FORTINET

Dynamic Security in AWS

Creating Seamless Protection for Cloud and On-premises Networks

Table of Contents

FORTINET

Executive Summary

With 2018 revenues of $15.5 billion, Amazon Web Services (AWS) is the undisputed leader of the $32 billion Infrastructure-as-a-Service (IaaS) cloud services market.[1] One consequence of this immense popularity is that cyber criminals are aiming their full arsenal of sophisticated malware at the infrastructure, applications, and data that reside on AWS. Therefore, security architects tasked with designing, implementing, and maintaining security for AWS environments should look for comprehensive solutions that deliver multilayer protections which augment native AWS tools. Seamless cloud-native integration and workflow automation are key to enabling lean security teams to manage growing AWS footprints. Moreover, because applications and workloads (and threats) tend to move between AWS and on-premises environments, security solutions must envelop the entire hybrid network to provide consistent, centrally managed protection that reduces both operational overhead and security risk.

Opportunities and Threats in AWS

AWS offers an unparalleled range of compute, storage, database, and other services that are very easy to access and use. Due to the fact that AWS delivers high levels of performance and availability, organizations have become increasingly confident in deploying all types of applications in AWS, including business-critical applications. The cloud services provider now serves hundreds of thousands of businesses in 190 countries.[2]

The growing popularity and magnitude of AWS gives cyber criminals ever-increasing opportunities for profit, destruction, and political gain. Cyber threats are highly sophisticated, and their developers and distributors are well-funded. Appropriately, AWS invests heavily in securing its infrastructure. Its customers, however, are responsible for protecting everything they deploy in AWS. For Amazon Elastic Compute Cloud (Amazon EC2) instances, this includes the guest operating system, as well as any application software or utilities they install on the instances. Customers are also responsible for the data in their Amazon S3 storage and Amazon DynamoDB databases.[3] Pretty much anything a customer touches becomes his responsibility to secure.

The task of defining and implementing the security for cloud-based applications and workloads typically falls to the security architect. When exploring the options on the AWS platform, architects find that AWS Security Groups offer only basic firewall capabilities. But they do not provide for deep application-aware inspection or inspection of encrypted traffic. As 60% of malware uses encryption to avoid detection,[4] a great deal of malware can potentially travel between AWS and on-premises networks. On its own, AWS-native security is also less effective at preventing the lateral (east-west) movement of threats between virtual private clouds (VPCs), availability zones (AZs), and regions.

As 60% of malware uses encryption to avoid detection,[5] a great deal of malware can potentially travel between AWS and on-premises networks.

While AWS is committed to the security *of* its cloud resources, security *in* AWS—including network, applications, and configurations—is the responsibility of the customer.

AWS Requires Three Levels of Security

The nature of the expanding attack surface and advanced threats necessitates broader, more comprehensive protection. Specifically, security in AWS must include protection on three levels: network security, application security, and platform visibility and control.

Network security

As the first line of defense, network security plays a key role in securing cloud-based assets. Virtual next-generation firewalls (NGFWs) deployed in AWS provide edge security in several ways:

- They block known attack variants as well as traffic from unauthorized sources.
- Deployed as termination points for secure VPN tunnels across VPCs and locations, the NGFWs encrypt authorized traffic to ensure confidentiality and integrity.

To protect application threats in one VPC or from infecting others, security architects can leverage their virtual NGFWs to implement logical intent-based segmentation. This refers to the creation of access rules and segments based on roles and business logic.[6] The NGFWs should be able to support zero-trust access strategies by adjusting access rules dynamically in response to infrastructure changes.

Finally, for DevOps teams working in AWS, network-level defenses ensure consistent security for all stages of container deployment and rollout. This includes cloud-based NGFWs that can recognize container labels when defining security policies to follow container workload across the application life-cycle stages.

Application security

Most applications running in AWS are web applications. Using web services to connect to data and other applications, applications running in AWS need protection from threats targeting the specific application platforms and application logic, as well as those that target security gaps in user interfaces (UIs) and application programming interfaces (APIs).

Cloud-based web application firewalls (WAFs) are a key component of web application and API protection (WAAP) application security. WAFs deployed in AWS should contain dynamic rule sets that cover the Open

Web Application Security Project (OWASP) Top 10 application threats. They should also offer the ability to define and enforce application-specific business logic.

Because application access from mobile devices exposes APIs to the internet, security architects should look for WAFs that provide robust API protection. This includes dynamic virtual patching of known and unknown vulnerabilities, so that applications can keep running while the application team updates the application servers. WAFs also need to include application profiling, whereby abnormal application behavior—which may be connected to the presence of a bot—can be pinpointed and remediated.

Finally, flexibility is essential. The way in which WAFs and other security solutions are deployed in front of web applications depends on the nature of the application environments and the preferences of each development team. In order to execute an effective WAAP strategy, security architects should be able to select the most suitable form factor for each application and team. Regardless of form factor—VM, Docker container, or a SaaS solution—all deployed security solutions should work together to implement a unified security policy.

48% of all data breaches are caused by hacking of web-based applications.[7]

Platform visibility and control

The advantage that AWS brings in its expansive suite of services also creates risk. Setting up an EC2, S3, or other service is a matter of a few clicks. Configuring security settings for each service, however, requires significant attention to detail. Misconfigurations can leave easily exploitable and damaging security gaps. Even correct but inconsistent configurations can result in noncompliance with corporate security policies and regulatory privacy rules.

Because of its complexity, security configuration should not fall to business users or novice security staff members. Instead, security team experts should create CloudFormation Templates (CFTs) in AWS to impose consistent configurations on all new cloud service deployments. To minimize template creation efforts in complex AWS environments, it is a good idea to leverage trusted, prebuilt CFTs that are known to adhere to security best practices.

As the templates themselves are subject to error, and because the threat landscape and cloud environments change continually, organizations operating in AWS must implement a cloud workload protection platform (CWPP) and cloud security posture management (CSPM). To optimize cloud platform visibility and control, security architects should expect CWPP and CSPM solutions to provide:

- Configuration assessments that uncover configuration mistakes and validate configurations against best practices, compliance regimes, and corporate policies
- Comprehensive compliance reporting
- Monitoring of activity in cloud accounts as well as cloud network traffic
- Secure storage of unsolicited data to thwart the activation of any embedded malware

Data breaches caused by cloud misconfigurations jumped 424% year over year, comprising 70% of all cloud data breaches.[8]

Maximize Security While Minimizing Management Overhead

The long list of requirements for adequately securing AWS environments can be overwhelming to many organizations, especially in light of the ongoing cybersecurity skills shortage—more than 4 million positions are unfilled worldwide.[9] A comprehensive cloud security solution can help security architects alleviate this burden by enabling streamlined operations, policy consistency, unified security workflows, and deep visibility into the AWS environment.

To do so, the solution must address the dynamic nature of cloud deployments. Although many organizations are expanding their AWS infrastructure, some applications and workloads born in, or migrated to, the cloud are being brought back on-premises. This trend has been affirmed by 74% of respondents in a recent survey.[10]

Automation is essential for lean teams

Wherever applications and workloads go, security must follow. A dynamic cloud security solution must allow this to happen in real time, with minimal staff intervention. Application security and user access policies established in on-premises security devices should be automatically imported into corresponding virtual tools when these applications are migrated to AWS. The same should be true of migrations in the opposite direction. When growth within AWS necessitates additional security coverage, the security platform should provide a mechanism for auto scaling, utilizing CFTs to ensure consistent security configurations.

One console sees all, controls all

All of the AWS and on-premises security components should be visible and controllable from a single pane of glass, through a centralized security management system. This enables lean security teams to competently manage their growing hybrid-cloud security infrastructure. If security managers can initiate automated workflows in the management system, they will be able to meet various business demands that often distract them from security management, such as audit responses, internal reporting, and frequent network permissions change requests.

Cloud environments are dynamic:

74%

of companies have moved an application to the cloud and then brought it back on-premises.[11]

All security functions—from NGFWs and WAFs to CWPP and CSPM—should work the same way in AWS as they do on-premises. This minimizes cross-training requirements and ultimately reduces the cost of cloud agility.

Likewise, because organizations use a wide variety of security software tools in AWS, and security administrators grow accustomed to particular interfaces, a dynamic cloud security solution should provide pre-built integrations with those tools. This allows the security platform components to be visible and configurable from the other tools and enables seamless sharing of data and objects. In turn, this facilitates real-time enterprisewide threat detection, analysis, and response.

Securing AWS environments can be overwhelming in light of the cybersecurity skills shortage—more than 4 million positions are unfilled worldwide.[12]

Conclusion: Complete, Consistent Cloud Security

Paradoxically, the same cloud dynamic that has delivered convenience and productivity to customers and employees has heaped enormous challenges on security teams. Security architects need a dynamic security solution that will enable them and their teams to deliver any application in any AWS region or on-premises (as well as on other cloud services), while ensuring the same security everywhere.

Such a solution is necessarily broad, integrated, and automated, but it does not come from a single technology provider. Rather, it incorporates best-of-breed technologies from leading vendors and the open-source community.

[1] "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018," Gartner, July 29, 2019.

[2] "About AWS," aws.amazon.com, accessed November 20, 2019.

[3] "Shared Responsibility Model," aws.amazon.com, accessed November 20, 2019.

[4] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[5] Ibid.

[6] "A Network Operations Guide for Intent-based Segmentation: Essential Practices for Risk Mitigation and Compliance Across the Attack Surface," Fortinet, February 6, 2019.

[7] "2018 Data Breach Investigations Report," Verizon, April 2018.

[8] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

[9] "Strategies for Building and Growing Strong Cybersecurity Teams (ISC)²: Cybersecurity Workforce Study 2019," (ISC)², 2019.

[10] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, Q2 2019.

[11] Ibid.

[12] "Strategies for Building and Growing Strong Cybersecurity Teams (ISC)²: Cybersecurity Workforce Study 2019," (ISC)², 2019.

www.fortinet.com

545978-0-A-EN

November 26, 2019 7:11 AM

eb-Dynamic-Security-in-AWS