# AWS Security Checklist Report

## AWS Security Checklist - Amazon Elastic Block Store (EBS)

| Item | Description |
|---|---|
| Encrypt data at rest | Encrypting your EBS volumes at rest helps protect your data from unauthorized access or disclosure in the event of theft or loss of your storage devices. |
| Use secure AWS Identity and Access Management (IAM) policies | Using secure IAM policies helps ensure that access to your EBS volumes is limited to authorized users and applications. |
| Implement backup and disaster recovery plans | Implementing backup and disaster recovery plans helps ensure that your EBS volumes are available and functional during a security breach or other disaster. |
| Monitor EBS volume activity | Monitoring EBS volume activity helps you identify potential security issues or anomalies in your EBS environment. |
| Regularly review and audit security controls | Regularly reviewing and auditing security controls helps ensure that your EBS resources are secure and compliant with your security policies. |