Security and Compliance

AWS responsibility – Security of the Cloud

- Protecting Infrastructure (Hardware, Software, Facilities and Networking) That runs all the aws services
- Managed services like S3, DynamoDB, RDS, etc.

Customer responsibility – Security in the Cloud

- For EC2 instance, customer is responsible for management of the guest OS (including security patch and update), Firewall & network configuration,IAM
- Encrypting application data

Shared Control

- Patch Management, Configuration Management, Awareness & Training

Example Like RDS:

AWS responsibility:

- Manage the underlying EC2 instance, disable SSH access
- Automated DB patching
- Automated OS patching
- Audit the underlying instance & disks & guarantee it functions

Your Responsibility

- Check pot / IP/ Security /group inbound rules in DB's SG
- In database user creation and permissions
- Creating a database with or Without public access
- Ensure parameter groups or DB is configured to only allow SSL connections
- Database encryption setting

Example S3:
Responsibility:
AWS:

- Guarantee you get unlimited storage
- Guarantee to get encryption
- Ensure separate of the data between different customers
- Ensure AWS employees can't access your data

Your:

- Bucket configuration, policy /public setting
- IAM User and Roles
- Enable encryption

@pvnakum7
github.com/pvnakum7