wallarm

PRODUCT DATASHEET

End-to-End API Security

One Solution to Protect Them All

Wallarm is the only solution that unifies best-in-class API Security and WAAP (Next-Gen WAF) capabilities to protect your entire API and web application portfolio in multi-cloud and cloud-native environments.

Why Do You Need End-to-End API Security?

Protecting APIs and web applications is crucial for modern organizations. To do so, you need complete visibility into your entire portfolio with the ability to detect & respond to a new breed of threats – all without adding complexity to your security stack or workflows.

Growing Attack Surface

The rampant growth in cloud-native applications is expanding the managed and unmanaged web apps & APIs being used in your organization, both internal and public-facing – which means a large and growing attack surface.

Changing Threats

OWASP Top-10 threats for web apps & APIs (Injections, BOLA, RCE, etc.) and other advanced threats are on the rise – which requires a new comprehensive security approach to mitigate organizational risk.

Increasing Data Flows

More organizations are pushing more sensitive data through their web apps & APIs, including PII, financial & health data, credentials and more – which increases the danger and impact of unintentional or malicious disclosure.

Inherently Open Designs

Bots, L7 DDoS and other automated behavioral attacks are increasingly abusing the essential nature of your web apps & APIs – which can lead to ATO & credential stuffing attacks, disrupt end-user experience and put business-critical services at risk.

Protect any web app or API

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

In any environment

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

Against any threats

- OWASP Top-10 Threats for web apps and APIs
- API Abuse (bots, L7 DDoS)
- Account Takeover (ATO) / Credential Stuffing

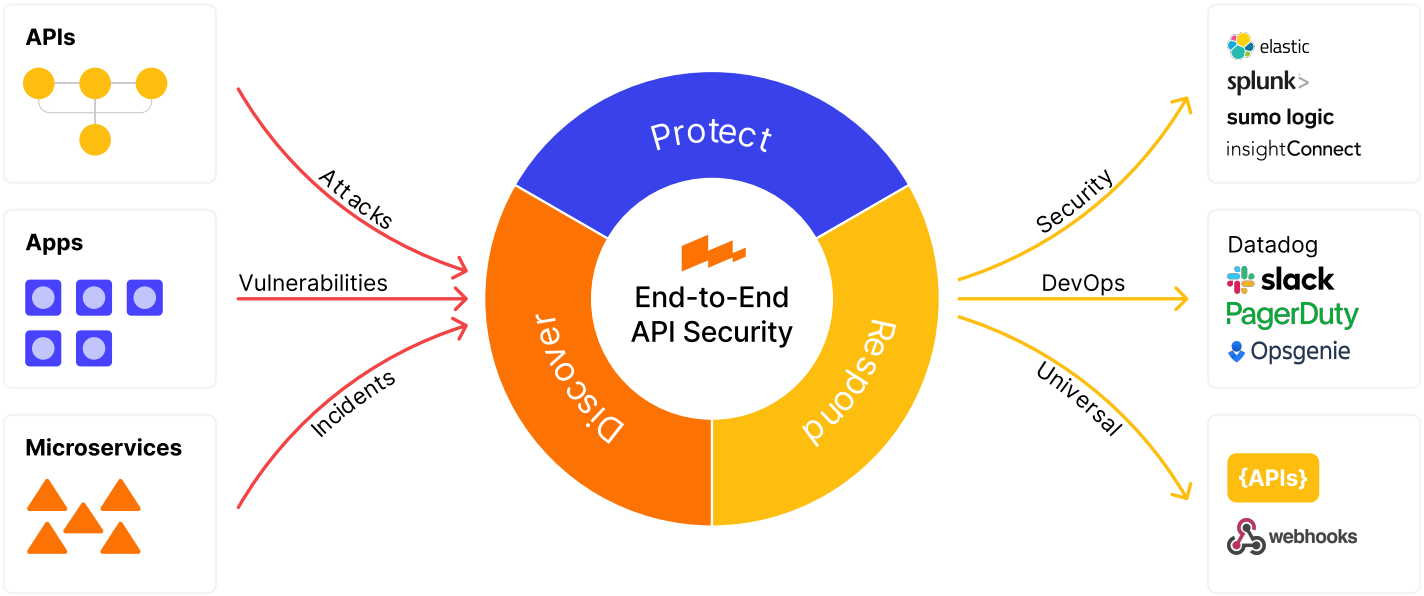
Design Principles

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.

End-to-End API Security

Security and DevOps teams choose Wallarm to discover all cloud-native APIs and legacy web applications running in their environment, and to detect & respond to threats against them.



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
- Identify sensitive data usage

Respond

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

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

Comprehensive Protection for APIs and Web Applications

Wallarm End-to-End API Security provides superior protection for your cloud-native applications – to address your digital transformation, compliance, zero-trust and API & web application security challenges.

Advanced API Security

Provides comprehensive API protection against OWASP API Security Top-10 risks and other advanced API threats.

Know your API Portfolio. Monitor your API portfolio for new / changed APIs, drift from spec, or unmanaged (including Shadow and Zombie) APIs – to improve attack surface control and minimize security coverage gaps.

Eliminate API Risk. Track and remediate risky API endpoints, especially those handling sensitive data such as PII, credentials, etc. – to prioritize API security efforts and minimize compliance & breach risks.

Guard Against API Vulnerabilities. Apply virtual patches and real-time mitigations without relying on 3rd party tools – to prevent 0-days and limit potential damage with a seamless & efficient workflow.

Boost your API Security. Protect against OWASP API Security Top-10 risks, other advanced API threats, and API abuse (such as ATO, bots, L7 DDoS) – to strengthen your security posture and reduce service & security impacts on customers and internal users.

Cloud-Native WAAP

Provides next-gen WAF and web application protection against OWASP Top-10 risks and emerging threats.

Unified Protection. Secure and manage your entire estate across any environment with a single solution – to improve coverage and workflows while reducing overhead.

Stop Emerging Threats. Defend against malicious bots, L7 DDoS, ATOs, 0-day exploits and other growing risks – to get full spectrum protection for web applications.

Eliminate False Positives. Scale protection automatically using grammar-based attack detection without relying on manual rules (RegEx) – to reduce workload and improve efficiencies.

Extend Existing Security Stack. Leverage your existing DevOps and security tools with native integrations, webhooks or APIs – to reduce learning curve and time-to-value while extending protections.

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.

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