sonraí SECURITY

Shared Responsibility Guide

AWS Shared Responsibility Model

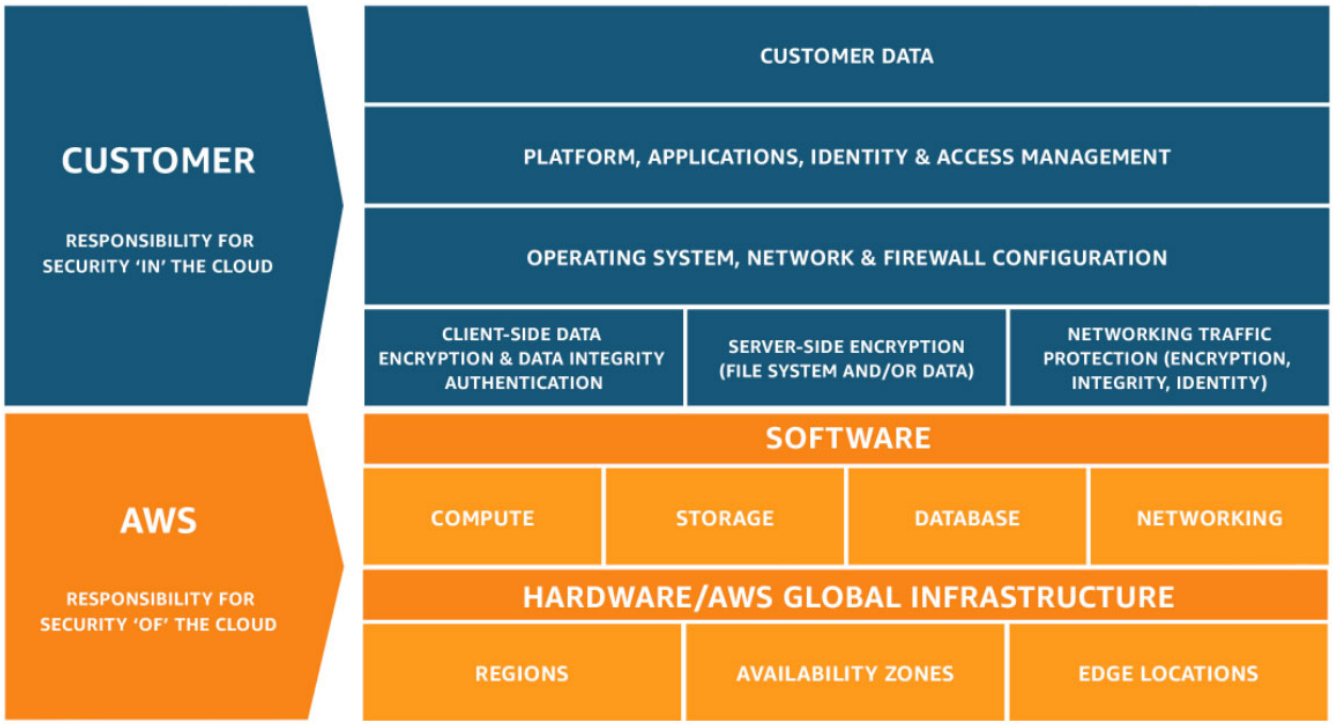
Introduction

Like most cloud providers, AWS operates under a shared responsibility model. AWS takes care of the security 'of' the cloud while AWS customers are responsible for security 'in' the cloud.

AWS has made platform security a priority to protect customers' critical information and applications taking responsibility for its infrastructure's security. AWS detects fraud and abuse and responds to incidents by notifying customers. However, the customer is responsible for ensuring their AWS environment is configured securely and data is not shared with someone it shouldn't be shared with inside or outside the company, identifying when an identity, human or non-human. misuses AWS, and enforcing compliance and governance policies.

AWS Responsibility

AWS is focused on the security of AWS infrastructure, including protecting its computing, storage, networking, and database services against intrusions because it can't fully control how its customers use AWS. AWS is responsible for the security of the software, hardware, and the physical facilities that host AWS services. Also, AWS takes responsibility for the security configuration of its managed services such as AWS DynamoDB, RDS, Redshift, Elastic MapReduce, WorkSpaces, and others.



sonraí SECURITY

Customer Responsibility

AWS customers are responsible for security in the cloud and usage of AWS services that are considered unmanaged. For example, while AWS has built several layers of security features to prevent unauthorized access to AWS, including multi-factor authentication, it is the customer's responsibility to make sure multi-factor authentication is turned on for users, particularly for those with the most extensive IAM permissions in AWS.

Furthermore, the default security settings of AWS services are often the least secure. Correcting mis-configured AWS security settings, therefore, is a low hanging fruit that organizations should prioritize to fulfill their end of AWS security responsibility.

As enterprises continue to migrate to or build their custom applications in AWS, the threats they face are no longer isolated like the old world of on-premises applications as identities are the new perimeter. Preventing many of these threats falls on the shoulders of the AWS customer.
So how are you securing your data?

Below are checklists to help you govern and secure your AWS, including but not limited to the following:

	Customer Responsibility	AWS Responsibility
Preventing or detecting when an AWS account has been compromised	✓	
Preventing or detecting a privileged or regular AWS user behaving in an insecure manner	✓	
Business continuity management (availability, incident response)		✓
Protecting against AWS zero-day exploits and other vulnerabilities		✓
Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters		✓
Providing physical access control to hardware/software		✓
Configuring AWS Managed Services in a secure manner		✓
Ensuring network security (DoS, man-in-the-middle (MITM), port scanning)	✓	✓
Ensuring AWS and custom applications are being used in a manner compliant with internal and external policies	✓	✓
Updating guest operating systems and applying security patches	✓	
Restricting access to AWS services or custom applications to only those users who require it	✓	
Configuring AWS services (except AWS Managed Services) in a secure manner	✓	
Database patching		✓

Are You Ready to Secure Your AWS Environment?

There's a lot to unpack here, and the truth is these are just a few issues you need to watch out for when using AWS. If you have questions, don't hesitate to reach out — Sonrai's technical team of security experts are standing by to help.

REQUEST A DEMO

Learn More

Sonrai Security offers a demo for AWS organizations and brings you that much closer to data security and compliance. See how we identify holes, such as excessive privilege, escalations, separation of duty, and potential risks that may arise from the identities, permissions, and data exchange within and across clouds.

Request a demo today!

sonraísecurity.com
info@sonraísecurity.com
646.389.2262

sonraí SECURITY