AWS Security Checklist Report

AWS Security Checklist - AWS Compute Optimizer

Item	Description
Enable encryption for Compute Optimizer data	Enabling encryption for Compute Optimizer data at rest helps protect sensitive information from unauthorized access or disclosure.
Enable AWS CloudTrail logging for Compute Optimizer	Enabling AWS CloudTrail logging for Compute Optimizer helps you monitor and audit changes to your Compute Optimizer resources.
Limit access to Compute Optimizer	Limiting access to Compute Optimizer helps prevent unauthorized access and limits the impact of security breaches.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Compute Optimizer resources are secure and compliant with your security policies.
Ensure data accuracy	Ensuring data accuracy helps Compute Optimizer provide accurate recommendations and avoid potential security issues.

This report has been generated by awscheck.fyi