



 SALT

# From Crawling to Running: Your API Security Journey in the Age of AI



Only 7.5% of organizations consider their API security programs to be 'advanced'.

APIs are crucial for innovation and business flexibility in today's digital world. However, they also expose organizations to security risks. 95% of organizations have experienced API-related security incidents in the past year, with almost a quarter suffering breaches due to API vulnerabilities. Traditional security measures struggle to keep pace, especially with threats magnified by AI. Gartner's recent warning emphasizes the urgency: "The average API breach results in at least 10 times more leaked data than the average security breach."



A robust and modern API security platform is essential to protect your data and applications in this evolving threat landscape. It should offer panoramic API discovery, proactive posture assurance, AI-driven threat detection, continuous monitoring, and early integration of security and governance in the development process.



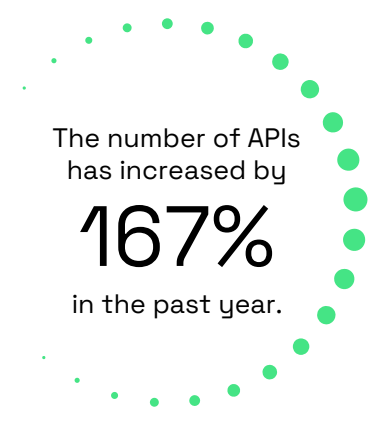
This guide will help you understand the journey of API security and what to look for in a modern API Security platform, including:

- Crafting Your API Security Strategy: It's a Journey
- Selecting an API Security Vendor
- Adaptive API Protection Platform to Safeguard Your Digital Ecosystem
- Modern API Security Platform Checklist



# Crafting Your API Security Strategy: It's a Journey

The journey to API security is an ongoing process that requires a phased approach to adapt to the changing threat landscape. Organizations should begin by gaining a thorough understanding of their API landscape. Then, they need to put in place and enforce security measures and, finally, implement advanced threat protection and risk mitigation strategies. This step-by-step approach, akin to crawling, walking, and then running, ensures that organizations can effectively handle API security risks while innovating and staying agile.

A circular infographic with a dashed green border. Inside, the text reads: 'The number of APIs has increased by 167% in the past year.' The percentage '167%' is prominently displayed in a large, bold font.

The number of APIs  
has increased by

167%

in the past year.

## 01

### Crawl: API Discovery

It is crucial to have a comprehensive API inventory as the cornerstone of an effective security strategy. Complete visibility into all APIs, including any undocumented APIs, is essential. Look for a solution that goes beyond basic discovery and provides in-depth insights into your API landscape. This includes identifying the existence of APIs, understanding their behavior, classifying them based on risk, and detailing their endpoints, versions, and parameters. A robust API inventory enables you to prioritize security efforts and proactively mitigate potential threats.

**Why it matters:** The constant creation and deployment of new APIs into your ecosystem, compounded by the increasing speed and quantity of GenAI-created APIs, increases the organizational risk of creating blind spots without continuous AI-based discovery.

## 02

### Walk: API Posture Assurance

Governance involves creating and upholding the rules for your APIs and ensuring that they comply with your organization's security and compliance standards. A strong API security solution should assist in defining policies for data classification, access controls, authentication requirements, and other aspects. It should automate the enforcement of these policies across your API landscape, consistently monitor compliance, and offer comprehensive reporting on your overall security stance.

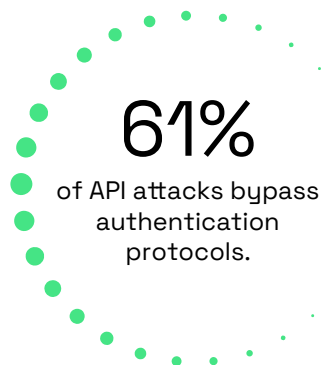
**Why it matters:** With modern applications being built on APIs, organizations require effective API posture assurance to reduce security risk, avoid compliance violations, and prevent potential data breaches, unauthorized access, and reputational damage.



# 03

## Run: API Behavioral Threat Protection

In the face of increasingly sophisticated threats and a growing number of AI-generated APIs, traditional API security measures are no longer sufficient. These attacks often bypass perimeter defenses and signature-based protections, leaving APIs vulnerable to exploitation. The Open Web Application Security Project (OWASP) API Security Top 10 is a compilation of the most significant security risks to APIs. These risks encompass vulnerabilities such as Broken Object Level Authorization (BOLA), Broken Authentication, and Excessive Data Exposure. Traditional API security measures often struggle to defend against these sophisticated attacks, including 'low and slow' attacks that evade detection by staying under the radar.



AI-powered behavioral threat protection has become essential to safeguard APIs in this evolving landscape. This advanced approach continuously monitors API traffic, analyzes usage patterns, and builds a dynamic baseline of normal behavior. This enables it to identify anomalies and subtle deviations that may indicate an ongoing attack. BOLA is a common issue where APIs fail to validate whether a user

should have access to a specific object or data. This can result in unauthorized access, modification, or deletion of data. Broken Authentication vulnerabilities occur when API authentication mechanisms are weak or flawed, allowing attackers to impersonate users or gain unauthorized access. Excessive Data Exposure occurs when APIs return more data than necessary, potentially exposing sensitive information. These vulnerabilities can be exploited by attackers to steal data, disrupt services, or gain unauthorized access to systems. By leveraging the power of artificial intelligence, API behavioral protection can adapt to the increasing complexity of threats and the proliferation of AI-generated APIs, providing a deeper level of security that goes beyond basic vulnerability scanning.

**Why it matters:** In the face of an evolving threat landscape driven by AI-generated APIs and sophisticated attacks that bypass traditional defenses, AI-powered behavioral threat protection is essential for safeguarding APIs and mitigating the risk of exploitation, data breaches, and service disruptions.





## 04

### Monitoring and Logging

Consider this as the surveillance system for your APIs. Detailed logging offers a comprehensive audit trail of all API activity, including requests, responses, errors, and security events. Real-time monitoring helps you identify anomalies and potential threats as they occur. An effective API security solution should provide customizable alerts that notify you of suspicious activity or security incidents promptly.

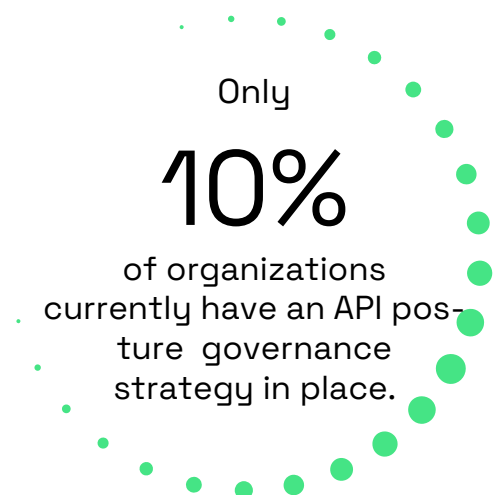
**Why it matters:** Robust API logging and monitoring are crucial for maintaining API security, providing a detailed audit trail, and prompt security and violation alerts, enabling swift incident response, and minimizing the risk of unauthorized access.

## 05

### Extend Posture Governance Left

Security should be integrated into the API development process from the beginning, not added as an afterthought. Seek a solution that seamlessly integrates with your development lifecycle and CI/CD pipeline. This will help you identify and fix vulnerabilities as well as compliance or regulatory issues early on before they impact production and expose your APIs to risk. Automated security testing of APIs should be considered as part of your development workflow.

**Why it matters:** Integrating posture governance into the API development process from the start, with CI/CD integration and automated testing, proactively identifies and remediates vulnerabilities, ensuring a robust and secure API ecosystem and minimizes risk before APIs are put into production.



# Selecting an API Security Vendor

Beyond the items above that are key criteria to consider for your API Security, here are a few additional criteria to look for in a vendor:



## **Scalability**

Can the solution handle your current and future API traffic with your expected growth rates?



## **Integration**

Will it seamlessly integrate with your existing security infrastructure?



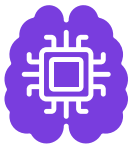
## **Ease of Use**

Is the solution intuitive and easy for your security team to manage?



## **Support and Services**

Does the vendor offer comprehensive support and services that align with your needs?



## **AI and Machine Learning Capabilities**

How does the vendor leverage AI and ML to enhance API security? Beware of "AI washing" – ensure the solution truly harnesses the power of AI for advanced threat detection and prevention.



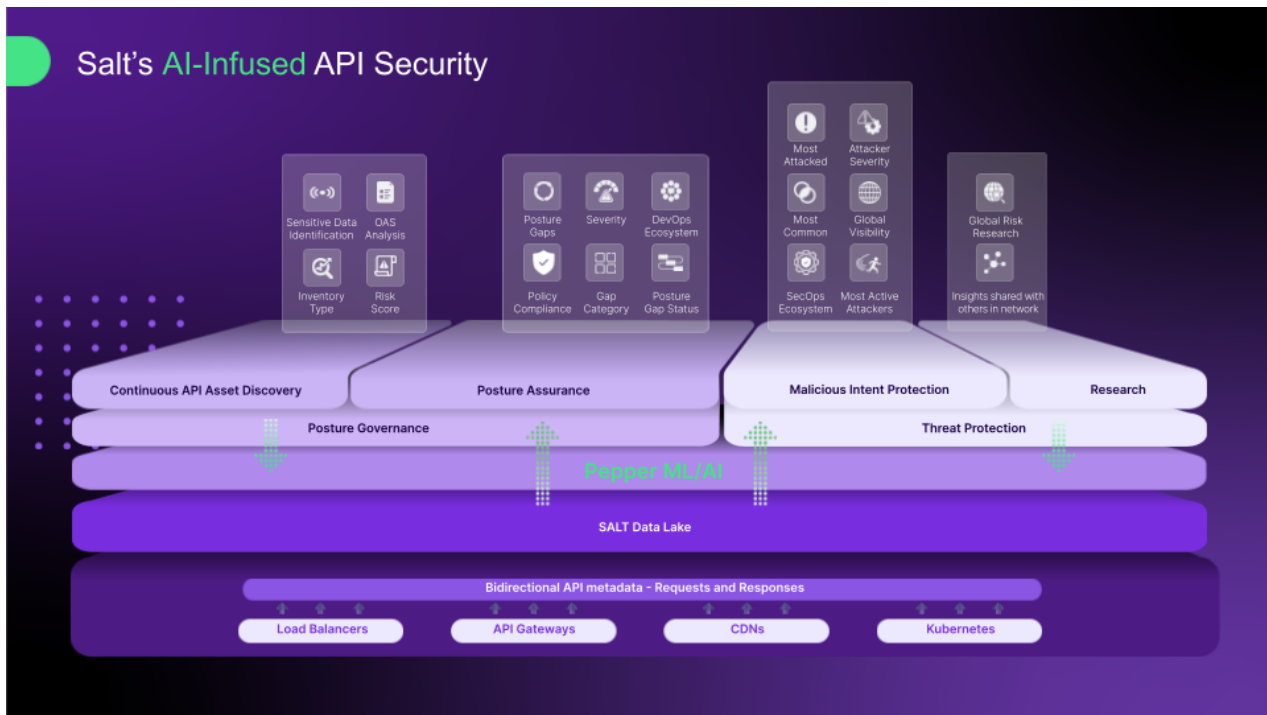
## **Response to AI-Generated Attacks**

How does the solution specifically address the risk of AI-generated attacks, including detection, prevention, and mitigation strategies?



# Adaptive API Protection Platform to Safeguard Your Digital Ecosystem

To effectively safeguard organizations from advanced threats, an API Protection Platform infused with AI must be utilized to combat these challenges directly.



## The Solution Should Offer:



### Unparalleled API Discovery

An AI/ML engine to automatically analyze trillions of API calls to discover all your APIs, including all undocumented APIs. It then builds a comprehensive inventory, which is continually updated, with contextual risk categorization, enabling you to prioritize security efforts effectively.



### Proactive API Posture Governance

It's not enough to just identify your APIs. You need to continuously monitor and enforce their security measures to protect your API landscape. Pre-built policy templates can help you align with your organization's governance standards and compliance requirements. Additionally, you should be able to create and customize governance rules to address the specific needs of your regulatory environment. This will help your APIs stay secure and compliant as your business and the threat landscape change.





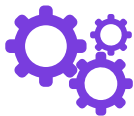
### **AI-Driven Threat Detection and Prevention**

In the noisy world of API traffic, detecting malicious activity using traditional security measures can be challenging. In this high-threat environment, AI and ML models are essential. These models need to be trained on trillions of API calls to identify hidden malicious signals effectively. Anomaly detection alone is insufficient; the platform must thoroughly analyze the content and behavior of each API call to uncover subtle patterns and deviations that indicate malicious intent. Utilizing AI-based attacker insights, this analysis can provide actionable intelligence, allowing security teams to swiftly and decisively neutralize threats and safeguard valuable assets and reputation.



### **Comprehensive Remediation Guidance**

The platform must provide actionable insights to remediate vulnerabilities and harden your APIs against future attacks.



### **Seamless Integration:**

A modern API Protection Platform must deploy easily in any environment, with prebuilt collectors offering friction-free deployments. It should integrate seamlessly with your existing security infrastructure, including SIEMs, SOARs, DAST, and other tools.

Salt Security is more than just a vendor; we are your partner in API security. Our team of experts is dedicated to working with you to understand your unique challenges and tailor a solution to meet your specific needs. We act as a trusted advisor on your journey toward API security, providing comprehensive support, professional services, and training.

With Salt Security, you get a platform and peace of mind, knowing that your APIs are protected by the most advanced, adaptive, and comprehensive API security solution available.

The API threat landscape continually changes, and traditional security measures are no longer sufficient. By teaming up with Salt Security, you can develop an API security strategy to protect your organization's digital future.

### **Ready to take the next step?**

Contact Salt Security today to schedule a demo and learn how our API Protection Platform can help you confidently navigate the evolving API threat landscape.



## 01

### API Discovery Requirements

- ☐ Continuously discover new and changed APIs, including shadow APIs.
- ☐ Create a comprehensive API inventory that includes endpoints and risk analysis.
- ☐ Classify APIs based on their functionality.
- ☐ Track how APIs are interacting with organizations' sensitive data.
- ☐ Identify subtle and sophisticated behavioral anomalies across different time intervals, from seconds to days.
- ☐ Administrative users can add and configure custom sensitive data classifications and categories, which will automatically apply to API learning.

## 02

### API Posture Assurance Requirements

- ☐ Enforce API security policies consistently across all your APIs.
- ☐ Automate compliance monitoring to track the overall security status of your APIs.
- ☐ Offer pre-built policy templates to simplify API governance.
- ☐ Provide tools for easy configuration and management of security rules.
- ☐ Ability to create complex, compound rules that comply with existing governance frameworks, including PCI, PSD2, NIST, and others.
- ☐ Automatic alerting when posture governance rules are violated.
- ☐ Automated remediation workflows for Posture Governance alerts integrate with Jira, ServiceNow, Splunk, and other systems.

## 03

### API Behavioral Threat Protection Requirements

- ☐ Real-time anomaly detection involves AI-powered continuous monitoring of API traffic and a dynamic understanding of normal behavior.
- ☐ Contextual analysis of API requests and responses using AI to distinguish between legitimate and malicious activity accurately.



<input type="checkbox"/>	Adaptive learning capabilities continuously refine behavioral models to stay ahead of evolving threats.
<input type="checkbox"/>	Automated response and mitigation capabilities to quickly block malicious activity and minimize the impact of attacks.
<input type="checkbox"/>	The solution detects single and double ID BOLA.
<input type="checkbox"/>	The solution identifies broken user authentication through actions such as login, password change, reset, and 2FA, detecting brute force and credential stuffing attacks.
<input type="checkbox"/>	Provide detections for single ID BOLA, PII consumption detection, and excessive usage detection over a 1-hour period.

## 04 API Monitoring and Logging Requirements

<input type="checkbox"/>	For comprehensive audit trails and forensic analysis, capture granular logs of all API activity, including request and response details.
<input type="checkbox"/>	Correlate attacker threat activities in a single view to reduce resolution time and cut through noisy anomalous traffic
<input type="checkbox"/>	Integrate with existing SIEM and SOAR platforms for centralized log management and automated incident response.

## 05 Extend API Posture Governance Left Requirements

<input type="checkbox"/>	Provide developers with clear guidance on 'good' API design, considering regulatory and compliance concerns specific to our organization.
<input type="checkbox"/>	Move posture governance earlier in the development process to identify security issues in API designs before coding.
<input type="checkbox"/>	Bridge the gap to facilitate communication between development and security teams to promote security awareness throughout the project lifecycle.
<input type="checkbox"/>	Assume AI is being used to develop APIs and enforce guardrails to reduce risk.

\*Gartner, Market Guide for API Protection, Dionisio Zumerle, Aaron Lord, Esraa ElTahawy, Mark O'Neill, 29 May 2024

GARTNER is a registered trademark and service mark, of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved."

