wallarm

2024 CYBER 150 IT-Harvest

2025 WINNER CYBER SECURITY EXCELLENCE AWARDS

Advanced API Security

Wallarm is the fastest, easiest, and most effective way to stop API attacks, period. Wallarm protects APIs, AI Apps, and AI agents with a complete inventory of APIs, risk assessment, and real-time blocking of attacks.

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

PRODUCT DATASHEET

Why Do You Need API Security?

Protecting APIs, GenAI apps, and AI agents is critical for modern organizations. To do so, you need complete visibility into your entire API landscape with the ability to detect & block a new breed of threats – all without adding complexity to your security stack or workflows.

Growing Attack Surface

The rampant growth in AI and cloud has expanded the usage of APIs, both internal and public-facing, which means a large and growing attack surface requiring protection.

Targeting APIs is Easy

APIs are increasingly targeted by bots and other malicious abuse, which can lead to account takeover, credential stuffing, and disrupt end-user experience, putting business-critical services at risk.

Increasing Data Flows

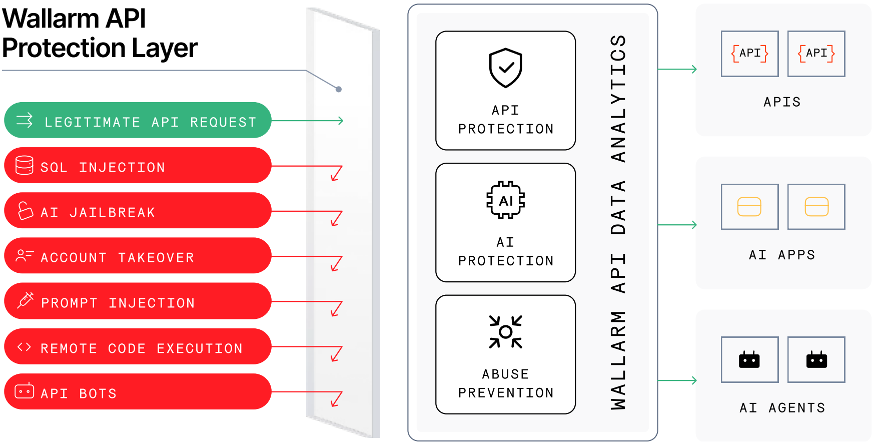
Organizations are pushing more sensitive data through APIs which increases the danger and impact of unintentional or malicious disclosure. The addition of GenAI apps and AI agents only exacerbates the problem of sensitive data transmitted over APIs.

Changing Threats

Advanced threats against APIs and AI are on the rise, while traditional attacks continue to increase in frequency. Modern API security requires a new, comprehensive approach to mitigate business risk.

API Security that Actually Blocks Attacks in Real-Time

API security that doesn't block attacks in real-time is too little, too late. Wallarm is designed from the ground-up to block attacks in real-time. Simply put, Wallarm is the fastest, easiest, most effective way to stop API attacks.



Advanced API Security Platform

The Wallarm platform delivers best-in-class API protection across multiple environments, supporting REST, GraphQL, gRPC, Websockets, and more. From simple injections to complex business logic attacks, Wallarm provides real-time protection against the API threats that matter, including those targeting AI. Wallarm addresses the following use cases.

API Attack Surface Management

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

API Discovery

- A complete inventory of API endpoints
- API endpoint risk scoring
- Rogue API detection

API Security Posture Management

- API endpoint risk scoring
- Sensitive data detection
- API specification enforcement

Real-Time API Protection

- Block API attacks in real-time
- Protection for REST, GraphQL, gRPC and more
- Block zero day attacks on day zero

API Abuse Prevention & Bot Management

- Machine-learning, behavior based detection
- API endpoint risk scoring
- Full visibility in API sessions

API Security Testing

- Active and passive vulnerability scanning
- Turn real-world attacks into API security tests.
- Remove risk before deploying to production

Trusted by Users, Hated by Attackers

Panasonic
VICTORIA'S SECRET
miro
UZ LEUVEN
Dropbox
Rappi
revenera
WARGAMING.NET LET'S BATTLE
SEMRUSH
SAMSUNG

> **"With Wallarm, we've been able to scale API protection to the scale we need and manage with our infrastructure-as-code approach."**
>
> Gustavo Ogawa, Head of Security, Rappi

Rappi