AWS Security Checklist Report

AWS Security Checklist - S3

Item	Description
Enable versioning	Enable versioning for your S3 buckets to protect against accidental deletion or overwrite.
Enable encryption in S3	Enable encryption for your S3 buckets to protect against unauthorized access to your data at rest.
Create IAM policies	Use IAM policies to control access to your S3 buckets and objects.
Enable object lock	Enable object lock to prevent objects from being deleted or overwritten for a defined retention period.
Enable bucket logging	Enable access logging on your S3 buckets to monitor and analyze access patterns and identify potential security risks.
Enable CloudTrail integration	Integrate your S3 buckets with AWS CloudTrail to capture and store data events for auditing and compliance purposes.
Enable AWS Config	Enable AWS Config to continuously monitor and record your S3 bucket configurations and evaluate them against best practices.
Set up S3 event notifications	Configure S3 event notifications to send messages when specific events occur in your S3 buckets, such as object creation or deletion.
Implement bucket policies	Use S3 bucket policies to manage permissions at the bucket level, controlling access to all objects within a bucket.
Set up CORS configurations	Configure Cross-Origin Resource Sharing (CORS) to control which origins can access your S3 buckets and objects.
Enable MFA Delete	Enable Multi-Factor Authentication (MFA) Delete to require additional authentication when deleting objects or changing bucket versioning settings.
Enable transfer acceleration	Enable S3 Transfer Acceleration to improve data transfer speed and reduce latency for your S3 buckets.
Implement bucket tagging	Use bucket tagging to organize and manage your S3 buckets and enable cost allocation tracking.
Configure lifecycle policies	Set up lifecycle policies to automate the management of objects in your S3 buckets, such as transitioning objects to different storage classes or deleting objects.
Implement public access blocking	Use S3 Block Public Access settings to prevent public access to your S3 buckets and objects.
Use VPC endpoints	Create VPC endpoints for Amazon S3 to securely access your buckets over a private network connection.

This report has been generated by awscheck.fyi