AWS Security Checklist Report

AWS Security Checklist - API Gateway

Item	Description
Use HTTPS	Use HTTPS instead of HTTP for all API requests to encrypt data in transit and prevent man-in-the-middle attacks.
Enable API Gateway Logging	Enable logging to Amazon CloudWatch Logs to help with security analysis, change tracking, and compliance auditing.
Restrict Access with API Gateway Resource Policies	Define resource policies to restrict access to your APIs, based on IP address, Amazon VPC endpoint, or other attributes.
Use AWS WAF with API Gateway	Use AWS Web Application Firewall (WAF) with API Gateway to protect against common web exploits such as SQL injection and cross-site scripting (XSS).
Implement Authorization with API Gateway	Implement authorization with API Gateway to control who can access your APIs and what actions they can perform.
Protect Against Denial-of-Service (DoS) Attacks	Configure rate limiting, throttling, and caching to protect against DoS attacks and to ensure high availability and performance.
Use API Gateway Access Logging	Use access logging to track and monitor requests to your APIs, and to help with troubleshooting and compliance auditing.
Secure API Gateway Credentials	Use AWS Secrets Manager or AWS Key Management Service (KMS) to securely manage API Gateway credentials such as API keys and client certificates.

This report has been generated by awscheck.fyi