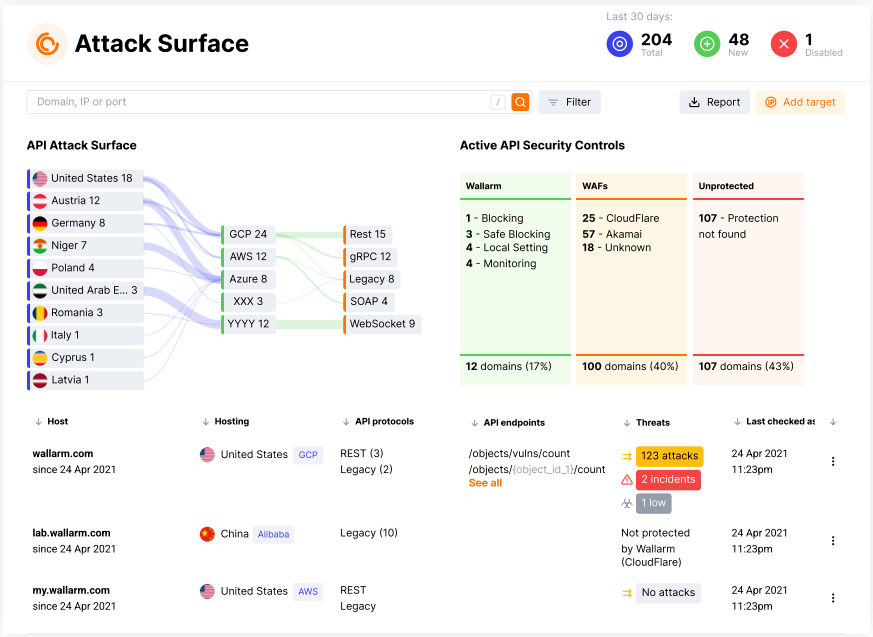
wallarm

SOLUTION BRIEF

Securing Your Digital Assets: Wallarm's API Attack Surface Management (AASM)

API Attack Surface Management (AASM) by Wallarm is an innovative solution designed for organizations to gain comprehensive control over their expanding API ecosystems. In a digital landscape where APIs are central to application delivery and integration, understanding and managing the associated attack surface is crucial.



A Holistic Approach with API Attack Surface Management

AASM stands out with its ability to offer a complete view and management of the API attack surface:

Domain and Subdomain Enumeration

Systematically identifies all host domains and subdomains under the organization's purview, ensuring no aspect of the network goes unnoticed.

API Discovery and Risk Assessment

Enumerates all APIs, evaluating and categorizing the risks they present. This step is crucial for understanding the potential attack vectors and preparing adequate defenses.

Application Assessment and Protection

Determines the presence and efficacy protecting each API, providing insights into the existing security measures and their effectiveness.

Security Misconfiguration Identification

Actively scans for and reports any security misconfigurations within the API setups, a common source of vulnerabilities.

API Leak Detection

Proactively identifies and alerts on any API secrets that have been inadvertently leaked, closing a critical gap in API security.

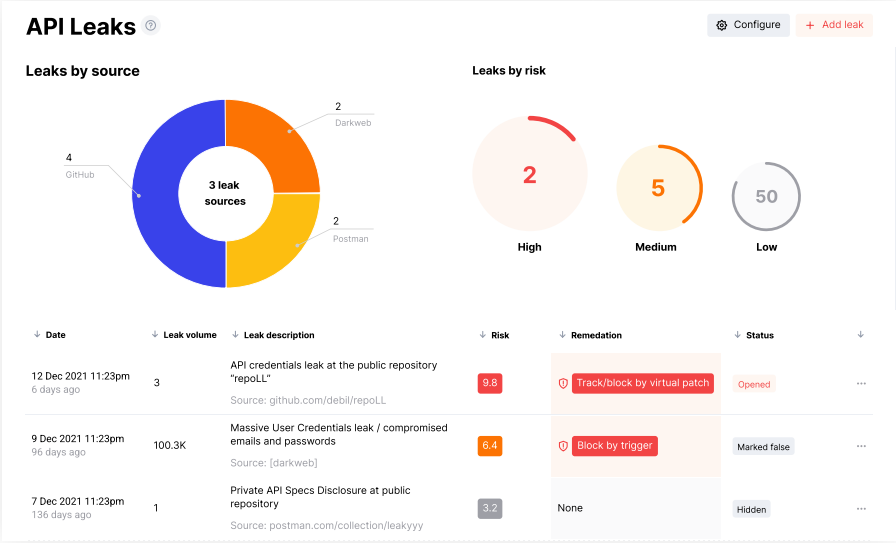
Transformation with Wallarm API Attack Surface Management

Before AASM

Prior to implementing AASM, organizations face limited understanding of their API vulnerabilities, exposing them to hidden attacks and unmitigated risks. This uncertainty can lead to surprise attacks or finding publicly exposed APIs. While they might use solutions like API gateways the lack of thorough discovery data could mean missing some threats. Moreover, without the ability to detect leaked API secrets, businesses are at risk of experiencing breaches that may be revealed by external sources.

After AASM

With the implementation of AASM, customers gain a comprehensive inventory of their API attack surface. This includes a detailed list of all APIs, the risks associated with them, and the protective measures in place. Customers are empowered to proactively utilize WAAPs offered by Wallarm) for API protection and governance. Additionally, AASM provides the capability to search for and catalog any leaked secrets, thereby enhancing security confidence and diminishing risk.



Enhancing Protection with API Leaks Detection

Complementing the broad capabilities of AASM, Wallarm's API Leaks Detection is the first generally available AASM capability aimed at preventing and managing inadvertent leaks of API secrets.

Core Capabilities of API Leaks Detection

- **Automated Detection of Leaks:** Wallarm continuously scans public repositories and digital platforms to detect any accidental leaks of API secrets, addressing a common yet critical security issue.
- **Proactive Token Management:** Upon detection of a leak, Wallarm enables immediate actions to block or manage compromised tokens, thus mitigating potential security breaches.
- **Comprehensive Tracking of Leaked Secrets:** Ensures ongoing monitoring and tracking of leaked API credentials, providing insights into their potential use and helping to prevent unauthorized access.

wallarm

SOLUTION BRIEF

API Leaks Detection Complementing AASM

While AASM provides an expansive view of the API attack surface, API Leaks Detection adds a focused, essential layer of security, specifically targeting the inadvertent exposure of sensitive API information. This integration ensures a fortified and comprehensive defense against a wide array of API-related security threats.

API Attack Surface Management

- Discover API Attack Surfaces
- Assess API Protection
- Detect API Leaks

Advanced API Security

- API Discovery, Posture Management
- API Security Testing
- API Abuse Prevention

Cloud WAAP

- OWASP Top-10
- API Protection
- Credential Stuffing, Distributed Rate Limiting

Integrated App and API Security Platform

Licensing and Packaging

AASM is available through various subscription plans based on the number of 'discovery seeds' an organization may wish to add. It offers flexibility, being available as a standalone product or in conjunction with Wallarm's Cloud-Native WAAP or Advanced API Security solutions.

AASM is available as a separate subscription, licensed by the number of ‘discovery seeds’ an organization wishes to add. A ‘discovery seed’ is any object that AASM uses to enumerate the attack surface, and includes domain names, text strings, and API tokens. Businesses can purchase AASM as a stand-alone or with Cloud-Native WAAP or Advanced API Security. AASM is available to Free Tier customers with a single discovery seed included.

How to Get Started

SIGN UP FOR A TIER ACCOUNT

Elevate your cybersecurity strategy with Wallarm's API Attack Surface Management and API Leaks Detection. Gain unparalleled visibility and control over your API ecosystem, and safeguard your digital assets against the evolving threats of the digital age. Reach out to Wallarm today to discover how these solutions can augment your strategic approach to API security.

BOOK A DEMO

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