How to Maximize Your Data Security in Amazon Web Services

Devolutions

AMAZON WEB SERVICES PROVIDES A CLOUD PLATFORM FOR INFORMATION STORAGE AND DATA PROCESSING

Amazon Web Services (AWS) provides a cloud platform for information storage and data processing to millions of clients around the world, including militaries and governments. It's one of the most powerful providers out there today. The advantages of using AWS rather than purchasing physical servers may seem obvious, but securing data becomes a much larger concern in a virtual environment.

Although Amazon does provide security expertise and infrastructure, you are ultimately responsible for the security of your data. A variety of measures are necessary to keep your data protected from cybercriminals, to comply with regulatory requirements, and to generally keep your information out of harm's way. In this article, we'll look at the AWS shared responsibility model of data security, as well as some best practices to help you maximize the security of your data on AWS.

AWS Shared Security Responsibility

The AWS security model involves a shared responsibility between you and Amazon. You are responsible for user authentication, securing user access, operating systems, applications, networks, and third party integrations. Amazon, in turn, provides secure infrastructure in the following forms:

- **Built-in tools** for creating and managing security policies
- **Built-in firewalls** for Amazon VPC apps for the creation of private networks
- **Private connections** that you can enable in local environments
- **Built-in encryption** that is customizable
- **Transport Layer Security** (TLS) that works across services

AWS provides features and tools for securing the aspects you are responsible for. Nonetheless, it is up to you to keep tabs on the security configurations, implement the settings appropriately, and manage access and privileges granted to users and third party groups. You can find more detailed explanations of how to accomplish these tasks in the AWS security blog.

Best Practices

In order to maximize security, it is important to understand vulnerabilities in your configuration and figure out what practices and solutions you should apply in order to resolve them.

Secure Access Control

To start, your access control configurations should employ the principle of least privilege (POLP), which states that the rights of access and permissions are granted on a need-to-know basis. By using POLP, you prevent compromised credentials from causing more extensive damage by limiting the number of unknown users who are granted access. In addition, avoiding using the root user after the initial setup of IAM is very helpful in making sure that access is granted only to approved users.

AWS Identity and Access Management (IAM) services enable you to grant different users varying levels of access to AWS resources and APIs. You can limit some users to read-only permissions, while allowing others access to all functionality through role-based permissions.

When using IAM, it is important to create policies per role, rather than per user. This will prevent you from accidentally providing permissions to the wrong users, while simultaneously helping you more easily manage your user permissions on the whole. You should also avoid granting admin privileges unless absolutely

necessary – and always revoke privileges when no longer necessary. Use strong password policies that prevent weak and recycled passwords.

Avoid Data Loss

Protecting your data isn't just about avoiding exposure to potential attackers, as it also ensures your data remains intact. Whether due to malware attacks, human mistakes, or natural disasters, data loss can create serious financial and productivity issues. The simplest way to ensure your data remains available is to duplicate it with backups.

AWS offers several different ways to backup your data and help you avoid loss and corruption, including simple duplication of data or AWS snapshots of EBS instances. With snapshots, you can set policies dictating when backups should occur, how many should be kept, and for how long. This helps you minimize the chance that changes are lost, and it provides you with a way to quickly restore lost or failed resources.

It is good practice to store your backup in a different location than your primary service, as with any cloud service. Following the 3-2-1 rule – in which three copies are kept in two different locations, one of which is off-site – can help you ensure that even your backups remain protected.

Comply with Regulations

Complying with regulations and restrictions concerning data security can be a challenge. It is important to fully maintain these standards in order to avoid substantial fines and loss of customer trust. If you can avoid storing sensitive information such as personal or financial data, do so. If you must store sensitive information in your databases, make sure your configuration meets compliance standards, such as using appropriate encryption or following required data deletion protocols.

Many of the services provided by AWS already meet common compliance standards, including PCI, HIPAA, and GDPR. However, it is up to you to make sure everything in your account maintains all the applicable standards. This includes accounting for data stored across regions and availability zones. You can learn more about AWS compliance standards and practices at the AWS Compliance Center.

Encrypt Your Data

One of the simplest ways to avoid exposure of your data in the case of a breach is encrypting your data. You should do so for both in-transit and at-rest data. AWS has built-in features for encryption that use AES 256-bit encryption. You should always use these features, unless you have an alternative encryption service available. The specific configuration varies slightly from one AWS service to the next, but they are all fairly similar.

If you do not have an external encryption service, you may use service managed keys at no additional charge. The downside of this option is that only server side encryption is enabled. You may opt instead to use the Key Management Service (KMS) provided by AWS for an additional cost. Almost all AWS services can work with KMS, allowing easy control over encryption keys. This can be done by creating your own independent infrastructure for encryption, or by using a Customer Master Key (CMK), defined by AWS. If you choose to use CMK, AWS will exchange your master key for you on a yearly basis. The largest advantage of using KMS is that it can be used for client side as well. In order to maximize security, you should configure both server and client side encryption services.

Conclusion

It might seem like there's endless room for improvement when it comes to securing your own data. However, starting with these relatively simple practices, you can drastically improve your chances of avoiding data loss or theft. Constantly staying up to date in regards to the threats out there, properly monitoring your data and security configurations, and backing up all of your data will make sure your data remains safe and available.