SALT

SOLUTION BRIEF

API Gateways and API Security

Overview

API gateways provide API management and other business capabilities, and many offer some security features that provide basic protection.

API gateways — management features

API gateways are proxies used for mediating APIs with capabilities that include:

- **Usage monitoring**
- **Access control enforcement**
- **Front-end and back-end service aggregation and composition**

API gateways — security features

Some API gateways have basic security features that include:

- **Access control (authentication and authorization)**
- **IP allow/block lists**
- **Message filtering**
- **Transport encryption**
- **Rate limiting**

What's needed to protect APIs

API gateway security features are important components of an overall API security strategy, but they do not provide protection against the top API threats, including those defined in the OWASP API Security Top 10. Even authenticated APIs are targeted by attackers using subtle methods to uncover and exploit vulnerabilities. Traditional access controls, block lists, and message filtering provided by API gateways leave you with only partial protection.

Protecting APIs from threats requires analysis of all API traffic to gain the context needed to identify and stop attackers. The proxy architecture of API gateways limits their ability to see the big picture - instead, they 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 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."

Gartner

Mark O'Neill,
VP Anaylst, Gartner

Salt Security customers include:

ally

EQUINIX

FINASTRA

ARMIS

TripActions

cross river

Salt Security protects the APIs that form the core of every modern application. Its patented API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and shift-left practices. Deployed in minutes and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives.

SALT

Request a demo today!

info@salt.security

www.salt.security