wallarm

PRODUCT DATASHEET

API Abuse Prevention

Proactive Runtime Protection Against API Abuse

Preventing API abuse requires a multi-layered approach, including proactive monitoring, access control, rate limiting, and threat detection. It differs from traditional approaches in that it requires a deeper understanding of API usage patterns and user behavior, as well as the ability to quickly respond to emerging threats through automated mitigation and real-time analytics. The Wallarm API Abuse Prevention solution helps organizations secure their APIs and prevent abuse.

API Abuse Prevention at a Glance

Wallarm API Abuse Prevention provides comprehensive real-time protection against malicious automated behavior. Key Benefits include:

Purpose-Built for APIs

APIs are designed to be open, so protecting them from abuse is a subtle balance involving access vs. protection. We allow you to assemble detectors and thresholds to customize protections appropriate for your API estate.

Detection & Protection

Guard against a blindspot in your API defenses by recognizing and differentiating between legitimate vs. malicious automated behaviors, and blocking those likely to cause harm based on your unique scenarios.

Session Visibility

Wallarm provides full transparency into the sessions in which API abuse occurred. Users are able to view the full API interaction, both before and after a specific attack occurred.

Eliminate the gap in your API protections with an integrated and customizable approach from Wallarm to prevent abuse of your APIs and to minimize the impact on your operations and legitimate users.

Why Do You Need API Abuse Prevention?

Your public-facing APIs are designed to be accessible. This opens them up to abuse, such as malicious bots being used to scrape data, overload systems, and commit fraud.

Traditional security tools, including Rate Limiting and DDoS Protection, can be useful at reducing volumetric attacks, but generally cannot distinguish between legitimate and malicious traffic. And while traditional bot management works reasonably well at finding bad actors *among human users*, since APIs are automated it's really about finding bad bots *among other bots*. To solve this problem, our approach is about intent and context — basically allowing you to assess the aims of each request, at scale.

Types of API Abuse

Wallarm API Abuse Prevention detects and protects against a variety of modern API threats, such as those covered in OWASP API1:2019 (BOLA) and API9:2019 (Improper Assets Management). Examples include:

Account Takeover (ATO)

Malicious actor gains unauthorized access to an account, for example via credential stuffing, which can lead to severe consequences such as identity theft, financial losses, and reputational damage.

Scanning and Scraping

Automated scripts probe or scrape data from your API, often with malicious intent, which can lead to downtime, data breaches, and unauthorized data access, resulting in theft of IP or sensitive end user data.

L7 API DoS Attacks

Layer-7 denial-of-service (DoS) attacks target your API at the application layer, overwhelming it with a high volume of API requests, which could lead to the app being unavailable to your users and the lost of their trust & business.

Guard Against API Abuse

The Wallarm API Abuse Prevention solution is delivered as part of the Wallarm End-to-End API Security solution, providing you with a single platform to protect your entire API estate. It gives you the visibility, configurability and management capabilities to prevent sophisticated API-specific malicious automated behavior from overwhelming your defenses and operations:

Visibility

Group and display indicators of automated behavior based on factors such as request patterns, timing anomalies, and API endpoint behaviors, to watch for potentially harmful actions.

Configurability

Structure your API Abuse protections by leveraging any combination of multiple detector types and defining weighting and thresholds, to suit your specific needs.

Management

Monitor malicious behaviors, get in-depth contextual information on them, and adjust settings to optimize access for legitimate use and reduce operational workloads and costs.

Wallarm API Abuse Prevention uses specialized detectors to identify and stop a wide variety of malicious bot activities, including API abuse, credential stuffing, security crawlers, and content scrapers. One of the key advantages of this approach is that it is not based on JavaScript challenges, which have proven to be ineffective against API bots. Instead, it uses a combination of machine learning and rules-based algorithms to accurately detect and stop malicious bot activity.

> **It's Sexy!** And it meets all of our API abuse prevention needs, providing us with the visibility, automated & configurable controls, and in-depth contextual insight to protect our legitimate users while blocking abusers.
>
> -Robert A, IT Director
> Large Hosting Company