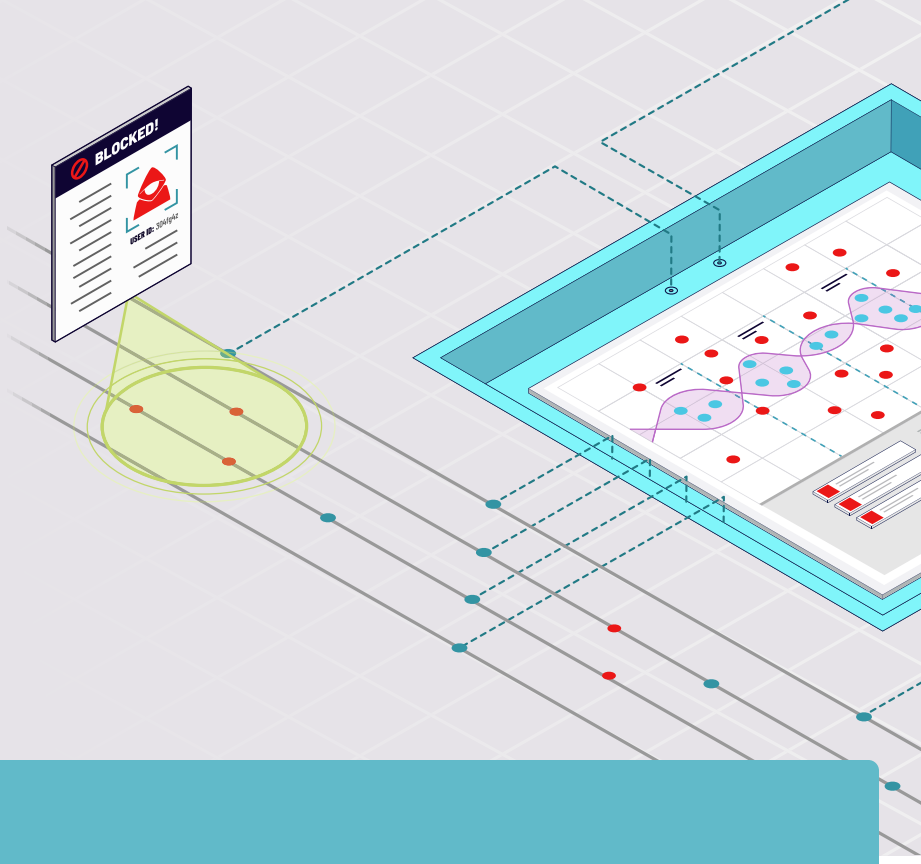
Salt Security Prevention Solution Brief



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 depend on manual efforts and traditional tools will not be able to protect applications from the new breed of attacks targeting APIs.

Current challenges preventing API attacks

Inadequate protection

The behavior of each API is unique and gaining a deep understanding of this behavior is essential to preventing API attacks. Traditional, proxy-based tools like WAFs and API gateways look at each API call in isolation and lack this understanding. They are limited by architecture to detecting only known attacks (e.g. SQL Injection, XSS) and miss the overwhelming majority of API attacks. Detecting and stopping API attacks requires looking beyond a single API call, analyzing large amounts of data, and the ability to piece together attacker activity into a clear picture.

Protecting rapidly changing APIs at scale

APIs are a core component of all modern applications and an important part of rapid development practices like continuous integration and continuous delivery (CI/CD). Security approaches and tools that depend on humans to define and maintain manual knowledge simply cannot keep up with the increasing use of APIs and constant rate of change in API environments.

Responding to attacks with confidence

Unlike developers, security teams typically do not have a deep understanding of APIs and their unique behavior. Identifying high priority alerts is a constant challenge due to this lack of understanding, and the need to dig through endless alerts to remove false positives. Once malicious activity is detected, security teams struggle to connect all needed information to gain a big picture, pinpoint attackers, and take action with confidence without heavy dependency on other teams.

Salt Security Prevention

Using big data and patented artificial intelligence (AI) Salt Security analyzes the activity of millions of users in parallel, creates a baseline of legitimate behavior and pieces together the subtle probing of attackers to identify and stop attacks early during reconnaissance.

With Salt Security Prevention, you will:

Protect against top API threats

Leverage big data and patented artificial intelligence (AI) to analyze API traffic and establish a granular baseline of legitimate behavior for your unique APIs. Subtle, malicious activities that fall outside the baseline are pieced together to identify attackers and stop them early during reconnaissance before attacks are successful. Salt Security requires no configuration to create the baseline and does not rely on signatures to keep your APIs protected.

Maintain protection despite changes

Continuously analyze API activity to distinguish between legitimate API changes and malicious activity. Salt Security adapts as your APIs change allowing you to maintain protection in rapidly changing CI/CD environments without the need to update security policies or require other human intervention.

Stop attacks with confidence

Salt Security correlates all attack activity from the same user into a single alert, with a clear attack timeline, even as attackers obfuscate their activity across many IDs, IPs, and devices. The attack timeline provides complete context to allow security teams to respond with confidence to attacks without the need for deep API expertise and without dependencies on development teams insights.

Customer examples

Finastra is able to quickly detect malicious activity in their APIs that requires user behavioral analysis and is missed by their WAF and API Gateway. This allows their SOC team to pinpoint the source of the activity, use **details provided by Salt Security to block the user in question, and stop the attack before it advances.**

Equinix uses Salt Security to maintain protection for their customer-facing dashboard. Despite the constant and active rate of updates, Salt Security discovers and automatically protects APIs so Equinix can provide their customers with updates and innovative features while keeping their service and customer data secure.

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/