Top 10 Amazon Cloud Security Mistakes—and Solutions

With 31 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. But access and ease-of-use go hand-in-hand with critical security concerns, as companies like Verizon, Booz Allen Hamilton, and OneLogin discovered after being breached 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 a million clients and 31 percent of the global cloud market, Amazon Web Services (AWS) is a behemoth in the cloud sector. An early innovator in the industry, they’ve been in the Infrastructure as a Service (IaaS) business for over a decade now, and it shows in their wide array of features and offerings, and their equally impressive set of controls and security measures. But that doesn’t mean your data on AWS is not vulnerable to a security breach.

On the contrary—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. Even entities with the ability to implement large-scale security measures aren’t immune; major federal contractor Booz Allen Hamilton, for example, was recently discovered to have left 60,000 Department of Defense files unsecured on AWS. This raises the question—if an operation of this scale, presumably with significant resources and expertise at their disposal, isn’t immune to AWS security mistakes, how can the rest of us hope to stay secure?

**Fear not.** According to Colin Estep, CSO at Sift Security, there are measures you can take that will allow you to take full advantage of AWS—and stay secure at the same time.

---

**About Colin Estep, CSO**

Before joining Sift Security as Chief Security Officer, Colin served in a variety of intelligence and analysis roles for high-profile employers including Netflix, Apple, and the Federal Bureau of Investigation. He has extensive experience in incident response, forensics, vulnerability management, and cloud computing.

---

**About Sift Security**

Sift Security is a next-generation cloud security provider, helping organizations optimize their security and cloud operations, incident response, and threat-hunting teams. Sift Security can be deployed standalone or integrated with your existing SIEM platform.
“AWS provides a lot of granular controls and can really lock down specific entities and files,” says Colin Estep. “Where it falls short is when users don’t know these controls exist, or don’t have the expertise to change permissions appropriately. AWS is very flexible, but there’s a steep learning curve and the user experience could be friendlier.” To make the learning curve less steep, Estep offers his view on the top 10 AWS security mistakes people make—and how to avoid them.

Top 10 AWS Security Mistakes

1. Using the root account for everyday activity

“We see root accounts getting overused,” says Estep. “People employ them by default for day-to-day tasks, and this creates 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 rarely required. Everyday tasks should be delegated to user accounts with limited authority. The danger, according to Estep, is two-fold:

- Overuse of your root account, especially by less experienced users, can result in unintentional sweeping changes to your permissions, policies, settings, and more. It’s sort of like giving your dog walker your SSN and the combination to your safe—he just doesn’t need that much access. Most users, especially in larger organizations, can do their jobs with much 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. This might sound alarmist, but it’s happened before. And, especially in larger organizations, the sheer number of users raises the risk of compromise.

The good news is that AWS gives you lots of flexibility to partition and determine role permissions—which brings us to the next AWS mistake that people often make.
2. Failing to partition user and role permissions

“Our AWS security rule of thumb around permissions is simple,” offers Estep. “Grant the least possible degree of privilege that a user can get by with.” This kind of limited role-based access might take some fine-tuning to get just right, but it effectively limits your data’s exposure. If a particular user has an occasional periodic need for more access beyond what you’ve granted them for day-to-day use, you can always grant additional privileges for the duration of a particular task and then default back to their standard.

3. Granting global access to S3 buckets

S3 buckets are simple storage buckets used to store and organize files; they often include sensitive personal data, such as customer billing information. But AWS users frequently neglect to put restrictions in place, meaning that access to these containers is possible to 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 AWS policies in place, the data in these buckets is highly vulnerable. Fortunately, third-party solutions exist that can make this process easier. Sift Security’s product, 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.

Access to S3 buckets is possible to anyone who can guess the appropriate name. The problem is compounded by the fact that Amazon issues S3 bucket names that are globally unique. Figuring them out isn’t that complicated. Without having the proper AWS policies in place, the data in these buckets is highly vulnerable.
4. Not using multi-factor authentication

More than 60 percent of data breaches are the result of passwords failing to provide enough protection. Bottom line? Today, a single authentication at login isn’t enough to keep your data safe, and multifactor authentication (MFA) is a must. By requiring users to login using their account password and then go through a second step, you can greatly reduce your company’s 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. These additional steps are relatively quick and painless, but they go a long way toward securing your data.

5. Not encrypting data at rest

Estep recommends that users leverage encryption on the cloud wherever possible. “AWS has a key-management service that lets you manage your encryption keys,” he says. 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. According to Estep, best practices for encryption 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.
6. Not utilizing network ACLs

“Nefarious entities are scanning all the time, hoping to infiltrate the network,” says Estep. 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. The problem is that AWS’s default network access control list (ACL) allows all traffic to flow in and out of its associated subnets.

What’s the solution? By using more specific network ACLs, Estep notes, “you can limit that traffic and reduce all that 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.

You can also reduce the false positives of overly chatty firewalls by using Sift Security’s Alert Prioritization functionality. Not only does it consolidate rules, third-party alerts, and anomaly detection, but Sift’s patent-pending algorithms can also identify clusters of risk that are more likely representative of real, significant risk.

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.

Sift Security’s Alert Prioritization not only consolidates rules, third-party alerts, and anomaly detection, but Sift’s patent-pending algorithms can also identify clusters of risk that are more likely representative of real, significant risk.
• 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.

• Sift Security's CloudHunter—provides deeper monitoring beyond Amazon's offerings, with customizable rules that let you both search for known threats and use machine learning to seek out unknown threats.

8. Failing to notice anomalous activity—or act on it

“Whenever a change is made,” says Estep, “you should notice and then ask why. Make use of your logs and data.” Many of the steps noted above will help you in your efforts to monitor your cloud activity—ACLs, for example, reduce noise to make unwanted traffic more obvious. But these measures only work if you have very strict processes in place that encourage immediate proactive responses. With Estep’s help, Sift Security has built a product that will trigger alerts and protections as soon as aberrant activity is detected. 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 a way 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 they have on your data and business. Set up a schedule and a process for rotating access keys to ensure you’re limiting exposure. AWS will actually 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.
10. Launching and using services without understanding the security implications

Eager new users tend to jump right into Amazon Web Services without completely understanding them or the security implications involved—and that spells trouble. “If you’re new to AWS,” Estep says, “experiment a little before you start putting anything into production.” 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,” Estep advises. “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.”

Leverage Amazon’s Cloud—The Right Way

AWS has a lot to offer businesses, including the ability to move and store data easily, employ a remote workforce, and reduce expenditures on hardware. But the ease of online storage and infrastructure comes with associated risks.

Before diving in the deep end and committing your entire business to AWS, test the waters. Do your research—make sure you have all the necessary security tools, and invest in training. Or talk to industry experts, like those of us at Sift. If you’d like to learn more ways to keep your data safe in the cloud, we’d love to hear from you. Visit us at www.siftsecurity.com for more information.