

## APIs - the dominant target in today's application environments

APIs are at the heart of today's modern applications, helping organizations connect with customers and partners, drive revenue, and innovate with digital transformation initiatives. APIs have also become the top application target for attackers, as countless high-profile breaches show. The Gartner prediction that "by 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications" has certainly come true. Traditional solutions including WAFs and API Gateways alone cannot protect your APIs against today's attacks, even if deployed on the leading cloud platform AWS.

### What happens when hackers target APIs?

- Data exfiltration
- Account takeover
- Service disruption
- Fraud
- Data loss
- Account misuse
- Service outages


## Introducing Salt Security

The Salt Security API Protection Platform secures your APIs across the full API lifecycle, regardless if your APIs are deployed in AWS or also on-premises. The Salt platform collects a copy of API traffic across your entire application landscape and uses big data, machine learning (ML), and artificial intelligence (AI) to discover all your APIs and their exposed data, stop attacks, and eliminate vulnerabilities at their source. The Salt platform:

- **Discovers all APIs and exposed data** – Automatically inventory all your APIs, including shadow and zombie APIs, and highlight all instances where your APIs expose sensitive data. Continuous discovery ensures your APIs stay protected even as your environment evolves and changes with agile DevOps practices.
- **Stops API attackers** – Pinpoint and stop threats to your APIs by identifying attackers early, during their reconnaissance phase, and prevent them from advancing. The Salt platform correlates activities back to a single entity, sends a consolidated alert to avoid alert fatigue, and blocks the attacker rather than transactions.
- **Improves your API security posture** – Salt proactively identifies vulnerabilities in your APIs even before they serve production traffic. The platform also uses attackers like pen testers, capturing their minor successes to provide insights for dev teams while stopping attackers before they reach their objective.

### Who uses Salt

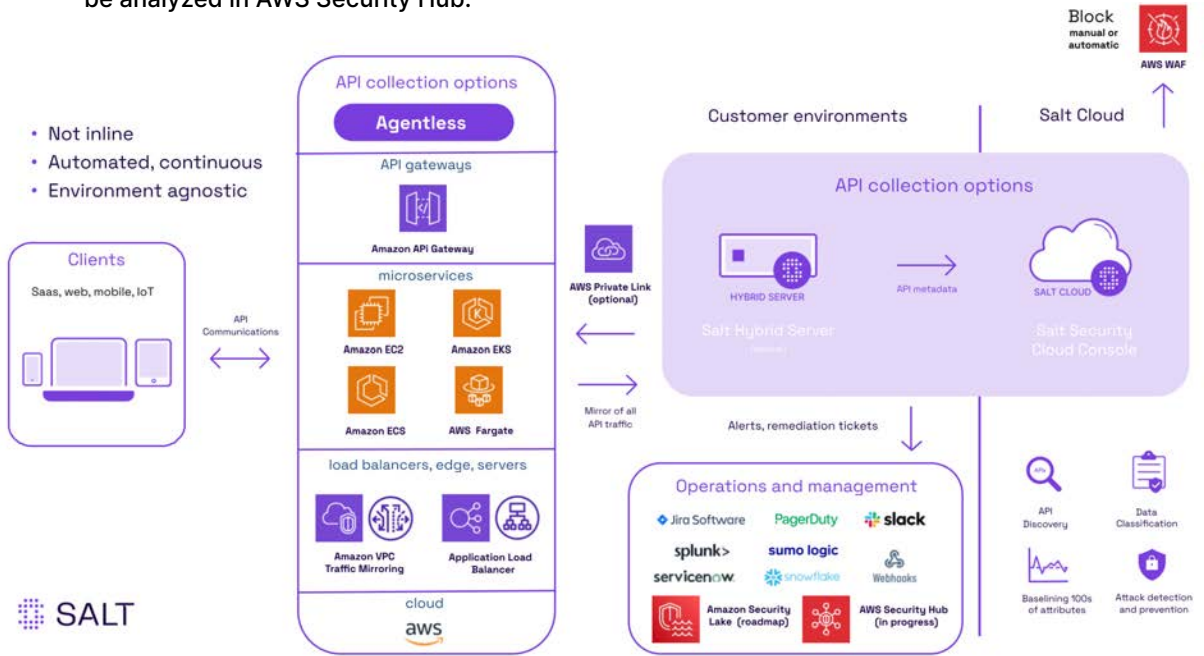
- Organizations of all sizes in every industry that build APIs to power customer-facing, partner-facing, and internal applications. We especially lead in FinTech, FinServ, Tech SaaS, and Pharmaceutical companies.
- Organizations that need to prevent API attacks to protect business-critical applications and customer data.
- Organizations that need to understand risk, meet compliance requirements, and eliminate API vulnerabilities.

### Benefits of Salt deployed on AWS

- Identify and stop attackers early, during the reconnaissance phase, before they can advance
- Eliminate blind spots with a continuously updated catalog of all known and unknown APIs across environments
- Protect against low-and-slow attacks and latest OWASP API Security Top 10 threats
- Integrating with AWS native compute, network and security services, Salt reinforces Amazon API Gateway and AWS WAF with contextual API security capabilities

# Salt in action

The Salt platform deploys flexibly in your AWS environment with no agents and no code changes. We get a copy of your API traffic through AWS and 3rd party service integrations, then send API metadata into the Salt Platform (built as SaaS on AWS). You get actionable API security insight from Salt, which can be used in AWS WAF to block malicious IPs, or can be analyzed in AWS Security Hub.



## How Salt helps your bottom line

The Salt platform saves your team significant time and effort in identifying and addressing API security gaps.

33%

Fewer undocumented APIs

20x

Faster to resolution

96%

Fewer alerts

3x

Faster API remediation

75%

Time savings for compliance

## Get the peace of mind your peers enjoy

We're proud of the customers we've been able to protect, enabling them to drive business innovation through their APIs.



**Salt Security** protects the APIs that form the core of every modern application, built as a secure SaaS platform on AWS, for customers using AWS as their mission critical cloud platform. Salt's patented API Protection Platform is 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.



**Request a demo today!**  
[info@salt.security](mailto:info@salt.security)  
[www.salt.security](http://www.salt.security)