wallarm

Wallarm API Discovery

The source of truth for your APIs

The Wallarm API Discovery Module, part of Wallarm API Security, provides visibility into your entire API portfolio, allowing you to regain control over your API attack surface and minimize and associated risks.

APIs are crucial to every business. APIs and applications are exploding, there are over 1.3B active APIs as of 2013*. Discovering APIs is critical for effectively managing and securing API architectures. It helps organizations understand the APIs they have deployed, how these APIs are used, and the data they access.

Why do you need API Discovery?

Enterprise security teams are responsible for protecting critical applications, this requires complete visibility into the application architecture and its associated APIs. It helps security teams understand the APIs they have deployed, how these APIs are used, and the data they access. With the booming use of APIs comes increased risks from:

Sensitive Data Flows

As more and more organizations are pushing sensitive data through their APIs, including Personal Identifiable Information(PII), financial & health data, credentials and more. This increases the danger and impact of unintentional or malicious disclosure.

Rapidly changing API Portfolio

Today the need of the hour for development teams is to build fast and innovate. Oftentimes they rely on open source, 3rd party, and diverse set of tools, protocols and frameworks to build applications. This constant change adds more complexity to the security stack.

Growing API attack surface

Organizations struggle to manage the explosive growth in API use, both externally and internally which means they have an ever expanding attack surface to protect.

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 real-estate from security controls. This includes shadow APIs that you don't know about, Zombie APIs that are deprecated and should be removed but are still active, and Legacy APIs that you know about and should not be accessible to users.

wallarm

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.

Eliminate your API Blind spots with API Discovery

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.Wallarm API Discovery provides security teams with runtime visibility into their entire API portfolio. This allows the security teams to:

- Regain control over your API attack surface
- Build an inventory and track APIs based on actual user traffic
- Identify and remediate risky APIs based on real-time traffic and OpenAPI specs

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.

wallarm

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 & Block Threats

Quickly search for an assess latent or active threats such as newly published CVE's or CWEs, on-going brute force attacks, and more-so you can remediate issues faster.

Secure Critical Endpoints

Automatically tag business-critical endpoint functions like authentication, payment, and user management for visibility to ensure compliance and enhancing security posture.

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.

BOOK A DEMO

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