SOLUTION BRIEF

Dynamic Cloud Security 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 its 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.

74% of companies are moving apps back and forth between the cloud and on-premises—which creates a critical need for consistent security across locations.[1]

Establishing Consistent Security Across Data Centers and the Cloud

Because cloud providers offer an increasing number of security services, it is often assumed that cloud platforms like AWS are safe—that everything running in these environments is automatically secured. But cloud security is maintained through a shared responsibility model. This means that AWS is only responsible for protecting the cloud infrastructure that runs the services offered—security of the cloud. Subsequently, customers are responsible for all the services, applications, and data they use—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.

Integrated Defenses That Span the Full Attack Spectrum

The different solutions that comprise the Fortinet Security Fabric for AWS are designed to increase end-user confidence in AWS cloud environments. All of these solutions are based on Fortinet virtual machine (VM) form factors, container form factors, and Software-as-a-Service (SaaS) offerings. They are also available via flexible procurement 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 Fortinet products are available as part of the Fortinet Security Fabric for AWS:

- **FortiGate.** Fortinet 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 multilayered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and from zero-day threats. Available as PAYG and BYOL VM or SaaS, as well as BYOL ECS container.
- **FortiMail.** Fortinet secure email gateways (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.** Fortinet 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.

- **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 Indicators of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to allow for rapid action. Available as BYOL and PAYG VM.
- **FortiCWP.** The Fortinet cloud workload protection service includes cloud security posture management (CSPM) capabilities that support visibility, compliance, data security, and threat protection. FortiCWP offers configuration assessment and compliance reports for global AWS cloud deployments complementing the in-line capabilities of FortiGate VMs, with application programming interface (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.

The Fortinet Security Fabric Delivers Complementary AWS Security

The Fortinet Security Fabric protects business workloads across both on-premises data centers and cloud environments—providing consistent, multilayered security for applications on-premises and in the cloud. Specifically, the Security Fabric offers deep, multilayer 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. Key solution capabilities include:

Single-pane-of-glass 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. The Security Fabric delivers consistent security management using a consistent operational model.

Cloud-native visibility and control. Organizations gain in-depth visibility into AWS application deployments. They no longer need to plan for specific deployment configurations. Instead, they get closer to applying intent-based policies. 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 that can scale out across the cloud infrastructure.

Broad protection across the attack surface. Fortinet offers the broadest set of network security products for AWS in the industry, giving organizations the ability to run any application anywhere, whether on-premises or in the cloud. Fortinet security performs identically and is best suited to address the operational requirements and constraints of AWS environments.

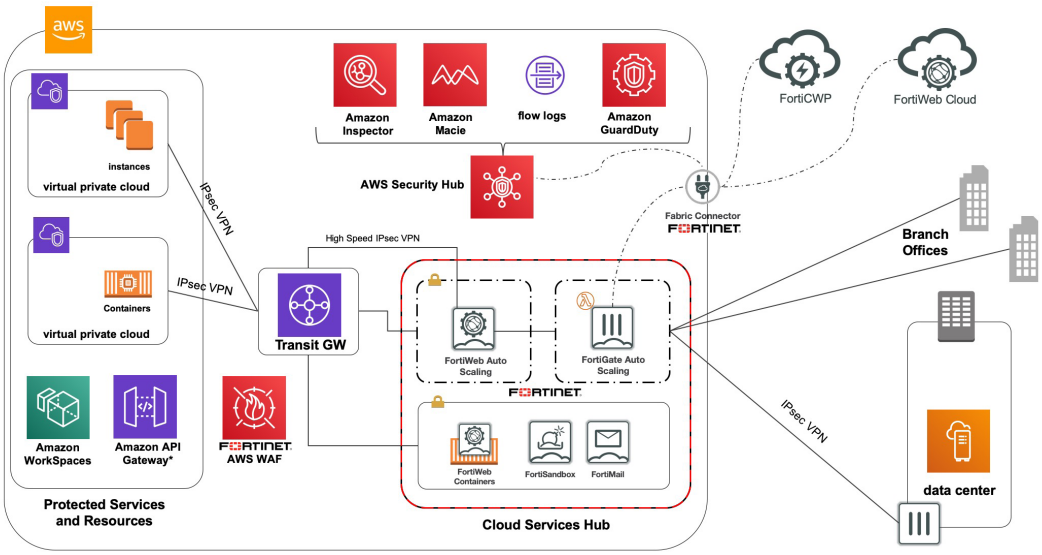

Figure 1: Fortinet dynamic cloud security for AWS.

Protection from zero-day attacks. Integrated Security Fabric solutions utilize the latest global threat intelligence (from FortiGuard Labs researchers) and also share local threat information in real time across the entire organization. This offers highly scalable zero-day attack protection that is fully integrated into AWS. It also helps to reduce the organization's risk from advanced persistent threats while increasing confidence for deploying applications at any scale in the cloud.

Compliance ready. Fortinet solutions offer best-in-class protection to help organizations comply with current industry standards like Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), as well as data privacy laws such as the European Union's General Data Protection Regulation (GDPR).

Securing an Array of AWS Public Cloud Threats

The Fortinet dynamic cloud security solution extends the Fortinet Security Fabric to AWS—offering consistent, best-in-class enterprise security to AWS-based cloud environments. The Fortinet Security Fabric supports public cloud use cases that include:

1. **Network security.** Leveraging the scale and flexibility of the AWS infrastructure, organizations can build effective and low-friction network security solutions for their organizations. A Fortinet cloud security services hub leverages the AWS Virtual Private Cloud (VPC) construct for implementing scalable, multi-layered security functionality into a single VPC per region. At the same time, it allows the rest of the organization's business units to operate autonomously using their own VPCs. Business units only need to attach their VPCs to the Cloud Services Hub VPC using a transit gateway (or other form of VPC peering).

   A FortiGate VM next-generation firewall (NGFW) is at the heart of a cloud security services hub solution. FortiGate VM unique network performance, cloud integration, and scalability allows security teams to maintain consistent protection and visibility while supporting productivity across their broader organizations. A Fortinet cloud security services hub solution supports specific needs that include:

- **SD-WAN.** When connecting multiple branches to the hub, organizations have the benefits of FortiGate Secure SD-WAN functionality with improved quality of experience (QoE), visibility, and branch network security for applications running in AWS.
- **Hybrid cloud.** When high-speed connectivity is required, the hub can provide secure site-to-site connectivity; this provides an ideal hybrid cloud solution due to opposite usage patterns from users and backups or machines.
- **VPC to VPC segmentation.** The hub's centralized nature provides an ideal place to define security policies for traffic between different business units and applications.
- **Remote access.** The hub is also the ideal place for terminating any remote access connections into the organization's applications and infrastructure—whenever VPN connectivity is required.

2. **Application and web security.** An increasingly essential percentage of modern business applications are deployed over public cloud infrastructures in general and via AWS in particular. At the same time, web applications are responsible for a high number of breaches. More than half (52%) of all breaches involve the hacking of web applications—by far the most common vector for hacking-based breaches.[2]

   The Fortinet dynamic cloud security solution for AWS protects business-critical applications from known and unknown threats—including zero-day threats, botnets, and API attacks. Fortinet mitigates risk from server vulnerability and supports compliance with the latest laws, regulations, and standards. Fortinet web security solutions include multiple options for AWS environments:

- **FortiWeb WAF-as-a-Service.** A SaaS implementation of FortiWeb web application firewall (WAF), which protects workloads within the same AWS region against sophisticated attacks.
- **FortiWeb ECS.** FortiWeb is available as part of the Elastic Container Service (ECS) marketplace on AWS, supporting customer requirements for containerized WAF functionality to protect single applications.
- **FortiWeb VM:** FortiWeb is also available in the AWS marketplace as an Amazon Machine Image (AMI) to support tailored protection of multiple applications.
- **Fortinet WAF Rules for AWS WAF.** A simple implementation of web security using static regular expression matching-based protection.

3. **Cloud workload protection (CWP).** Misconfiguration directly contributes to risk within cloud-based infrastructures. Last year, more than half of all breaches were caused by either human errors or system glitches (as opposed to malicious or criminal attacks).[3] As more security-related incidents are attributed to configuration mistakes, the need to address these types of threats increases.

Fortinet FortiCWP service interacts with the platform to help maintain platform hygiene as well as to monitor activities in AWS. FortiCWP deeply integrates with different AWS services such as Security Hub, GuardDuty, Inspector, and VPC Flow Logs. Its specific functionalities include:

- **Configuration assessment** of the customer's AWS environment and benchmarking against best practices in a systematic way
- **Cloud account activity monitoring** to mitigate risk of unauthorized or unsupervised access
- **Cloud traffic monitoring** for any traffic over any cloud network associated with the AWS account
- **Cloud data security scanning** through AWS S3 buckets for sensitive and malicious data

Multilayered Security That Reduces Risk

The Fortinet Security Fabric delivers comprehensive and fully programmable multilayer security and threat-prevention capabilities for AWS users. Fortinet cloud security for AWS helps organizations establish consistent protection in a shared responsibility model—from on-premises to the cloud.

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

[1] Daniel Hein, "74% of Companies Move Apps To the Cloud, Then Back On-Premise," Solutions Review, August 16, 2019.

[2] "2019 Data Breach Investigations Report," Verizon, April 2019.

[3] "2018 Cost of a Data Breach Study," Ponemon Institute and IBM Security, July 2018.

November 27, 2019 10:16 AM

549977-0-0-EN

sb-Dynamic-Cloud-Security-AWS