The Salt Security API Protection Platform

Discover all your APIs, identify and block attacks, and harden API security across the development lifecycle

Your Growing API Attack Surface

Hundreds of millions of application programming interfaces (APIs) power the digital economy, and that figure continues to expand at a relentless pace. While development teams deploy tools to help them conquer the complexity of managing their API inventory and increase their velocity, the resulting sprawl is creating far greater concerns. APIs now represent the broadest and riskiest attack surface in the enterprise.

Today we're seeing APIs become a preferred attack vector for cybercriminals and hackers. In fact, a Salt Security survey in 2022 shows that 95% of companies report they've suffered an API security incident within the previous 12 months. Clearly, traditional security approaches are unable to detect and stop API attacks.

How Can You Protect Your APIs?

Web application firewalls (WAFs), API gateways and management tools, identity and access management (IAM) tools, and other security technologies were never designed to provide the type of visibility, insight, and runtime protection needed to prevent successful attacks on APIs.

Those tools provide their own value, but to protect APIs, companies need a platform specifically created to address the unique challenges of API security:

- **Visibility:** API sprawl continues unabated, making it nearly impossible to stay up to date on new and changed APIs. Organizations also need insights into where their APIs expose sensitive data.
- **Attack prevention:** Every API is unique, so attacks are unique, and organizations need the ability to detect the low-and-slow behavior of bad actors probing APIs in search of business logic flaws.
- **Proactive security:** Remediation insights, gleaned from pre-production testing as well as runtime, help developers harden their APIs. Organizations must beware not to overly rely on shift-left tactics, however, since such pre-production testing won't uncover flaws in business logic, and developers cannot be expected to build secure APIs every time.

Cloud-Scale Big Data and Patented Artificial Intelligence Is the Answer

To protect your business from being a victim of a successful API attack, you need a platform built from the ground up to automatically discover new and changed APIs, detect and stop attacks on APIs in the early stages, and fix vulnerabilities in new and running APIs. The platform must take a full lifecycle approach to protect all of the APIs running in your environment — and do so without impacting performance or the user experience.

Achieving this level of protection is possible only with automation, powered by cloud-scale big data and highly trained artificial intelligence (AI). Humans — even deeply experienced security analysts — simply can't analyze hundreds of attributes across millions of API calls to create the rich context needed to detect threats such as a multi-day credential stuffing attack.

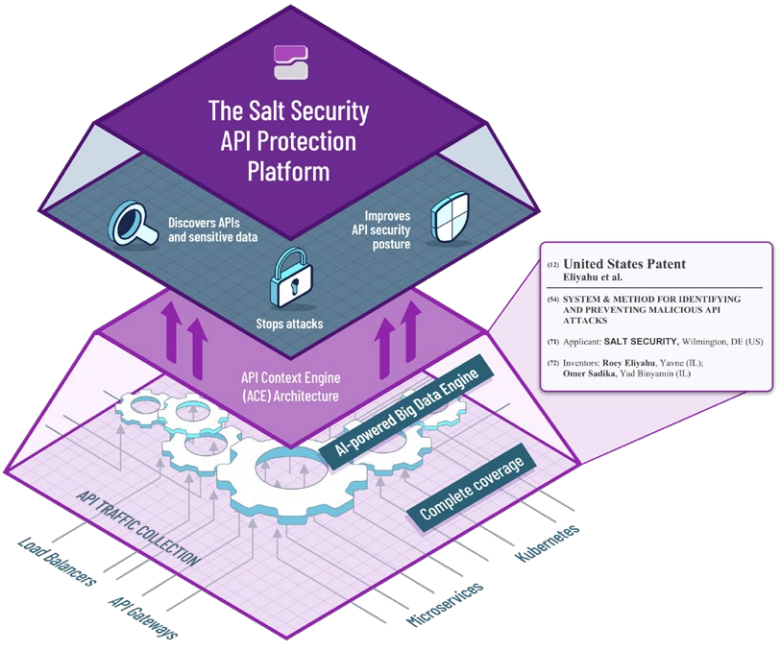
That's what makes the Salt Security API Protection Platform unique: its ability to collect, store, and analyze millions of attributes and correlate them over time to identify attackers during reconnaissance. Using the most mature AI and machine learning (ML) algorithms, extensively trained through years of exposure to thousands of environments, the Salt Security platform provides all the context needed to protect all of your APIs — even the ones you didn't know you had.

Salt – The Only Patented, AI-Powered Approach to Protecting APIs

Delivering complete API security across the full lifecycle, the Salt Security API Protection Platform creates the context and visibility to show you all your APIs, stops attackers during the early stages of an attempted attack, and shares insights to improve API security posture.

The Salt Security API Protection Platform is based on our API Context Engine (ACE) Architecture:

- **Cloud-scale big data engine:** The Salt platform captures all of your API traffic and baselines your full environment to build the rich, deep context needed to span long attack timeframes.
- **Patented, time-tested, and customer-proven AI and ML algorithms:** The Salt platform correlates behavior to build a rich attacker fingerprint and timeline in one alert, reducing alerts by 96% to prevent alert fatigue. Only Salt has had its AI and ML algorithms in market for more than four years, enriched by learning across 1000s of customer and application environments.
- **Frictionless deployment:** By avoiding agents or code changes, the Salt Security platform deploys out of band, never introducing latency or affecting user experience.
- **Application environment flexibility:** the Salt platform supports more than 60 options for integrating into environments, across API gateways, cloud services, load balancers, and cloud-native environments such as Kubernetes. Whether an organization's applications are running on-premises, in the cloud, or in hybrid mode, Salt supports them all. Salt also supports any API format, including REST, GraphQL, SOAP, and others.



The Salt Security Advantage

API discovery: Collect all your REST, GraphQL, and other API traffic, and dynamically build a full inventory, including new and changed APIs, while discovering and alerting on exposure of sensitive data.

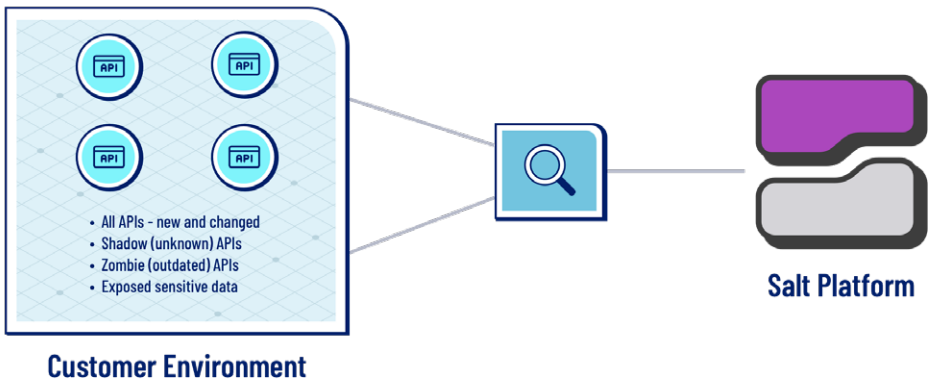
Attack prevention: Baseline your APIs and isolate anomalous behavior, differentiating between changes to APIs and malicious activity and block attackers before they reach their objective.

API hardening: Scan and test APIs during build and capture insights during runtime, with specific remediation details that developers can use to improve API security posture.

Continuously Discover All Your APIs

API inventory is one of the biggest blind spots for cybersecurity teams today. Unless your company already has an advanced API security platform, you almost certainly have unknown or shadow APIs, zombie APIs (those thought to be deprecated but still in use), incorrectly documented or undocumented APIs, and APIs with unknown vulnerabilities such as exposing sensitive data.

You can't protect what you can't see. The Salt Security platform automatically and continuously discovers all your internal, external, and third-party APIs, including unknown (shadow) and outdated (zombie) APIs.



Key capabilities:

- Always up-to-date API inventory with granular details of each API, including exposed sensitive data, to help you assess risk
- Continuous API discovery so you know when new APIs are released, existing APIs are updated, or new vulnerabilities are introduced
- Security insight, analysis, and context to help you manage risk and eliminate vulnerabilities

Detect and Block Attacks on Your APIs

Attackers are focused on finding and exploiting vulnerabilities in the business logic of your APIs. Because APIs are unique, attackers take days, weeks, or months to probe and understand how your APIs work and where they may have vulnerabilities.

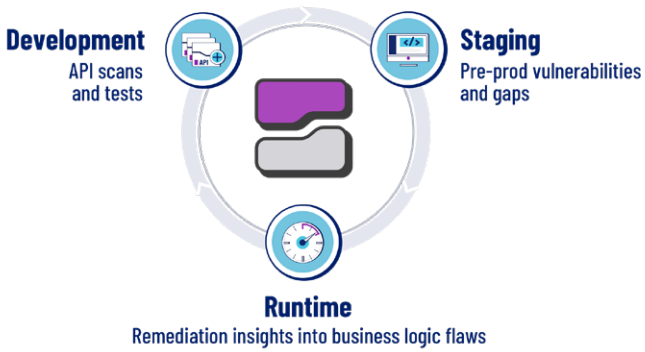
The Salt Security platform detects these low-and-slow attacks, uncovering the reconnaissance actions of bad actors early in their probing. With Salt, you can choose to manually or automatically block attackers using the inline devices you already have deployed.

Key capabilities:

- Granular baseline for each API, storing hundreds of attributes about thousands of APIs and their endpoints, across thousands of users over time
- ML/AI-driven big data engine pinpoints anomalies and minimizes false positives
- A single alert provides you with a complete attacker timeline, even as attackers obfuscate their activity across many IDs, IPs, and devices
- Manual or automatic blocking, leveraging your existing inline security controls

Accelerate Remediation and Shift Left

It's not enough to find and block attackers exploiting a vulnerability in your API. You will also want to remediate the security gap in your APIs. The Salt Security platform lets you simulate runtime behavior and attacks as part of your CI/CD pipeline process, so you can bake security into your development cycle. The Salt platform also identifies vulnerabilities found only at runtime and provides clear remediation details dev teams can apply to harden existing APIs.



Key capabilities:

- API design analysis scans and tests APIs while they're still in design to identify potential vulnerabilities
- API drift analysis compares API definitions in OAS/Swagger files against live test traffic to identify gaps between documentation and APIs in action
- Remediation insights learned during runtime help development teams improve the security posture of running APIs
- Development teams receive insights automatically using existing workflows and tools such as Jira or Slack

The Benefits for Your Business

Never worry about your APIs again. With the Salt Security API Protection Platform, your company can

- *Eliminate security blind spots and identify all APIs*
- *Identify and stop an attack early, with a 20x faster time to resolution*
- *Eliminate API vulnerabilities and harden security 3x faster with a full lifecycle approach*
- *Protect sensitive data from exfiltration*
- *Increase development velocity, enabling teams to release secure code to end users faster*
- *Simplify compliance*

About Salt Security

Salt Security protects the APIs that form the core of every modern application. Its API Protection Platform is the industry's first patented solution to prevent the next generation of API attacks, using machine learning and AI to automatically and continuously identify and protect APIs. Deployed in minutes, the Salt Security platform learns the granular behavior of a company's APIs and requires no configuration or customization to pinpoint and block API attackers. For more information, please visit https://salt.security.