Web Application Firewalls and API Security

Overview

Web Application Firewalls (WAFs) are proxy-based tools that inspect HTTP traffic to monitor, filter, and block malicious HTTP activity. These tools depend on signatures and are best used to prevent attacks exploiting known vulnerabilities.

WAF - attributes

- Inline proxy
- Dependent on signatures to identify attacks
- Require configuration for customization
- Must be kept up to date to detect new attack types and when application changes are made

WAF - attack types prevented

- SQL Injection (SQLi)
- Cross Site Scripting (XXS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Remote Code Execution (RCE)

What's needed to protect APIs

WAFs provide some protection against application attacks, but architecture limitations prevent WAFs from protecting against the top API threats, including those defined in the OWASP API Security Top 10. These top threats target the unique logic of each API and cannot be identified by signatures or even by customizing a WAF's protection with configuration. Making matters worse, most managed WAF rulesets are tailored to mainstream commercial and open-source software packages like the content management systems Drupal and Wordpress. These are not where organizations typically build or integrate APIs, so managed rulesets provide only minimal protection.

Protecting APIs from threats requires analysis of all API traffic to gain the context needed to identify and stop attackers. A WAF's proxy architecture limits the ability to see the big picture - instead, WAFs provide protection one transaction at a time. Without broader context, and the ability to stitch together disparate activities from a single user, a platform cannot stop attacks in progress, for example.

To fully protect APIs, organizations need:

- **Simple deployment** – no agents, no proxy, no app changes or performance impact
- **Automation** – establish baselines and adjust to changes with no tuning or configuration
- **Broad reach** – see all your APIs, even those deprecated or not in gateways or documentation
- **Deep analysis** – correlate activity, find what's new, distinguish "bad" vs. "safe" different
- **Enforcement** – tap the "low and slow" attack pattern to stop attackers before they succeed
- **Full lifecycle coverage** – protect and improve APIs across build, deploy, and runtime

Salt Security - a unique architecture for securing APIs

At its core, the Salt Security solution is architected to leverage big data and patented artificial intelligence (AI) to enable the collection, analysis, and correlation of millions of users and their activity in parallel. By virtue of this architecture, the Salt Security solution can holistically see the subtle probing by attackers during the reconnaissance phase. Equipped with this capability, you can identify and stop them early in their attack methodology, avoiding a security incident or breach.

The Salt Security API Protection Platform works with any WAF, API gateway, development platform, and cloud environment to provide complete protection of APIs, including defending against the threats defined in the OWASP API Security Top 10 list.

Discover all your APIs

- Dynamically inventory all APIs, including shadow, zombie, new, and changed APIs
- Catalog exposed PII and other sensitive data to meet PSD2, PCI-DSS, GDPR, and CCPA requirements

Stop attacks

- Correlate anomalous activity to identify attackers
- Pinpoint attacks early, during the reconnaissance phase, and shut down the attacker
- Cut incident response from hours to minutes with a comprehensive attack timeline view

Remediate vulnerabilities

- Share remediation details with DevOps to eliminate vulnerabilities in APIs
- Continuously harden APIs during development to ensure security doesn't slow application rollout

> *"[The Salt Security Solution] contrasts with many other API management solutions that require manual configuration, such as API throttling limits, thus providing protection of APIs only after an attack has already been mounted – which is too late."*

Mark O'Neill
VP Analyst, Gartner

Gartner

Salt Security customers include:

ally
EQUINIX
FINASTRA
cross river
TripActions
ARMIS

Salt Security protects the APIs that are at the core of every modern application. The company's API Protection Platform is the industry's first patented solution to prevent the next generation of API attacks, using behavioral protection. Deployed in minutes, the AI-powered solution automatically and continuously discovers and learns the granular behavior of a company's APIs and requires no configuration or customization to prevent API attacks.

Request a demo today!
info@salt.security
www.salt.security

SALT