Salt Security Discovery Solution Brief

Overview

APIs have fundamentally changed in recent years. Due to the push for digital transformation, the number of APIs has exponentially grown and significant sensitive data is increasingly being exposed. This exponential growth has resulted in an enormous attack surface that has emerged virtually overnight. Adding to the challenges, applications have moved from long release cycles to agile development with a CI/CD model resulting in a continuously changing attack surface. Security teams that are unaware of APIs and sensitive data exposure cannot properly protect applications from potential attacks.

Current challenges without complete API discovery

Protecting what you don't know

API documentation is critical for security teams to understand the data and functionality that each API is exposing but, developer created OAS/Swagger documentation often lacks needed details and in some cases does not exist at all. OWASP defines Improper Assets Management as top risks in the API Security Top 10. Without proper visibility, security teams have an unknown attack surface and cannot fully assess risk leaving Shadow APIs and unknown vulnerabilities.

Identifying exposure of sensitive data

PII, authorization tokens, and other sensitive data, are increasingly being exposed through APIs and are rich targets for attackers. OWASP defines Excessive Data Exposure as a top risk in the API Security Top 10. Compliance, privacy regulations, and risk assessment requires knowing your sensitive data exposure points but can be challenging given the number, complexity, and interconnected nature of APIs.

Maintaining visibility despite rapid changes

Innovation demands and development practices like CI/CD, drive constant and frequent changes to APIs. These practices often result in unknown or Shadow APIs being released to production or existing APIs being updated without informing security teams all of which create unknown exposure, an unknown attack surface, and additional risk.

Salt Security Discovery

Salt Security Discovery protects you from the OWASP API Security Top 10 threats by automatically and continuously finding all known and unknown APIs in use across your environments. This helps to eliminate blind spots, determine sensitive data exposure, and keep APIs protected even as your environment evolves and changes.

With Salt Security Discovery, you will:

Achieve comprehensive visibility

Automatically discover all public, private, or partner-facing APIs with granular details down to the parameter level. This not only verifies the accuracy of manual inventory efforts, but also eliminates Shadow APIs and Shadow API Endpoints to help improve visibility of your complete API attack surface.

Discover and report your sensitive data

Identify all PII, tokens and other sensitive data that flows through your APIs across all environments. This helps ensure that no sensitive data is unknowingly exposed and helps demonstrate compliance to auditors.

Maintain up-to-date API inventory

Gain a current view of all APIs in your production environment by continuous discovery. This helps you see APIs as they are deployed, stay up to date even as frequent changes are made, and verify that all APIs meet security requirements at all times.

Customer examples

City National Bank uses Salt Security Discovery to maintain an up-to-date, comprehensive inventory of all APIs in their application environment. This helps their security team perform regular risk assessments of new APIs as they are deployed and gain an understanding of where PII and other sensitive data is being exposed. This also helps security work more efficiently with development teams while not getting in the way of rapid development cycles.

Payoneer uses Salt Security to fill in the gap they have with incomplete or missing OAS documentation. This has eliminated Shadow APIs and Shadow Endpoints while improving the security team's view of APIs, sensitive data exposure, and risk. In addition, dependencies on development to provide comprehensive documentation has reduced while giving security more visibility into APIs through the release process.

Next steps

Find out how Salt Security prevents API attacks with a simple to deploy solution that requires no configuration or customization.
Discover all of your known and unknown APIs, stop attacks in real time, and quickly eliminate vulnerabilities.

Request a demo today: salt.security/demo/