FORTINET

WHITE PAPER

Why Your AWS Cloud Environments Need Advanced Security

Executive Summary

Organizations are turning to Amazon Web Services (AWS) in vast numbers to extend internal data centers and take advantage of the elasticity of the cloud. While AWS secures the infrastructure, AWS end-users are responsible for protecting everything residing within it—as described in the AWS Shared Responsibility Model. Faced with a fluid, fast-growing attack surface, however, organizations continue to rely on a multiplicity of disparate security technologies, platforms, and management tools to protect their AWS environments.

This fragmented, complex approach to managing security across every AWS instance means that organizations lack transparent security visibility and control. They also find themselves in a reactive security mode instead of taking a proactive approach in responding to threats. Moreover, one of the reasons end-users opt for AWS is its elasticity—the ability to quickly scale up and down cloud services based on business requirements and user demands. This elasticity means it is difficult to extend and scale security components to meet this rapid change.

What Keeps AWS On Top?

AWS is shaking up the cloud computing market in the same way parent company Amazon has changed the retail landscape. Indeed, the popularity of AWS—from servers, storage, and networking to remote computing, email, and security—is such that the organization now comprises 10% of Amazon's total revenues and more than 50% of the parent company's profits[1].

AWS is also the market leader in Infrastructure-as-a-Service (IaaS), with 33% market share.[2] And its other offerings such as Platform-as-a-Service (PaaS) continue to gain momentum. It thus should be no surprise that AWS boasts a global customer base that spans the newest startup companies to Fortune 500 companies.

What makes AWS so successful? Four criteria dominate. First, AWS is innovating at lightning speed, keeping pace with industry trends and rapidly adding new services like data analytics and machine learning. Second, the organization has a vast, global customer and partner ecosystem. Third, AWS has market experience, having been among the first to market for public cloud services more than 10 years ago. Finally, there's the fiscal argument. Developing, deploying, and managing critical applications in AWS delivers a 64% savings when compared with deploying the same resources in onpremises or hosted environments.[3]

Addressing Security Challenges For Workloads With AWS

IT and business leaders welcome the adoption of AWS' on-demand infrastructure and services and are capitalizing on the promise of increased agility, lower costs, and improved flexibility. However, as often is the case with new opportunities, challenges also occur when moving workloads onto AWS. While the AWS infrastructure has embedded security tools and controls, the individual AWS environments—public, private, and hybrid—lack a consolidated security architecture. This results in various security challenges that CISOs must tackle.

1. Cloud Proliferation Creates Security Silos

The surge in demand for AWS results in a proliferation of AWS cloud environments. A survey by RightScale found that enterprises are running applications in an average of 4.8 clouds (3.1 clouds in production and experimenting with 1.7).[4] Another discovered that companies use an average of 16 cloud-based Software-as-aService (SaaS) applications to help run their business.[5] While these organizations may have other cloud providers outside of AWS, the likelihood is that they have multiple AWS instances.

When it comes to security, the result is a multi-cloud environment that leverages security within silos. When Shadow IT is added to the mix, where individual departments or teams use cloud services and applications outside of the corporate IT procurement process, the complexity of managing these multiple cloud instances, including AWS, increases.

AWS security is based on a Shared Responsibility Model. AWS is responsible for the security of the cloud, including the compute, storage, and database resources. End-users, meanwhile, are responsible for security in the cloud, such as data, applications, operating systems, and firewalls. But when security tools and processes reside within each AWS deployment, this incurs inefficiencies, diminishes the security posture, and increases complexity.

2. Lack of Security Visibility and Controls

With AWS cloud environments residing within their own silos, this prevents end-users from seeing across and between each AWS instance, not to mention having a consolidated view of the entire attack surface and security components that includes each AWS instance.

This creates manual processes for cybersecurity teams that are already overburdened, as they must build and consolidate security logs for each AWS account and deploy and manage security policies accordingly. Since there are currently 1 million unfilled cybersecurity positions today, a number that is expected to grow to 3.5 million in a few years, security leaders—even if they have budget to add more security headcount—cannot find the subject-matter security professionals needed to fulfill these additional security tasks.[6]

3. Growing, Evolving Attack Surface

Migration of on-premises infrastructure to AWS and the adoption of new digital transformation (DX) initiatives on AWS expand the attack surface. Moreover, cloud deployments aren't static, experiencing fluctuations and changes based on traffic and data volumes and business demands. As a result, it is more difficult to seamlessly extend security tools to accommodate these variables, with already overtaxed security teams typically turning to manual processes to overcome the problem.

4. Cloud Agility and Scalability Complicates Security Protections

Dynamic cloud workloads have peak and off-peak hours. Indeed, it is this scalability that makes AWS such an appealing proposition for organizations. However, the effective application of AWS cloud security requires an ability to scale up and down in concert with the workload.

But traditional security architectures don't meet this requirement. Connections between security elements and cloud silos break and must be manually reconnected. And as workloads scale horizontally, security protections can be compromised. One option to address the latter issue is to deploy more network security firewalls, but this can be prohibitively expensive, with firewalls frequently sitting idle during nonpeak sessions.

5. Threat Prevention and Detection

Many attacks are multivector and polymorphic. With separate AWS instances, organizations lack the ability to share real-time threat intelligence across their AWS environment as well as with other potential access points in their IT infrastructure—endpoints, email, data center, and so forth.

Disaggregated security also prevents security organizations from automating processes such as compliance tracking and reporting and real-time threat-intelligence sharing. Additionally, it is impossible for security teams to segment users, applications, and devices and to centrally manage security policies and controls across them. All of these issues create security gaps that hacktivists can exploit.

Conclusion

As more and more organizations migrate workloads, data, and applications to AWS, their cloud environments quickly evolve. These AWS instances present significant security challenges, as complexity escalates, visibility gets obscured, manual processes burgeon, and overall risk postures increase.

Traditional security approaches cannot scale to protect this expanding attack surface, and the lack of integration thwarts automation of processes and protections. They also cannot accommodate the rapid and evolving changes taking place in the threat landscape, where attacks target multiple entry points concurrently and zero-day threats are increasingly accessible to all types of bad actors. Security leaders are unable to extract themselves and their teams from a reactive security approach and develop a proactive security model that reduces risks.

[1] Jordan Novet, "Amazon cloud revenue jumps 45 percent in fourth quarter," CNBC, February 1, 2018.

[2] Mike Robuck, "Report: Amazon Web Services still rules the cloud roost for market share," FierceTelecom, April 27, 2018.

[3] Larry Carvalho and Matthew Marden, "Quantifying the Business Value of Amazon Web Services," IDC, May 2015.

[4] "Cloud Computing Trends: 2018 State of the Cloud Report," RightScale, January 2018.

[5] "State of the SaaS-Powered Workplace," BetterCloud, 2017.

[6] Jon Oltsik, "Research suggests cybersecurity skills shortage is getting worse," CSO, January 11, 2018.

October 9, 2019 12:41 AM

200412-A-0-EN

D:\Fortinet\White Paper\AWS Cloud Environments\wp-why-your-aws-cloud-environments-need-advanced-security