wallarm

PRODUCT DATASHEET

API Threat Prevention

Automated Protection Against API Threats and API Abuse

The Wallarm API Threat Prevention module, part of Wallarm API Security platform, provides comprehensive real-time protection against advanced API threats which jeopardize your internal and end-user operations.

Advanced API Security at a Glance

Wallarm API Threat Prevention provides comprehensive real-time API threat protection. Key Benefits include:

Coverage

Protect all your API assets regardless of protocol – from REST and SOAP to GraphQL, gRPC and WebSocket – from API-specific risks.

Detection

Identify, consolidate and prioritize unique API risks, from OWASP API Security Top-10 threats to API abuse, to optimize security team effectiveness and workload.

Response

Assess and remediate any weaknesses which open you up to attack, and automatically implement rules to protect against any further assaults.

Why Do You Need API Threat Prevention?

As you adopt an API-first approach to support customers, partners, and internal operations, you need API-focused protection for your growing API portfolio from these security challenges.

Growing Attack Surface

The explosive growth in API use, both internal and public-facing, means a rapidly changing API portfolio with a great number of them unmanaged – which results in a sizable and expanding attack surface.

Focused API Protection

OWASP API Security Top-10 risks (Injections, BOLA, RCE, etc.) and other advanced API threats are on the rise – which requires a new API-first security approach to mitigate organizational risk.

Sensitive Data Protection

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 Abuse Prevention

API bot, L7 DDoS and other automated behavioral attacks are increasing – which can lead to ATO & carding attacks, disrupt end-user experience, and put business-critical services at risk.

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

Protect any API

- Complete protocol support: REST, GraphQL, gRPC, WebSocket
- Microservices
- Serverless

In any environment

- AWS, GCP, Azure, IBM Cloud
- Private, Hybrid and Multi-Cloud
- Kubernetes / Service Mesh
- Zero-Trust

Against any threats

- OWASP Top-10 Risks and Sophisticated API Threats
- API Abuse (bots, L7 DDoS)
- Account Takeover (ATO) / Credential Stuffing

Wallarm Helps You Reduce API Risks

Wallarm API Threat Prevention provides comprehensive security against API threats across your entire cloud-native API portfolio:

Defends Against OWASP Top-10 API Risks. Get full coverage against API-specific threats (e.g., Injections, BOLA, RCE, etc.), and scan & mitigate vulnerabilities continuously – to ensure your end-user and internal operations are not jeopardized.

Safeguards Sensitive Data. Understand where sensitive data (e.g., PII, API keys, etc.) is used and limit unintentional and/or inappropriate exposure – to reduce data breach and compliance risks.

Blocks API Abuse. Stop application layer Denial-of-Service (L7 DoS), account takeover (ATO), and credential stuffing attacks with flexible rules and session / token management – to limit automated abuse and ensure critical business services are not interrupted.

Brings Full Protocol Support. Get support for modern API protocols (including REST, SOAP GraphQL, gRPC, and WebSocket), automatic recognition of different protocols / formats, and ability to chain parsers for payload decoding – to ensure continuum of coverage across your entire API portfolio.

Consolidates API Security Stack. Implement best-in-class API threat detection and response capabilities via single tool which deploys anywhere and integrates with your existing security stack – to ensure full spectrum protection without adding workflow and operational costs.

Key Benefits

- **Performant.** Cloud-native design optimized for maximum performance and **near-zero latency** that scales API threat protection to meet your current and future needs.
- **Vigilant.** Protect your APIs against emerging threats, including: **OWASP API Security Top-10** and 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**.

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.

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