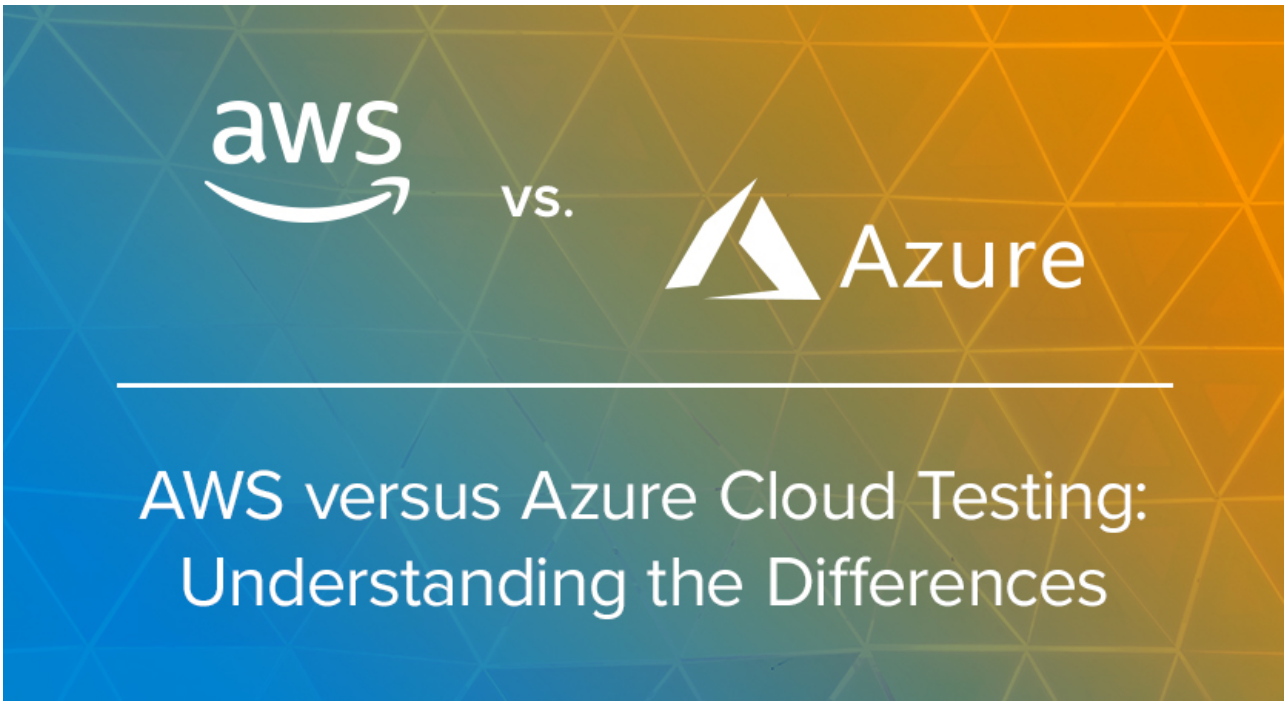
AWS versus Azure Cloud Testing: Understanding the Differences

written by Charles Horton | January 26, 2021



If your organization is currently leveraging the cloud, there's a good chance you are either using Amazon Web Services (AWS) or Microsoft Azure. Together, these two products make up 51% of the market share for cloud service providers. Given the way many cloud adoption programs operate, you might be using both. No matter which platform you're on, it is important to note that each cloud provider has its own security considerations.

First, we should cover some background around cloud computing and security. With traditional on-premise models, security teams have access to established tools, technologies, and methodologies for dealing with security events in the environment. The cloud on the other hand, has relatively fewer security tools, resources, and established procedures available, as well as an overall higher probability for data

to be exposed if a mistake is made.

As organizations migrate their resources from on-premise environments to the cloud, significant "technical debt" may also occur. Meaning there may be a lack of understanding around the technical aspects and security risks of the cloud environment. Nevertheless, organizations continue to migrate to the cloud, as its benefits often outweigh potential security concerns. Among the top reasons for cloud adoption is providing access to data from anywhere, disaster recovery, flexibility, and relieving IT staff workloads. These benefits, among others, are why organizations pay and trust cloud providers to host and manage their data and applications – but should they rely on the providers for security?

While both AWS and Azure certainly have robust cloud computing security efforts in place, it is important to understand that cloud security is a *shared responsibility* among providers and organizations. While cloud providers will provide underlying security for the platform infrastructure, the users of the platform still need to securely configure cloud services. This is where cloud pentesting becomes critical to organizations using the cloud.

Cloud Penetration Testing 101

Cloud penetration testing is used to identify security gaps in cloud infrastructures and provide actionable guidance for remediating the vulnerabilities to improve an organization's overall cloud security posture and achieve compliance [read: 4 Reasons You Need Cloud Penetration Testing]. Testing can differ between cloud platforms and knowledge of the nuances can help your organization reach cloud security maturity.

There are three main components to NetSPI's cloud pentesting methodology:

1. **Internal Testing:** Testing the internal networks and

services, much like you would an on-premise data center or on-premise network for internal virtual network vulnerabilities.
2. **External Testing**: Testing any services that may be exposed to the Internet; Services that are fully run and operated by the cloud provider, like Azure app services, or any network services that may be externally exposed through virtual machines or firewalls.
3. **Configuration Review**: An analysis of the services that are being used in a specific cloud provider to identify misconfigurations, enumerate available services and the network architecture, and learn how everything is being implemented inside of the environment. Notably, configuration review informs internal and external pentesting engagements.

For an introduction to cloud pentesting watch this webinar: Intro to Cloud Infrastructure Penetration Testing.

AWS versus Azure Cloud Pentesting

From an external and internal network pentest perspective, AWS and Azure are fundamentally similar. Some may argue that one or the other is slightly more likely to have external issues arise, but where AWS penetration testing and Azure penetration testing differ greatly is in the configuration review process. Given that they are two separate platforms, they will have different approaches for services configuration.

Let's start with Azure. As part of the migration to Azure, the on-premise Microsoft network, users, and groups (commonly tied to Office 365) are all transitioned to Azure Active Directory. As this happens, it can create situations where users from the on-premise environment are given direct, or indirect, rights to resources in the cloud. Whether users or administrators are aware, these accounts are now targets for attackers, as the attacker might have an easier time going after a non-administrative account from the internet.

While AWS can integrate (or federate) directly with Active Directory, AWS has its own Identity and Access Management (IAM) platform. The IAM system in AWS can be complicated, and if administrators are not careful, they can easily grant exploitable permissions to IAM users through policies and roles. A common target for privilege escalation in AWS is EC2 instances that are configured with excessively permissioned roles. If an attacker can gain access to the EC2 instance, they can use native AWS technology to escalate their privileges in the account.

Each of the cloud platform's vulnerabilities can be correlated with the way the identity and authorization policies are applied to the different applications and services hosted in the cloud. NetSPI's goal during a cloud penetration test is to identify these vulnerabilities and show how these issues could be practically exploited in a cloud environment.

Regardless of the platform, investing time to understand your chosen cloud provider and its architecture will help security teams avoid "technical debt", and be better prepared to efficiently find and fix vulnerabilities in any of the services specific to each cloud provider. Look for an experienced penetration testing company like NetSPI to test your Azure, AWS, or other cloud infrastructures as part of internal testing, external testing, and configuration review.