulnerability and supports compliance with the latest laws, regulations, and standards. Additionally, FortiSandbox can protect externally facing collaboration applications from advanced persistent threat risks resulting from malicious file uploads.

The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic for remote access in AWS.

3. **Security automation for web applications and APIs.** Businesses that develop applications natively in the cloud without on-premises infrastructure or dedicated security staff need tools that can automate security for web applications and provide web-based application programming interface (API) gateway functionality. Fortinet offers advanced web application protection through managed rules for the AWS WAF service. This extends best-of-breed security protection from Fortinet to customers utilizing the AWS WAF. This solution is totally programmable and can be fully integrated into DevOps pipelines and application life-cycle operational routines, thus eliminating the need for dedicated security personnel.

4. **Secure access VPN.** The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic for remote access in AWS. By leveraging AWS's multiregion global infrastructure, organizations can instantaneously scale their services globally and provide remote access VPN termination close to the end-user. Remote access VPN can be used to enable access to cloud-based applications as well as on-premises applications that are connected to the cloud over other forms of private links or VPN.

5. **Cloud services hub.** Since AWS connectivity far outperforms that of the typical midsize enterprise, organizations can offer security services at a global scale. Leveraging AWS transit architectures and services allows organizations to build a security hub encompassing a variety of Fortinet security solutions to share security services across multiple AWS virtual private clouds (VPCs) and networks worldwide. This cloud services hub can provide network visibility, VPN connectivity, NGFW, advanced WAF, sandboxing, and mail security. The Fortinet Security Fabric provides a broad set of services while leveraging cloud elasticity and on-demand scalability for optimized price/performance and scalability.

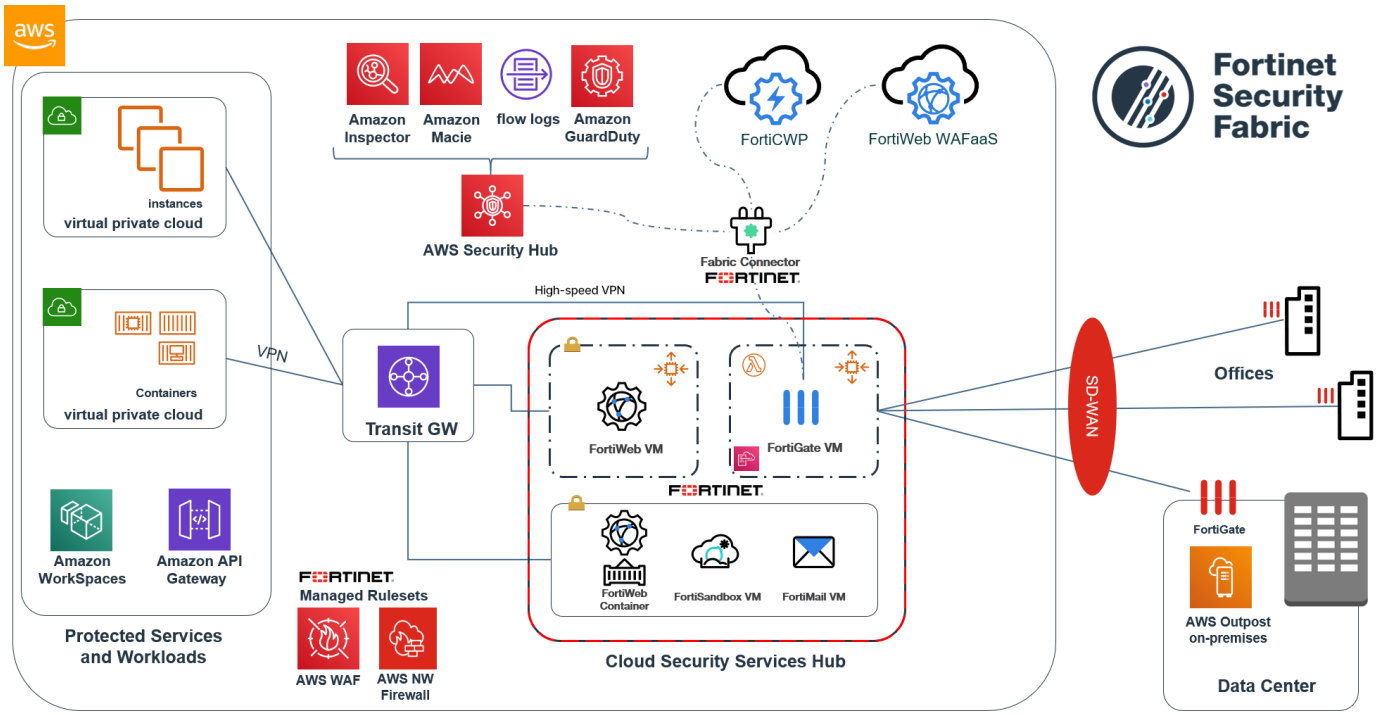

Figure 1: The Fortinet Security Fabric for AWS.

How the Security Fabric Complements AWS Security

The Fortinet Security Fabric offers deep, multilayered protection and operational benefits for securing applications from known and unknown threats in and out of AWS as well as for managing global security infrastructures from AWS.

Integrated Security Fabric solutions utilize the latest threat intelligence and share information in real time across the entire organization.

Key capabilities of the Security Fabric for AWS include:

- **Single-pane control and management.** The Security Fabric enables both cloud and on-premises security functionality to be centrally managed from within AWS, which 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 AWS application deployments. They no longer need to plan for specific deployment configurations. Instead, they get closer to applying intent-based policy. By using dynamic address groups, logical naming of cloud-based resources, and AWS Guard Duty threat feeds, security policies can be implemented as Security Fabric resources scale-out across 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 AWS infrastructures and the ability to implement tighter control over usage patterns to protect the organization from risks.
- **Protection from zero-day attacks.** Integrated Security Fabric solutions utilize the latest threat intelligence and share information in real time across the entire organization. This offers highly scalable zero-day attack protection that's fully integrated into AWS. It also helps to reduce the organization's risk from advanced persistent threats and increases confidence for deploying applications at any scale in the cloud.
- **Compliance ready.** Security Fabric solutions offer best-in-class protection to help organizations comply with current industry standards like Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) as well as data privacy laws such as the EU's General Data Protection Regulation (GDPR).

Integrated Defenses That Span the Full Attack Spectrum

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

All of these solutions are based on Fortinet Virtual Machine (VM) form factors, container form factors, and API integrations. They also provide flexible payment options:

- **BYOL.** Licenses purchased from a Fortinet channel partner for different products are transferrable across platforms. For instance, the same VM license for FortiGate VM on VMware will work for the FortiGate for AWS platform by using the bring-your-own-license (BYOL) model.
- **PAYG.** Many Fortinet solutions can be consumed using a pay-as-you-go (PAYG) on-demand usage model from the AWS marketplace.

The following solutions are part of the Fortinet Security Fabric for AWS:

- **FortiGate.** These NGFWs deliver some of the industry's best threat-protection capabilities 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 a variety of supported use cases. Available as PAYG and BYOL VMs.
- **FortiWeb.** Fortinet 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. Available as PAYG and BYOL VM as well as BYOL Docker Container.
- **FortiMail.** Our SEGs utilize the latest threat intelligence from FortiGuard Labs to deliver consistently top-rated protection from common and advanced threats while integrating robust data protection capabilities to avoid data loss. Available as BYOL VM.
- **FortiSandbox.** Our sandboxing solutions offer a powerful combination of advanced detection, automated mitigation, actionable insight, and flexible deployment to stop targeted attacks and subsequent data loss. Available as BYOL and PAYG VM.

- **AWS Fortinet WAF Partner Rules.** For basic protection of AWS-based web applications and API gateway services, Fortinet security intelligence is implemented via the AWS WAF enforcement engine. Available as a PAYG service.
- **FortiManager.** Fortinet provides single-pane-of-glass management and policy controls across the extended enterprise for insight into networkwide, traffic-based threats. This solution includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices. Available as BYOL VM.
- **FortiAnalyzer.** This solution collects, analyzes, and correlates data from Fortinet products for increased visibility and robust security alert information. When combined with the FortiGuard Indicator of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to allow for rapid action. Available as BYOL and PAYG VM.
- **FortiCASB.** The Fortinet cloud access security broker (CASB) solution includes cloud security posture management (CSPM) capabilities that support visibility, compliance, data security, and threat protection. FortiCASB offers configuration assessment and compliance reports for global AWS cloud deployments complementing the in-line capabilities of FortiGate VMs, with API-level protection for the public cloud. Available as BYOL subscription service.
- **Fabric Connectors.** These enable open integration of the Fortinet Security Fabric to automate firewall and network security insertion into the AWS cloud with multiple existing components within a customer's ecosystem as well as the ability to integrate with security intelligence services from AWS.

Multilayered Protection that Reduces Risk

Fortinet breaks down the barriers that inhibit security visibility and management across private, public, and hybrid cloud platforms. The Fortinet Security Fabric for AWS helps organizations maintain consistent security protection in a shared responsibility model, from on-premises to the cloud. It delivers comprehensive and fully programmable multilayered security and threat prevention capabilities for AWS users.

At the same time, it streamlines operations, policy management, and visibility for improved security life-cycle management with full automation capabilities. CISOs and other business leaders can ensure that their security architecture covers the entirety of the network attack surface when using the Fortinet Security Fabric.

[1] "Cloud innovation will power enterprise transformation in 2018," ZDNet, November 9, 2017.

[2] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

April 20, 2021 10:26 AM

D:\Fortinet\Work\2021\0420\sb-amazon-web-services-cloud-security

309622-A-0-EN