dash™

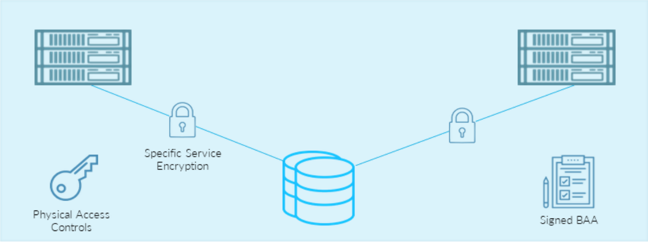
The Cloud Shared Responsibility Model

What is The Shared Responsibility Model?

Most major public cloud providers including, Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure follow a “Shared Responsibility Model” for security and compliance. This means that security and compliance are a shared responsibility between the cloud platform and the cloud customer. This applies not only for regulatory compliance such as HIPAA/HITECH, PCI DSS, and FedRAMP, but also for cybersecurity frameworks such as NIST CSF and ISO 27001. Cloud providers implement a certain set of security protections and safeguards, but customers are responsible for building secure solutions with these cloud services.

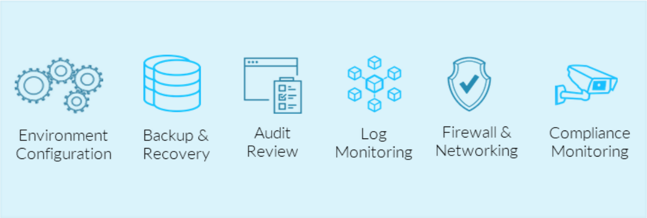
The AWS Shared Responsibility Model

The AWS Shared Responsibility Model defines security responsibilities for the cloud provider and AWS customers. This model applies to a majority of AWS security and compliance programs including HIPAA and is defined and included inside AWS Business Associates Agreement (BAA).



Cloud Platform Responsibilities

Cloud platforms are responsible for security **“OF”** the cloud



Your Organization’s Responsibilities

You are responsible for security **“IN”** the cloud

AS WELL AS

All Administrative controls and policies

AWS Responsibilities

Under the Shared Responsibility Model, AWS is responsible for **"Security OF the Cloud".** AWS will fulfill a number of HIPAA physical safeguards as well administrative reporting related to cloud services. Physical safeguards managed by AWS include:

- Signing a business associates' agreement (BAA)
- Breach notification
- Physical server security
- Facility locks and access
- Employee access to systems
- Availability of encryption

AWS cloud services have built with many security features built in. Many AWS services can be setup and configured with backup, encryption, and access control settings. These protections are provided by AWS, but ultimately become the responsibility of the cloud customer.

Cloud Customer Responsibilities

AWS cloud customers are responsible for the **"Security IN the Cloud".** This means that cloud service settings, operating systems, and applications fall under the responsibility of the cloud customer. AWS customers must implement administrative safeguards and technical safeguards in order to maintain HIPAA compliance under the AWS Shared Responsibility Model. Policies should be customized to fit your organization's technologies, and staff structure.

HIPAA Administrative Policies must include:

- A Policy for defining a Security and Privacy Officer
- Procedures for system access
- A set process for backup and disaster recovery
- Processes for incident investigation and response
- Processes for intrusion detection
- Processes for audit logging

HIPAA Technical Safeguards must include:

- Audit logging
- Anti-virus and anti-malware
- Backup and disaster recovery (DR)
- Firewall and network access
- Intrusion detection systems (IDS)
- Vulnerability scanning

Technical safeguards can be implemented using AWS services and configuration or other 3rd party tools and configuration. It is possible to use many AWS services to address these technical safeguards, but it is important to note that organizations must handle all configuration and management of these AWS services and controls.

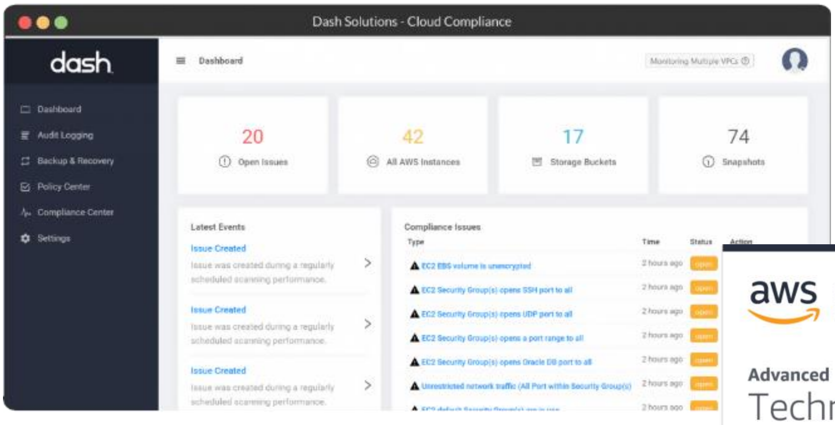
Executing on the Shared Responsibility Model

For HIPAA Compliance, organizations should take the following steps for fulfilling their role in the Shared Responsibility Model:

1. Sign the Amazon Web Services BAA
2. Create Administrative Policies and Procedures
3. Build on AWS HIPAA Eligible Services
4. Implement Technical Controls
5. Monitor, Access, and Improve Organization's Security Plan

Simplify Cloud Compliance with Dash ComplyOps

Dash ComplyOps makes it easy for organizations to address all administrative and technical safeguards required under the shared responsibility model. Organizations can use ComplyOps to build administrative policies for the organization and implement technical security controls. Dash continuous compliance monitoring scans your organization's AWS cloud environment for security and compliance issues and enables your team to quickly fix cloud security issues maintain compliance in AWS. Learn how your team can streamline your cloud security program with Dash.



20 Open Issues

42 All AWS Instances

17 Storage Buckets

74 Snapshots

Latest Events

Issue Created
Issue was created during a regularly scheduled scanning performance.

Issue Created
Issue was created during a regularly scheduled scanning performance.

Issue Created
Issue was created during a regularly scheduled scanning performance.

Compliance Issues

Type	Time	Status	Action
▲ EC2 EBS volume is unencrypted	2 hours ago	open	
▲ EC2 Security Group(s) opens SSH port to all	2 hours ago	open	
▲ EC2 Security Group(s) opens UDP port to all	2 hours ago	open	
▲ EC2 Security Group(s) opens a port range to all	2 hours ago	open	
▲ EC2 Security Group(s) opens Oracle DB port to all	2 hours ago	open	
▲ Unrestricted network traffic (All Port within Security Group(s)	2 hours ago	open	
▲ EC2 default Security Group(s) are in use	2 hours ago	open	

aws partner network

Advanced
Technology
Partner

Healthcare
Competency