



The Definitive Guide to API Security Posture Management

Table of contents

Why API security has become imperative	3
Why posture management?	6
Posture management features you can't live without	8
Akamai's approach to posture management	11
How posture management for APIs can help you	13

Why API security has become imperative

APIs allow an organization's developers to build with efficiency, in a profession where speed is nonnegotiable. However, while APIs are developer-friendly — and key for the interoperability of software and data assets — API security has not kept pace with the speed of innovation.

Eighty-four percent of organizations have experienced an API security incident in the past 12 months, up from 78% in 2023.¹ In part, this is because APIs also provide efficiency for attackers.

Many APIs are built with misconfigurations, coding errors, and a lack of authentication controls. As a result, an API attack can be quite simple to conduct and a direct way to steal data.

And when it comes to data, only 27% of enterprises with full API inventories know which APIs return sensitive data, from customer data to intellectual property — down from 40% in 2023.² With attacks up and visibility down, enterprises need a way to assess and improve their API security posture.

1, 2. Akamai, 2024 API Security Impact Study

What comprehensive API security looks like

As your company's use of APIs expands, your attack surface expands with it, creating new security challenges.

When it comes to securing APIs, the tools that organizations traditionally use, such as API gateways and web application firewalls, can provide some protection. But as your API estate becomes more complex — for example, encompassing a sprawl of unmanaged APIs that are difficult to see and secure — something needs to change.

APIs merit a substantial presence in the enterprise security game plan. And a dedicated API security solution — one that's designed to take on today's API risks and attack methods — can provide the visibility and capabilities for executing on that plan. It's not unlike the concept of defense in depth, where tools complement one another to cover every step of the attack path.



A comprehensive API security platform — built to provide API discovery, posture management, runtime protection, and security testing — can help you see hidden API risks, identify API attack paths, and mitigate the threats you've uncovered in real time.

In our related ebook, *The Definitive Guide to API Discovery*, we explain the first critical element of API security — locating your APIs. Once you have discovered and inventoried all the APIs in use across your organization, the next step is enhancing your overall API security posture.

Posture management may be especially important for companies that purchase a third-party providers' applications and use, brand, and sell them as their own. For example, nearly every new car in the past five years shares nearly identical telematics functionality.

If an attacker finds vulnerabilities in a manufacturer's API endpoints, they gain an easy ingress point for remote account takeover attacks and data breaches.

What this guide covers

API posture management gives you the tools to manage, monitor, and maintain the security of your APIs throughout the API lifecycle. This definitive guide focuses on the key requirements for API security posture management — including vulnerability detection and sensitive data protection. It explores methods of posture management and introduces the posture management capabilities of the Akamai API Security solution.

Why posture management?

API posture management ensures that you put your best foot forward when it comes to API security. It helps you understand the risk of discovered APIs by finding what kinds of data are flowing through, if there are any vulnerabilities or misconfigurations present, if APIs are properly authenticated, and more. The ability to identify API vulnerabilities and remediate them quickly allows you to take corrective action before an attack occurs.

Comprehensive posture management provides visibility into all activity around APIs so you can enforce security policies, ensure compliance with regulations, and audit changes to your API ecosystem. It protects and secures your APIs

Only 27% of enterprises with full API inventories know which of their APIs return sensitive data, down from 40% in 2023.³

3. Akamai, 2024 API Security Impact Study

against malicious attacks, unauthorized users, and data breaches – any one of which can lead to significant reputational damage, loss of business, and regulatory penalties.

Implementing posture management best practices minimizes the API attack surface and mitigates much of your API risk. Building thorough inventories of your organization's APIs and sensitive data stores is essential for good posture management. On the next page, we'll discuss additional elements of API posture management: vulnerability detection, API monitoring, and problem remediation.

- **Vulnerability detection**

Analysis: Inspect source code for common weaknesses, understand how an API interacts with external systems, and evaluate its authorization and authentication features.

Observation: Inspect traffic to and from an API to identify misconfigurations, detect vulnerabilities, and develop an understanding of baseline API behavior.

Posture management is just one piece of a complete API security program. It's also critical to use comprehensive preproduction testing to stop vulnerabilities from ever reaching production.

- **API monitoring**

Identify and monitor API calls in production, trace API requests, detect deviations from baseline usage, and create alerts when API usage exceeds predefined thresholds.

- **Remediation**

Fix identified weaknesses or vulnerabilities to make an API more secure and compliant through code changes, fine-tuning security settings, or patching API flaws. Good posture management enables remediation to occur before a vulnerability can be exploited.

Posture management features you can't live without

You may already know — or strongly suspect — that your API security posture isn't as strong as it could be. Here are some key features that your posture management tools must include.

- **Sensitive data classification**

An API that supplies weather data from public sources is of much less concern than one that transmits credit card information. API posture management tools should be able to quickly identify how many APIs are able to access credit card data, phone numbers, Social Security numbers (SSNs), and other sensitive data, along with the number of users who have accessed sensitive data via your APIs.

- **Configuration assessment**

Many cyberattacks gain entry as the result of simple misconfiguration of the networks, API gateways, or firewalls that broker and protect API traffic. Strong posture management requires the ability to scan infrastructure and software configurations regularly, including log files and configuration files. Regular scanning helps uncover misconfigurations and vulnerabilities and identifies risks created by configuration drift.

- **Attacker confidence score**

Look for an attacker confidence scoring engine that uses advanced machine learning algorithms trained to evaluate external and internal signals, including API behavior, network traffic patterns,

geolocation data, threat intelligence feeds, and other contextual factors. This can help you determine the confidence level that a detected runtime incident is the result of malicious activity. This unique capability allows customers to quickly hone in on critical threats and create automatic remediation and notification flows for high-probability attacks.

- **Custom workflows**

Along with customizable severity, you need to be able to create workflows to take action immediately when vulnerabilities are identified. Custom workflows could range from creating trouble tickets to notifying key stakeholders to updating network configurations.

- **Autogenerated documentation**

API documentation tells the consumers of an API what it does and how to use it. Secure APIs must be evaluated for compliance against specifications and accurately documented. Poor or nonexistent documentation makes security testing more difficult, increasing the risk that an API reaches production with an undetected vulnerability.

This problem is often exacerbated by outsourcing API development. Regardless of the source of the problem, out-of-date, incomplete, and missing documentation are unacceptable if you want your API security program to be successful.

The **OpenAPI specification** (formerly referred to as Swagger) defines standard interface descriptions. Posture management tools should have the ability to automatically generate complete OpenAPI documentation based on the API's current and future state to help ensure that all APIs are properly documented and that documentation is up to date.

Insurance leader enhances API security posture with Akamai

As consumers move away from bricks and mortar in favor of digital, financial services companies must innovate at an accelerated pace. Like many of its peers, Aflac, the leading provider of supplemental health insurance in the United States, faced growing API security challenges.

Aflac turned to the Noname API Security Platform (now part of Akamai API Security) to meet its needs. The posture management module helps the team identify the types of data that traverse the company's APIs, providing visibility into which APIs access sensitive data and identifying any anomalies in data access.

Read the [full Aflac case study](#) to learn more.



We were aware that our API footprint was large, and we wanted to be completely confident that we had every API accounted for, that we had full visibility into their operation, and that they were being continuously tested for security risks.

— DJ Goldsworthy, VP, Security Operations and Threat Management, Aflac

Akamai's approach to posture management

The Akamai API Security solution's posture management module provides a comprehensive view of traffic, code, and configurations to assess your organization's API security posture. Akamai determines what your true attack surface looks like across APIs and web applications and uncovers all forms of sensitive data moving through your APIs, helping you to secure sensitive data.

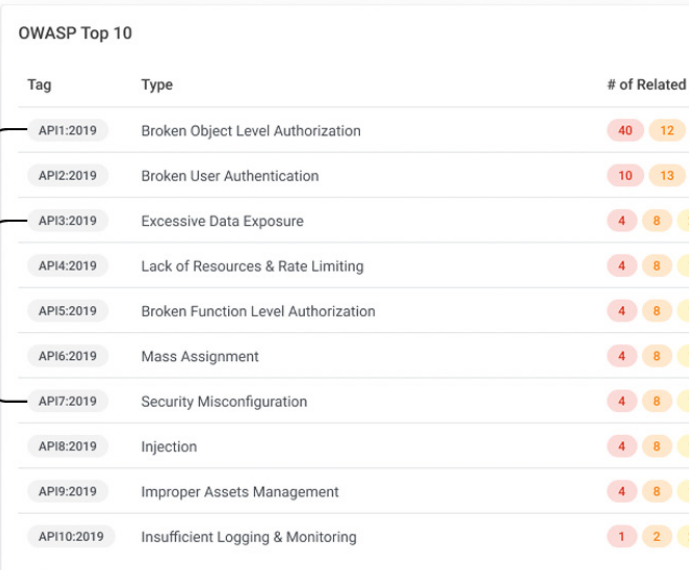
Simple API misconfigurations can leave you defenseless against cybercriminals. Once inside, hackers can quickly access and

exfiltrate your sensitive data. The Akamai API Security solution's posture management module provides these key features:

- Out-of-band integration for continuous API discovery on-prem, and in hybrid and public clouds
- A simple, searchable API inventory that includes details of schema, network placement, and datatypes
- Automated API documentation generation (OAS/Swagger)
- Context-aware analysis of API misconfigurations and vulnerabilities with prioritization
- Detection of all vulnerabilities in the OWASP API Security Top 10
- Automated discovery and classification of sensitive data and API changes

API Exposure

API security risk and issues are not all discoverable in source code alone. Observing traffic behavior within the context of the network provides the full content to derive risk findings.



Tag	Type	# of Related I
API1:2019	Broken Object Level Authorization	40 12
API2:2019	Broken User Authentication	10 13
API3:2019	Excessive Data Exposure	4 8 2
API4:2019	Lack of Resources & Rate Limiting	4 8 1
API5:2019	Broken Function Level Authorization	4 8 1
API6:2019	Mass Assignment	4 8 1
API7:2019	Security Misconfiguration	4 8 1
API8:2019	Injection	4 8 1
API9:2019	Improper Assets Management	4 8 1
API10:2019	Insufficient Logging & Monitoring	1 2 2

API exposure

In addition to uncovering risks within an API's code, it's also important to observe API traffic with an eye toward behavior — typical versus atypical — and within the context of the network.

The Akamai API Security solution's posture management looks at the widest possible set of sources to detect vulnerabilities, including log files, replays of historical traffic, configuration files, and much more. The solution detects all vulnerabilities in the OWASP API Security Top 10, and protects APIs from data leakage, authorization issues, abuse, misuse, and data corruption.

Akamai intelligently identifies and prioritizes potential vulnerabilities. Vulnerabilities can be remediated manually, semiautomatically,

or fully automatically through integrations into WAFs, API gateways, SIEM and ITSM tools, workflow tools, and other services.

API data protection

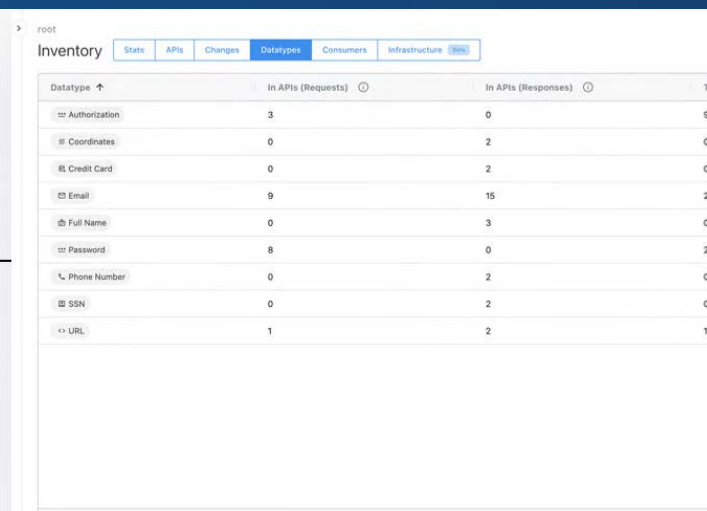
Protection of sensitive data types requires accurate inventory of data traversing endpoints for policies and controls to be applied accordingly — DLP policies for APIs are straightforward and actionable.

Compliance is taking on a whole new dimension with the growth of API usage. A wave of regulations has emerged in response to the growing attack surface. Regulated industries must now factor APIs into their plans for compliance.

The Akamai API Security solution's posture management module identifies all forms of sensitive data moving through your APIs, including all personally identifiable information (PII) such as credit cards, SSNs, addresses, insurance information, and more. By reducing access to these data types and implementing a data management framework, we help you ensure sensitive data is where it needs to be and secure from malicious threats.

API Data Protection

Protection of sensitive data types requires accurate inventory of data traversing endpoints in order for policies and controls to be applied accordingly — DLP policies for APIs are straightforward and actionable.



Datatype	In APIs (Requests)	In APIs (Responses)	Total
Authorization	3	0	3
Coordinates	0	2	2
Credit Card	0	2	2
Email	9	15	24
Full Name	0	3	3
Password	8	0	8
Phone Number	0	2	2
SSN	0	2	2
URL	1	2	3

How posture management for APIs can help you

Every time a customer, partner, or vendor engages with your organization digitally, there's an API behind the scenes facilitating a rapid exchange of (often sensitive) data. Gaining visibility into every API across your organization and assessing their risk attributes – for example, which APIs return sensitive data – can help you protect your organization against a fast-rising attack vector. API security posture management can also help you ensure compliance with global regulations that aim to prevent data breaches.



Learn about **data protection regulations** that require seeing and securing all APIs.

Learn how we can help you by scheduling a **customized Akamai API Security demo.**

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on **X**, formerly known as Twitter, and **LinkedIn**. Published 12/24.

