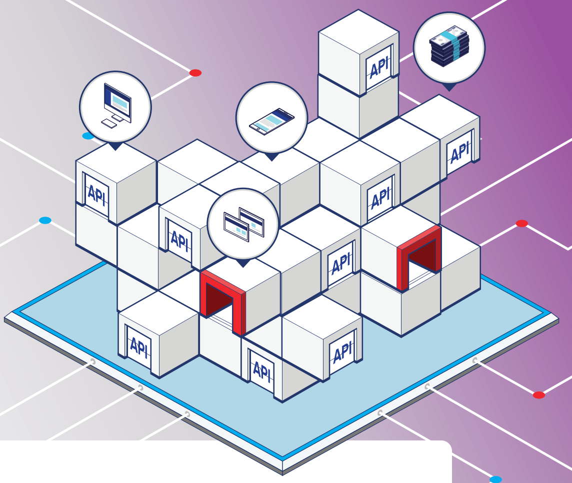
SALT



Never worry about your APIs again

APIs are the dominant target in today's modern app landscape

APIs have been around for over two decades and have evolved significantly since the early days. In recent years, use has exploded, with APIs becoming increasingly prevalent in the application environments of all businesses to enable rapid development, fuel digital transformation, and connect customers and partners with services.

APIs today expose more sensitive data than ever before, making them a valuable target for attacks and organizations are becoming aware of the need for API security. Traditional tools like web application firewalls (WAFs) and API gateways are limited by architecture and lack the context required to identify and stop attacks targeting APIs.

Why API security is harder and more critical

Increased use of APIs, growing the attack surface	Greater exposure of sensitive data	More frequent API changes thanks to agile development

Salt - the context you need to protect all your APIs

Salt Security protects the APIs that form the core of every modern application. Only Salt provides the architecture needed to protect APIs across build, deploy, and runtime phases. The Salt C-3A Context-based API Analysis Architecture combines complete coverage with an ML/AI-driven big data engine. The Salt platform taps that rich context to discover all APIs, stop attackers during their early stages, and share remediation insights to improve API security posture.

Key capabilities of the Salt platform

Discover all APIs and exposed data

The Salt platform automatically inventories all APIs, including shadow and zombie APIs, across all application environments. Salt also highlights all instances where APIs expose sensitive data. Continuous discovery ensures APIs stay protected even as environments evolve and change as a result of agile methodologies and DevOps practices.

Stop API attackers

Pinpoint and stop threats to APIs with Salt's patented AI technology that baselines legitimate behavior and identifies attackers in real time, during reconnaissance, to prevent them from advancing. The Salt platform correlates all activities back to a single entity, sends a single consolidated alert to avoid alert fatigue, and blocks the attacker -- not just transactions.

Improve API security posture

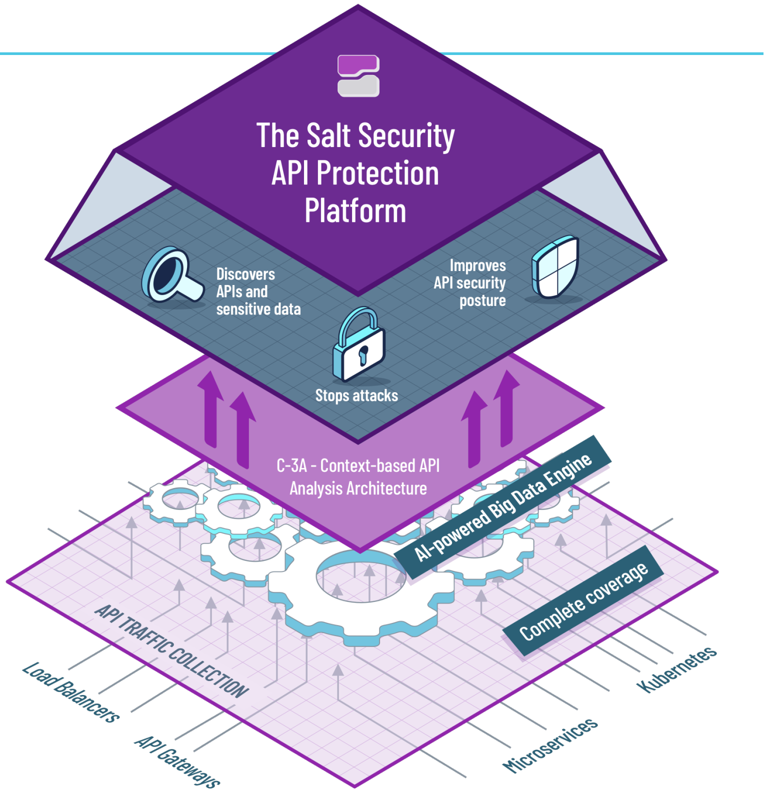
The Salt platform proactively identifies vulnerabilities by analyzing your APIs and API documentation to identify gaps even before your APIs serve production traffic. Salt also uses attackers like pen testers, capturing their minor successes to provide dev teams with insights for remediation. Insights from Salt enables continuous improvement of your API security posture while not slowing down the speed of development.

Salt Use Cases

- Discover Shadow APIs
- Prevent Sensitive Data Exposure
- Stop API Attacks
- Prevent Account Takeover
- Prevent Data Exfiltration
- Reduce Investigation Time
- Provide Remediation Insights
- Simplify Compliance

The Salt Architectural Advantage

- **Complete coverage** - Salt collects all API traffic – across load balancers, API gateways, WAFs, Kubernetes clusters, cloud VPCs, and app servers - to dynamically provide a full inventory. Salt is deployed with no app or network changes and requires no configuration or tuning.
- **AI-powered big data engine** - Every API is unique. ML and AI are applied in the Salt big data engine to baseline APIs and isolate anomalous behavior, differentiating between changes to APIs and malicious activity to pinpoint attackers and avoid false positives.
- **Context-based detection** - Salt combines complete coverage and a big data engine to discover all APIs, see the sensitive data they expose, find and stop attackers, and capture insights for development teams to improve API security.


The Salt Security API Protection Platform
Discovers APIs and sensitive data
Stops attacks
Improves API security posture
C-3A - Context-based API Analysis Architecture
AI-powered Big Data Engine
Complete coverage
API TRAFFIC COLLECTION
Load Balancers
API Gateways
Microservices
Kubernetes

Quick setup, not inline, no agents, no configuration

Unlike traditional, intrusive proxy deployments that add latency and can cause service disruption, Salt has a DevOps friendly setup. Salt does not deploy inline and supports a variety of quick and easy setup options including API gateway integrations, containers (Docker, Kubernetes, etc.), and support through traffic mirroring on-prem or from the cloud.

Supported platforms and technologies

API gateways and management

akana
Amazon API Gateway
apigee
axway
Azure API Management
IBM API Connect
Kong
MuleSoft
TIBCO
WSO2

Cloud environments

aws
Google Cloud
Azure

Server and microservices infrastructure

docker
vmware

Proxies and network devices

cisco
CLOUDFLARE Workers
envoy
f5
Gigamon
NGINX

SIEMs and incident response

PagerDuty
snowflake
splunk>
sumo logic

DevOps integration

Jira Software
servicenow
slack
Webhooks

API technologies

Any HTTP web traffic
REST (JSON)
SOAP (XML)

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