7 Cloud Security Best Practices for Amazon Web Services

Temporary and permanent storage of data in the cloud has grown in popularity over the years. Companies like Land O'Lakes and Boeing moved their information to the cloud last year to simplify the technology they used. Video-streaming behemoth Netflix finished their journey to the cloud in early 2016 after seven years of moving systems and customer services to Amazon Web Services (AWS).

What inspired this change from on-premises storage to the cloud? Ease of use and implementation, the cost-effectiveness of the cloud over having to maintain physical servers, and worldwide access to cloud storage without being dependent on a single network or location are just a few of the positives that encourage companies to migrate. Some cloud providers, like AWS, can even scale in either direction to support growing business needs—meaning you only pay for what you use.

This transition to the cloud brings a new set of security risks to the table, though. According to Digital Guardian, you lose some control over sensitive company data once you put it in the cloud, since that data is transferred to the cloud provider, versus stored on-premises. To prevent interception of data while stored or transferred within the cloud, companies should ensure they are encrypting files during storage and transit using a managed file transfer solution like GoAnywhere MFT. The cloud also allows personal devices to connect to and interact with data, and this has its own positives (flexibility in cloud use) and negatives (compromised information if a connected device is stolen or hacked).

Amazon Web Services markets itself as a "secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow." As companies move to AWS for their cloud storage needs, they'll have the opportunity to increase their productivity and reliability as long as they maintain best practices for cloud security.

If you're getting ready to move your data to Amazon Web Services or already have, here are seven best practices for AWS we recommend getting the most out of your cloud security.

1. Document your AWS processes and procedures, then keep them updated

Imagine you have a very specific file structure set up in the cloud, complete with categorical folders that are protected by different levels of permission. You know that all company sales data should go in a specific folder, but a coworker, though meaning well, *doesn't know* and decides to transfer sales data to a different, unprotected folder. Chaos ensues.

To avoid this type of confusion, create consistent cloud practices everyone can follow. Document your AWS processes and procedures. Store them in a common space that the organization can access, like a shared drive on the internal network. And update the document every time something changes in your cloud approach to help coworkers, stakeholders, third party vendors, and trading partners remain on the same page.

2. Use AWS CloudTrail to track your AWS usage

Understanding what actions users take in the cloud is an important step toward keeping your data secure and in the hands of those you trust. Use an AWS service like Amazon CloudTrail to anticipate *and prevent* security vulnerabilities in the cloud through "governance, compliance, operational auditing, and risk auditing of your AWS account".

AWS CloudTrail can do the following tasks, and more:

- Create API call history logs
- Record when objects or data are created, read, or modified
- Calculate and give you risk reports on your cloud storage account
- Determine who makes changes to your cloud storage infrastructure
- Track who logs in to your accounts (including successful and failed login attempts)

3. Complete risk assessments as often as possible

Even though the cloud is run by Amazon Web Services, both AWS and your organization are responsible for making sure nothing falls through the cracks. This includes maintaining "adequate governance over the entire IT control environment regardless of how IT is deployed" and having "an understanding of required compliance objectives and requirements," among other things.

AWS completes and publishes risk assessments for their services, and you should do the same for the data you've stored in the cloud. Each time you give a new key player (including third party vendors and trading partners) access to your AWS cloud storage, walk through the following steps:

1. Review the risks you currently know about and ensure they're still being addressed
2. Identify and add new risk scenarios to your list. Plan for how to tackle them
3. Identify the key players who have access to AWS and ensure they're following standard security hygiene
4. Assess your AWS account. Make sure your settings, policies, and security are still relevant
5. Consider the steps you should take next to manage your data and prevent future risk

Remember, risk assessment is an ongoing process that allows you to find and address security concerns in your infrastructure. Since storing data in the cloud takes away some of your control over sensitive company information by not being on-premises, it's vital you complete assessments often to keep on top of potential security gaps and vulnerabilities.

4. Follow standard security hygiene for host and guest systems

Practicing standard security hygiene is one of the easiest ways to keep your data protected. These habits should become second nature, just like washing your hands or brushing your teeth, and will benefit you immensely without requiring much time or resources.

Enable multi-factor authentication for all accounts

Amazon Web Service's MFA requires a user to provide two pieces of information to prove they're authentic. The first piece is knowledge (something you know, your login credentials), the second is possession (something you have, an authentication code sent to an AWS MFA enabled device). Just enable multi-factor authentication for your AWS accounts to get an immediate boost in security.

Remove privileges from defunct accounts

When an employee, trading partner, or third party vendor leaves the relationship, clean out their account and delete any privileges they were given. This removes the temptation for a renegade player—or a hacker guessing at passwords and emails—to return at a later date and compromise sensitive company information.

Disable password-only access for guests

Even guest accounts should use multi-factor authentication wherever possible, even if they have limited authorities and privileges.

5. Manage and review AWS accounts, users, groups, and roles

Every so often, we recommend you review your AWS accounts, users, groups, and roles to gain a proper overview of the privileges and permissions they have. Are any of these stagnant or similar to other setups? Consider combining them. Are any of them no longer necessary? Limit the clutter. The less overlap there is, the better.

Administrators of Amazon Web Services accounts should pay special attention to the permissions listed for their S3 buckets. Several different types of access can be given to users, including list, upload, delete, view, and edit. A bucket can also be set to viewable for AWS account holders or anonymous users, which may cause high risk depending on the files in the bucket, so make sure to review your S3 buckets and permissions to avoid potential security pitfalls.

The bottom line? Provide your accounts, users, groups, and roles with the least amount of privileges they need to function. If someone needs temporary access, it's better to add them in as they're required and remove them right after to avoid information falling into the wrong hands.

6. Protect your access and encryption keys

If you're using AWS to store your data in the cloud, you're bound to have access keys and encryption keys. Access keys help AWS verify your identity against your login attempt and give you *access* to the resources you've been given. Users with different access keys may not be able to see the same things you do, so it's imperative you keep your keys safe.

Similarly, encryption keys are used to encrypt and decrypt data. Since they unlock sensitive information, keep them separate from your data. This best practice is especially important for companies who need to comply with regulations like HIPAA, FISMA, and PCI DSS. "Essentially, the

compliance requirements all say the same thing," writes Luke Probasco for Pantheon, "encryption keys should never reside in the same environment or server as the encrypted data. This is a technical way of saying, don't leave your key under the doormat a hacker walks in over."

Here are just a few ways to keep your access and encryption keys safe:

- Periodically delete any unused keys
- Use temporary access keys instead of permanent ones wherever possible. This way, if an attacker compromises an account or discovers a user's credentials, their access will be time-sensitive
- Watch the encryption key life cycle and make sure new ones are properly saved and secured
- Create procedures for worst case scenarios in the event a key is lost or tampered with

An easy way to protect your keys is to use AWS Key Management Services, the service Amazon offers that "makes it easy for you to create and control the encryption keys used to encrypt your data." AWS KMS even integrates with AWS CloudTrail, Amazon's log auditing service, so you can view logs of your key usage.

7. Secure your data at rest and in transit

When moving data between your network and the cloud, *always* encrypt your files and protect your communication using SFTP, FTPS, or SCP. Furthermore, keep them encrypted even when they're at rest, sitting in an AWS S3 bucket or on a server. You can choose to encrypt single files or entire folders depending on your needs.

A managed file transfer solution can encrypt your files both ways using modern encryption methods. Good MFT software will help you stay up-to-date as encryption standards change over time, while also making sure your data transfers are easy to manage and audit.

GoAnywhere MFT, our managed file transfer solution, integrates with Amazon Web Services in a variety of ways. To learn how GoAnywhere MFT can meet your cloud needs, check out our Amazon EC2 platform page or request a demo.