wallarm

PRODUCT DATASHEET

Wallarm API Discovery

Know What You Have, Protect What You Have

The Wallarm API Discovery module, part of Wallarm API Security platform, provides visibility into your entire API portfolio, allowing you to regain control over your API attack surface and reduce associated risk.

Why Do You Need API Discovery?

APIs are a crucial component of today's digital world. In early 2021, *451 Research* estimated that the average organization has 15,000 to 20,000 APs in use, with a 200% growth rate.

But with the booming use of APIs comes increased risks from:

- **Proliferation.** Organizations struggle to manage the explosive growth in API use, both externally and internally – which means a sizable and expanding attack surface.
- **Development Speed.** Reliance on open source, 3rd party, and diverse internal development teams results in a veritable alphabet soup of protocols, languages, and frameworks – which adds complexity and cost to your security stack.
- **Unmanaged APIs.** *Gartner* estimates that by 2025, less than 50% of enterprise APIs will be properly managed – which conceals a massive chunk of your API estate from security controls.
- **Sensitive Data Exposure.** More organizations are pushing more sensitive data through their APIs, including PII, financial & health data, credentials and more – which increases the danger and impact of unintentional or malicious disclosure.

API Discovery at a Glance

Wallarm API Discovery provides runtime visibility for your API portfolio. Key Benefits include:

- **Visibility.** Track and manage all your API assets to understand your real attack surface and guard against surprises from deprecated or unmanaged endpoints.
- **Monitoring.** Build complete API inventory based on actual usage to identify out-of-spec code, track changes, and keep tabs on sensitive data flows.
- **Protection.** Assess and remediate any weaknesses which open you up to attack and automatically implement rules to protect against attacks.

Software engineering leaders responsible for API technologies should manage and govern all APIs by investing in discovery, cataloging and automatic validation and by using an adaptive governance approach to manage a wide range of use cases and API types.

Gartner

Predicts 2022: APIs Demand Improved Security and Management (Dec-2021)

Wallarm Helps You Regain Control and Reduce Risk

As rampant API growth surpasses the capabilities of traditional application management tools, the first step is to get all your APIs under control. Wallarm API Discovery enables you to inventory, track and correct issues based on actual user traffic.

Know your API Portfolio

Discover all your APIs, including Shadow APIs, Rogue APIs, Zombie APIs, and deprecated endpoints—so you can improve control of your attack surface and reduce risk.

Monitor Changes in your APIs

Get alerts when new APIs pop up or when existing APIs change—so you can minimize API drift and prioritize scrutiny (e.g., pen testing or bug bounty programs) and guard against protection gaps.

Segment your APIs

Differentiate assets in your portfolio, such as public-facing vs. internal or new vs. old—so you can tailor your security program to focus on critical needs and optimize your security efforts / spend.

Track Sensitive Data Usage

Understand sensitive data usage, including PII, financial & health data, credentials and more—so you can ensure compliance with applicable regulations / standards and reduce risk of improper exposure.

Compare Actual to Spec

Leverage automatically created OpenAPI (Swagger) specs based on actual traffic—so you can reduce security gaps and ensure security team has full visibility.

Detect & Respond to Threats

Quickly search for and assess latent or active threats such as newly published CVEs or CWEs, on-going brute force attacks, and more—so you can remediate issues before they become problems.

What It Does?

Wallarm API Discovery continuously analyzes actual traffic to:

- Enumerate all your managed and unmanaged APIs endpoints, including:
  - **Exposed and Internal APIs**—your real API footprint.
  - **Shadow APIs**—those you don't know about.
  - **Zombie APIs**—those that have been deprecated but are still alive.
  - **Rogue APIs**—those that exist outside of official security and operational processes.
  - **Legacy / Unused APIs**—those that should be removed but are still in use.
- Automatically build specs (OpenAPI / Swagger) of your APIs.
- Identify all changed or removed APIs and endpoints in your portfolio.
- Identify sensitive data usage, including PII, financial data, credentials and more.

How's It Deployed?

Wallarm API Security platform supports SaaS, public / private / hybrid cloud, or on-prem deployment.
It integrates into your existing API gateways, proxies, load balancers, and ingress controllers to ensure that all your external and internal APIs are discovered, cataloged, analyzed, and secured.
In addition, it integrates broadly into your existing security stack and workflow to reduce learning curve and to improve time-to-value.

Book a Wallarm demo
or start your free trial now

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107
www.wallarm.com