SALT

PROTECT YOUR SAAS, WEB AND MOBILE APPLICATIONS FROM API BREACHES

THINK YOU'RE PROTECTED? THINK AGAIN.

APIs are found at the core of every SaaS, web, mobile, microservices and IoT application and as API use has exploded the quantity and exposure of sensitive data has increased. With this, API attacks have become more frequent and more complex, making them the number one threat for organizations delivering applications. The market has already seen a huge increase in API attacks over the past few years, including breaches at Facebook, T-Mobile, Panera Bread, Verizon, and vulnerability disclosures at Uber and the United States Postal Service (USPS).

The Open Web Application Security Project (OWASP) has recognized API breaches as an increasing concern and released the first ever OWASP API Security Top 10 outlining the top threats for APIs.

Discovering APIs is Step One

"The first difficulty [Protecting APIs is] actually finding and discovering the APIs" says Gartner's Mark O'Neill. Not knowing the APIs that exist and the sensitive data that they expose presents unknown risk for organizations and leaves security teams at a disadvantage. Teams need ways to discover known and unknown APIs as well as new APIs as they are released.

Current Solutions Don't Protect Against Increasing API Attacks

Gartner says "Protecting web APIs with general-purpose application security solutions continues to be ineffective". This includes proxy-based solutions which only have a narrow view and are limited to known attacks. Preventing API attacks requires deep understanding of API logic and every unique API behavior, both of which can only be achieved with big data to unlock the full power of artificial intelligence (AI).

Remediating Vulnerabilities To Eliminate Risk

Remediating API vulnerabilities is critical to keeping APIs, applications, and data secure. Understanding where vulnerabilities are and properly prioritizing for remediation can be challenging for development teams tasked with delivering new code under tight deadlines. Efficient remediation requires clear, prioritized and actionable insights for developers.

A new approach to API security is needed – one that leverages big data and AI to deliver API discovery, attack prevention and vulnerability remediation.

USE CASES

API Inventory

Dynamic discovery of all public, private or partner facing APIs and applications in your environment

Account Takeover

Prevent account takeover that can lead to account misuse

Compliance

Identify APIs exposing PII data relevant to GDPR, PSD2, PCI-DSS, HIPAA

Service Disruption

Stop attackers from taking down your applications and services even with a single API call

Data Exfiltration

Protect critical company and customer data from mass downloads and data exfiltration

API Vulnerabilities

Efficiently identify and eliminate API vulnerabilities with clear and actionable insights for developers

THE SOLUTION

Detect and prevent API attacks with the power of AI.
Deploys in minutes. No configuration required. Ever.

Discovery

Inventory All Your APIs And Eliminate Blind Spots

Find all known and unknown APIs across your environments automatically and continuously for a complete inventory. This helps you eliminate blind spots, assess risk, determine sensitive data exposure (e.g. PII) even as your APIs evolve and change.

Prevention

Stop Attackers Early During Reconnaissance

As attacks evolved from a single malicious call to a series of distributed events, there is a need to connect these events to a single attack source. At the core of the Salt Security solution is big data and patented AI to enable the collection, analysis and correlation of millions of users and their activity in parallel. This allows the solution to piece together the subtle probing of an attacker during reconnaissance to identify and stop them early in the process.

Remediation

Eliminate API Vulnerabilities At Their Source

Bridge the gap between security and development teams to efficiently eliminate vulnerabilities. Leverage each attacker as your personal pen-tester and gain valuable insights from real attacks so development teams understand where and why vulnerabilities exist so they can be quickly prioritized and eliminated.

QUICK SETUP, NOT INLINE, NO CONFIGURATION NEEDED

Unlike common, intrusive proxy deployments that add latency and can cause service disruption, Salt Security has a DevOps friendly setup. The solution is not inline and has a variety of quick and easy setup options including API gateway integrations, sensors, containers (Docker, Kubernetes, etc.) and support through traffic mirroring on-prem or from the cloud.

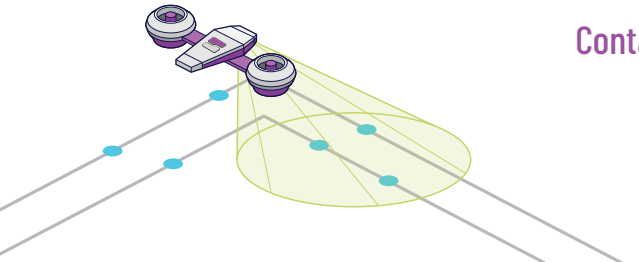
WHY NOW?

APIs are at the core of innovation for your SaaS, web, mobile, microservices and IoT applications. With the quantity and exposure of sensitive data transmitted across these environments increasing, API attacks have become more frequent, more complex, and the number one threat for any company delivering applications. Without Big Data and AI, traditional solutions have a narrow view and completely miss modern API attacks including the new OWASP API Security Top 10 threats. Don't wait until you're breached - discover what you don't know and stop attackers before they are successful.

WHY SALT SECURITY?

Today's security solutions work based on proxy architectures, depend on signatures and detect only known attacks (e.g. SQLi, XSS, etc.). They also require constant configuration and produce heaps of false positives. Current API attacks are inherently sophisticated, target unique application logic, and are completely missed by your current security stack. Salt Security protects you from the OWASP API Security Top 10 threats and more with a patented solution that uses big data and AI to detect and stop attacks in real time, before they are successful.

SALT



Contact us now to start discovering what you don't know.

contact@salt.security
https://salt.security