WAAPs and API Security

Overview

Web Application and API Protection (WAAP) products are application security tools that combine capabilities including Web Application Firewall (WAF), Distributed Denial of Service (DDoS) protection, Bot Mitigation, and some level of API protection. These tools are based on proxy architectures and inspect HTTP traffic to monitor, filter, rate limit, and block malicious HTTP activity. Given the nature of combined feature sets, particularly DDoS protection, they are typically offered by cloud and CDN providers. These tools depend on signatures and are best used to prevent attacks exploiting known vulnerabilities.

WAAP - attributes

- Inline proxy
- Combination of application security capabilities
- Dependent on signatures and configuration to identify and stop attacks

WAAP - attack types prevented

- SQL Injection (SQLi) / Cross Site Scripting (XXS)
- Distributed Denial of Service (DDoS)
- Credential Stuffing
- Content Scraping

What's needed to protect APIs

WAAPs provide protection against a wide variety of application attacks, but architecture limitations prevent WAAPs 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 WAAP's protection with configuration. Making matters worse, most managed WAF rulesets within WAAP 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. Bot mitigation features of WAAPs may not be designed with API context in mind, focusing instead on broader web application attacks or well-known bot and botnet signatures. API security features of WAAP are often limited to enforcement against API schema definitions like Open API specification or Swagger. In many organizations, such API documentation is often incomplete, not produced at all, or not made available to security teams.

Protecting APIs from threats requires analysis of all API traffic to gain the context needed to identify and stop attackers. A WAAP's proxy architecture limits the ability to see the big picture - instead, WAAPs 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