wallarm

PRODUCT DATASHEET

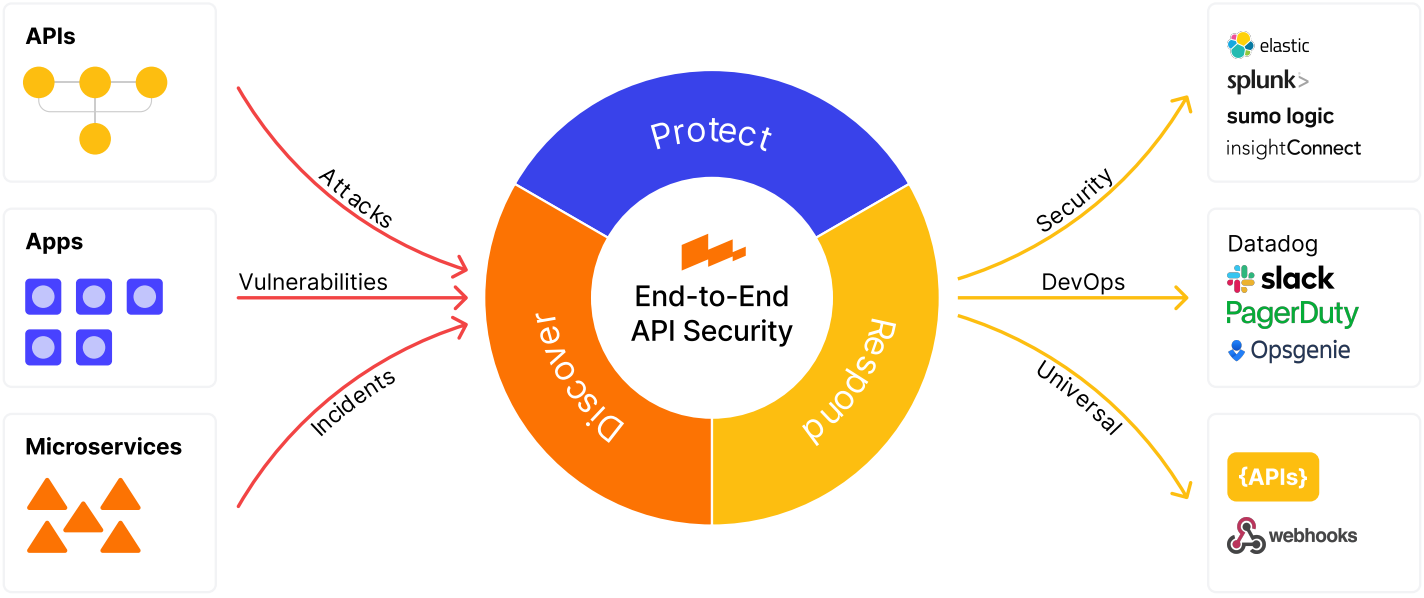
API Security Platform

Strong Foundation for Outstanding API Security

The Wallarm API Security Platform delivers our integrated product suite to protect your entire API and application portfolio in multi-cloud and cloud-native environments, along with integration into your existing security stack – to protect your entire API and application portfolio.

Wallarm Delivers Cloud-Native Application Security

Wallarm API Security Platform provides the underlying infrastructure for all Wallarm products and services, along with deployment and integration support, required to enable comprehensive advanced API security and cloud-native WAAP capabilities – to better protect your customers and internal users.



Discover

- Inventory all your assets automatically
- Map and track changes in exposed APIs and services
- Reconstruct API and app topology from the traffic
- Identify sensitive data usage

Protect

- Secure against OWASP Top 10
- Mitigate API specific threats
- Block bots and L7 DDoS

Respond

- Monitor threats with complete observability
- Drill down into malicious requests
- Receive alerts on only the incidents that matter

API Security Made Easy

The Wallarm API Security Platform delivers the power of our Advanced API Security and Cloud-Native WAAP solutions.

Advanced API Security

Provides comprehensive API protection against OWASP API Security Top-10 risks and other advanced API threats – including comprehensive visibility into your API estate, detection and remediation of API vulnerabilities and threats, and protection of sensitive data.

Cloud-Native WAAP

Provides next-gen web application & API protection (WAAP) against OWASP Top-10 risks – including unified protection to stop emerging threats and eliminate false positives while extending your existing security stack.

It delivers our integrated product suite and enables integration into your existing security stack, which produces unmatched benefits for DevOps and Security teams charged with securely delivering and supporting cloud-native applications.

- Designed for privacy, flexibility and performance
- Hybrid SaaS approach offered "as a service"
- Supports all protocols (REST, SOAP, GraphQL, gRPC, WebSocket)
- Enables easy installation in any environment
- Serves up tightly coupled plug-and-play products and services
- Provides prevention, detection, and response capabilities via single platform
- Delivers comprehensive visibility across entire API estate
- Applies security coverage that spans all API threat vectors
- Facilitates central management and reporting across all products and services
- Bolsters DevSecOps effectiveness and efficiency in support of sweeping API Security
- Maintains extensive support for partner ecosystems and third-party integrations

Design Principles

At the foundation of the Wallarm design ethos is privacy, flexibility and performance.

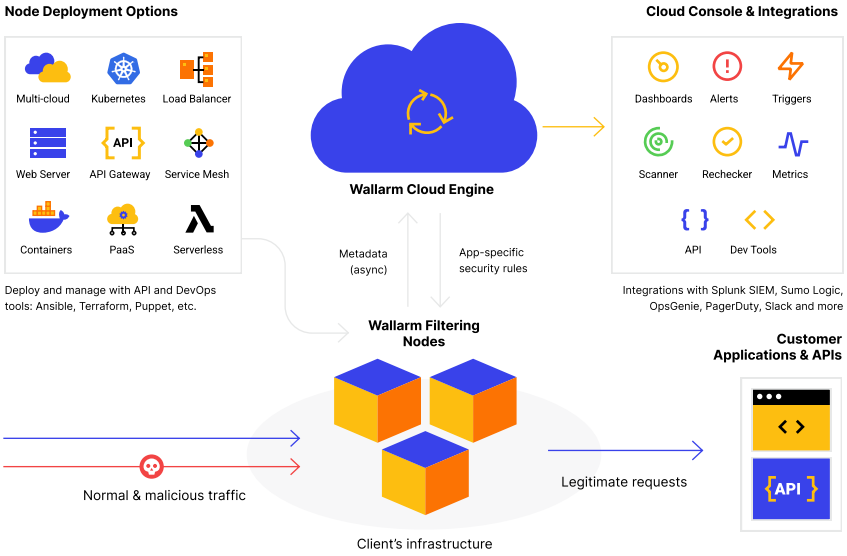
- **Privacy.** All traffic inspection is handled within the customer environment, with only metadata and sanitized & redacted malicious requests being sent to the Wallarm Cloud Engine.
- **Flexibility.** Wallarm nodes can operate out-of-band analyzing copy of traffic or be deployed inline with a variety of the cloud-native options.
- **Performance.** Wallarm delivers broad API security with near-zero latency and false positives to minimize impact on end-users and security teams alike.

Key Benefits

- **Performant.** Cloud-native design optimized for maximum performance and near-zero latency that scales web app and API threat protection to meet your current and future needs.
- **Vigilant.** Protect your portfolio against emerging threats, including: OWASP Top-10 web app & API risks, other API-specific threats, credential stuffing (ATO), JWT attacks, and 0-day exploits.
- **Trusted.** The leader in G2's API Security category, and relied on by 200+ customers to protect over 20,000 applications.

How It Works

Wallarm nodes are injected between the public Internet (where end-users are typically located) and the protected application, and act as reverse proxies for end-user requests. All the traffic inspection is handled within the customer environment with Wallarm nodes, and only metadata and sanitized and redacted malicious requests are sent to the Wallarm Cloud Engine.



Where It Works

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 maximize time-to-value.

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

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