

Advanced API Security

Advanced Coverage for Modern Environments

Wallarm Advanced API Security provides comprehensive real-time API discovery and threat prevention across your entire portfolio – regardless of protocol – in multi-cloud and cloud-native environments.

Why Do You Need Advanced API Security?

APIs are crucial to your organization. You need API-focused monitoring and security to protect them.



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 means 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.



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 API Threats
- API Abuse (bots, L7 DDoS)
- Account Takeover (ATO) / Credential Stuffing

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



“

Advanced API Security at a Glance

Wallarm Advanced API Security consists of two modules: API Discovery and API Threat Prevention. Combined, these modules provide the advanced API security coverage required to address the compliance and business risks associated with modern API-first organizations.

Wallarm API Discovery

Know your API Portfolio – including Shadow and Zombie APIs to improve control over attack surface.

Subdivide your APIs – such as internal vs. public-facing APIs to tailor your security efforts.

Compare Actual to Spec – based on actual traffic to reduce gaps in security coverage and documentation.

Monitor Changes in your APIs – such as new APIs, changed APIs, or drift from spec to minimize gaps in security coverage.

API Risk Scoring & Assessment – providing ability to triage problematic endpoints and prioritize mitigation efforts.

Track Sensitive Data Usage – including PII, financial & health data, credentials, etc. to ensure compliance.

Detect Weak Authentication – including JWT weaknesses and attacks to deter unauthorized access.

Wallarm API Threat Prevention

Full API Protocol Support – including REST, GraphQL, gRPC, WebSocket to protect modern API portfolios.

Virtual Patching – prevent 0-day exploitation to limit damage until patches are available.

Real-time Mitigation – without relying on 3rd party tools to ensure seamless & efficient workflow.

OWASP API Security Top-10 – protect against advanced API threats to strengthen your security posture.

API Abuse Prevention – including behavioral and advanced rate limiting protection against bot and L7 DDoS attacks to mitigate service & security impacts.

Session Management – automate response and configure security controls with granular session-based rules to reduce workload and optimize protection.

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