Salt Security Remediation 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. Eliminating vulnerabilities is critical to keeping APIs secure, but can be a daunting task with the average organization managing hundreds of constantly changing APIs.

Current challenges remediating API vulnerabilities

Identifying security gaps in APIs

Detecting attacks requires different skills and efforts compared to identifying API security gaps that need remediation. It is one thing to identify and block a brute force attack and yet another to understand the rate-limiting mechanism is flawed. Blocking attackers without continuously improving your API security posture is a never ending battle.

Improving developer security awareness

Developers struggle to find the balance between rapid development and keeping up with security best practices. With complex and unique logic in APIs, standard security best practices do not always directly translate. Additionally, developers who build functionality do not think like attackers, who look to make APIs perform in unintended ways.

Limited development resources

Development teams can be overwhelmed by the number of API vulnerabilities that need to be addressed. It is crucial to identify the highest priority vulnerabilities attackers might exploit but can be difficult to separate them from other lower priority theoretical vulnerabilities. This often leaves high priority vulnerabilities open while increasing risk.

Salt Security Remediation

Salt Security Remediation helps security and development teams find balance to support rapid innovation and efficient elimination of API vulnerabilities. With detailed insights, development teams understand why a vulnerability exists and exactly where it exists in the API so they can quickly prioritize and eliminate risk.

With Salt Security Remediation , you will:

Improve your API security posture

Use attacker efforts during reconnaissance as they probe your APIs for vulnerabilties giving development teams insights to eliminate vulnerabilities before they are exploited. This complements current efforts by finding high priority vulnerabilities missed by other solutions like penetration testing, security testing, and scanning.

Release more secure APIs

Receive continuous feedback and detailed insights to improve security awareness for best practices to minimize future vulnerabilities. Developers receive details on what is vulnerable in the API and how to close the gaps with simple instructions. Insights can be integrated with ticketing systems like Jira to route remediation tasks to the right team and bridge the gap between security and development teams.

Focus on vulnerabilities that matter

Help development teams focus on real attack attempts that uncover high priority threats where remediation efforts will have the most impact. This is unlike output from scanning solutions that include many theoretical threats.

Customer examples

AppsFlyer uses Salt Security to improve remediation workflows by sending insights generated by Salt Security to the appropriate developer so they can quickly resolve API vulnerabilities. With this process and additional detail, they've seen remediation times go from days to hours while reducing the new vulnerabilities in new releases.

A Celsius Networks uses Salt Security Discovery Insights to enrich their security testing tools and enable comprehensive testing of their APIs. Remediation instructions are generated when a vulnerability is detected and used by development teams to resolve vulnerabilities before releases move to production. This integration helped automate and speed up remediation while also improving education developers to reduce new vulnerabilities.

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/