netskope

WHITEPAPER

Top 10 Amazon Web Services Security Mistakes and Solutions

With more than 30 percent of the global cloud market and a wide variety of customizable features, Amazon Web Services (AWS) has become the go-to provider of cloud services for many companies.[1] But access, ease-of-use, and the pace at which DevOps teams make changes requiring continuous monitoring of configurations go hand-in-hand with critical security concerns, as many enterprises discovered after experiencing a breach in the AWS cloud. Fortunately, there are steps you can take to keep your company secure. Follow along to learn the top 10 AWS security mistakes made by businesses and what you can do to stay safe.

With more than 30 percent of the global cloud market, Amazon Web Services (AWS) is a behemoth in the cloud sector.[2] While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Security teams need to understand their part in the shared responsibility model, where customers retain control of what security they choose to implement to protect their own content, platform, applications, systems, and networks, no differently than they would for applications in an on-site data center.[3]

The complexity of Amazon's feature-rich service means that users aren't always aware of the best security controls and practices of the system. With organizations in various stages of public cloud adoption and with different cloud maturity capabilities, an organization's maturity level combined with Amazon's speed of innovation requires focus on configurations that may be exploited in a specific context.

Learn about the top 10 AWS security mistakes people make and how you can avoid them.

#1 USING THE ROOT ACCOUNT FOR EVERYDAY ACTIVITY

The root account can be overused. Users employ them by default for day-to-day tasks, and this can create a lot of additional risk. Your root account, sometimes called a root user or superuser, by definition has full control over the account, including the ability to delete the account and everything in it. This level of access is required for certain tasks, but should be used rarely.

Everyday tasks should be delegated to user accounts with limited authority. The danger in not doing this is two-fold:

- Overuse of your root account can result in unintentional sweeping changes to your permissions, policies, settings, and more. It's like giving your dog walker your social security number and the combination to your safe, he doesn't need that much access. Most users, especially in larger organizations, can do their jobs with more limited authority.
- The more you use your root account, the more likely it is to be compromised. Once that happens, the attacker has the ability to do anything to your data, including delete it. In larger organizations, the sheer number of users raises the risk of compromise.

The good news is that AWS gives you the flexibility to partition and determine role permissions. You can use a third-party solution like Netskope to audit root user activities, and alert on poor practices, such as regular usage of a root user in an AWS account.

[1] Market Share Analysis Public Cloud Services: Public Cloud Services, Worldwide, 2016

[2] Market Share Analysis: Public Cloud Services, Worldwide, 2016

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

#2 FAILING TO PARTITION USER AND ROLE PERMISSIONS

An AWS security best practice for permissions is to grant the user only the level of privilege required to effectively do their jobs. This kind of limited role-based access might take some fine-tuning to get just right, but it effectively limits your data's exposure. You may be concerned with who can stop, start or create new EC2 instances in your AWS environment. If a particular user has an occasional need for more access beyond what you've granted them for day-to-day use, grant additional privileges for the duration of a particular task and then default back to the standard.

With Netskope, users can be assigned the granular permissions they require to perform their job and be alerted to modifications that may violate the principle of least privilege. You get visibility across your environment, can govern users with access control, and prevent risky activities like this from taking place.

#3 GRANTING GLOBAL ACCESS TO S3 BUCKETS

An Amazon S3 bucket is a public cloud storage service available in AWS Simple Storage Services (S3), an object storage offering; they can often store sensitive personal data like customer billing information. AWS users can forget to put restrictions in place, meaning that access to these containers is possible for anyone who can guess the appropriate name. The problem is compounded by the fact that Amazon issues S3 bucket names that are globally unique, meaning there's only one "JohnSmithCorp_ Customers" bucket in the cloud. Figuring them out isn't that complicated.

Without having the proper access policies in place, the data in these buckets is highly vulnerable. Adding to the complexity, Access Control for files and folders may be different from the bucket level policies. Fortunately, third-party solutions exist that can make this process easier. Netskope, for example, takes the guesswork out of S3 access by detecting S3 buckets that are open to the outside world, letting you know where and how to take the proper steps to lock them down. Verifying public access for Read/Write requires deep expertise in S3 ACLs and Netskope's solution detects misconfigurations.

#4 NOT USING MULTI-FACTOR AUTHENTICATION

Many data breaches are the result of passwords that fail to provide enough protection. Today, a single authentication at login isn't enough to keep your data safe, and multi-factor authentication (MFA) is a must. By requiring users to login using their account password and then go through a second step, you can reduce your company's risk exposure. Some common examples of MFA include:

- OTP (one-time passwords): Sending OTPs via phone or email to the user to verify their identity before completing their login.
- USB hardware tokens: Attaching a USB that generates an OTP to authenticate the user before allowing access.

AWS users looking for a way to employ MFA without adding another line item to their security budget can make use of free tools like Google Authenticator. With Netskope, it's easy to monitor if best practices like MFA are being followed. You gain a continuous security assessment of your environment to quickly identify and remediate risks. These additional steps are relatively quick and painless, and they go a long way toward securing your data.

#5 NOT ENCRYPTING DATA-AT-REST

AWS has a key-management service that lets you manage encryption keys. Ideally, users should employ the service to encrypt data-at-rest but, like a number of other AWS features, many users simply don't realize that the capability exists. Encryption best practices include specifying an encryption key and who can use it, and then locking down the key. While encryption won't prevent a breach, it ensures that your data, in the event of a breach, remains private.

Use Netskope for added layers of security to inspect objects in S3 that contain sensitive data that is left unencrypted in S3.

#6 NOT USING NETWORK ACLS

Port scans and probes are a very popular threat vector to find the weakest link to infiltrate a network.. Without implementing the proper safeguards, a lot of unnecessary, unwanted, and potentially unsafe traffic will continue to hit your security groups. These groups often act as a firewall at the instance level but the more traffic that hits them, the harder it is to effectively monitor potential threats. Using the default Network ACL allows a lot of traffic in and generates a larger number of alerts downstream, increasing the signal-to-noise ratio

What's the solution? By using more specific network ACLs you can limit that traffic and reduce the noise. For example, if you only allow SSH to originate from a certain IP block within the ACLs, you will not receive block notifications in the VPC flow logs from the instances themselves. As a result, compromised credentials could not be used from other IP addresses, and SSH scanning won't hit your instances.

With Netskope you can identify security groups with configurations that violate best practices.

#7 FAILING TO USE MONITORING AND LOGGING SERVICES

AWS provides a number of ways to help users manage, understand, and fine-tune their cloud services for increased security and all-around better operations, and the more you can learn about these methods, the better. New or non-expert users in particular should strongly consider using the following:

- **AWS Config**—helps you evaluate the configuration of your AWS resources to assist with compliance audits, operations troubleshooting, and security assessments.
- **CloudWatch**—lets you collect and track metrics, monitor log files, set alarms, react to changes automatically, and more.
- **CloudTrail**—enables auditing of risk and operations, logs and monitors account activity, provides event histories to simplify security analysis, and more. Through the AWS CloudTrail service, Netskope provides granular visibility into AWS audit logs. Netskope records logs into SkopeIT to make it easier for you to consume the information.

The Netskope Continuous Security Assessment capabilities provide deeper monitoring beyond Amazon's offerings. Continuously assess the security of your environment so you can quickly identify and remediate risks and potential vulnerabilities.

#8 FAILING TO NOTICE ANOMALOUS ACTIVITY OR ACT ON IT

Whenever a change is made in your AWS environment, you should notice and then ask why. Make use of your logs and data. Many of the steps noted in this paper will help you in your efforts to monitor your cloud activity - ACLs, for example, reduce noise to make unwanted traffic more obvious. These measures only work if you have very strict processes in place that encourage immediate proactive responses.

Netskope triggers alerts and protections as soon as aberrant activity is detected. Quickly identify compromised credentials or potential account takeover situations and other anomalies by tracking login attempts, login failures, and more. Customize anomaly detection based on specific rules or use machine-learned intelligence to identify cloud anomalies. If you don't have such a system in place to notify you of out-of-the-ordinary behavior, you might notice security issues very late in the game or not at all.

#9 NOT CHANGING YOUR SECURITY CREDENTIALS (ACCESS KEYS) REGULARLY

Compromised security credentials give a potential infiltrator access into your cloud resources. By changing out your security credentials on a regular basis, you can limit the amount of time allotted to each key and therefore the impact on your data and business. Set up a schedule and a process for rotating access keys to ensure you're limiting exposure. AWS will auto-expire and auto-renew these credentials within some applications but depending on the location of your applications, you may need to take additional steps to set up an access-key rotation process.

Developers can often hard-code access keys into their code. You can use Netskope DLP to identify access keys embedded in code and Netskope policy to restrict uploads through the AWS Admin Console or through the AWS CLI. With the Netskope Continuous Security Assessment, you have an easy way to monitor for the creation and deletion of access keys.

#10 LAUNCHING AND USING SERVICES WITHOUT UNDERSTANDING THE SECURITY IMPLICATIONS

Eager new users may jump into AWS without completely understanding them or the security implications involved. If you're new to AWS taking extra time to learn how different degrees of access play out in the real world, and which policies and procedures to put in place, can go a long way to reducing risk down the road. Start simple and then slowly build on the basic services. If you're quickly spinning up different services, it's hard to untangle what's needed and what's not and to understand what security controls need to be implemented. With Netskope's controls you get visibility into the services used via the console and the CLI.

Learn more about how you can boost your AWS security posture at www.netskope.com

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.