wallarm

PRODUCT DATASHEET

Integrated App and API Security

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

Why Do You Need 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.

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.

Targeting APIs is Easy

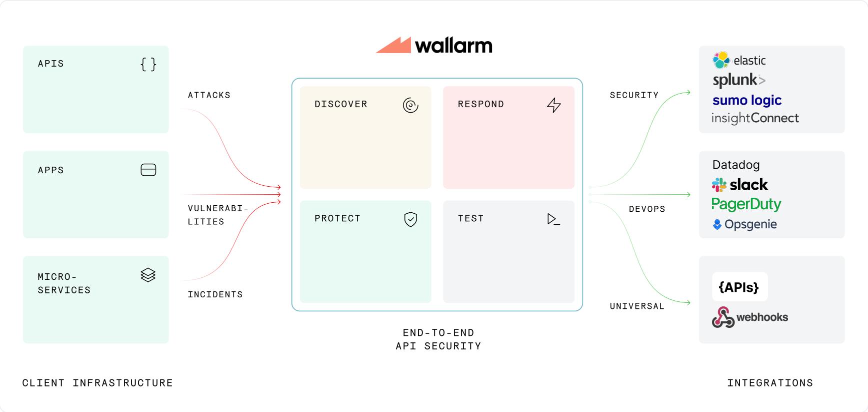
Bots, L7 DDoS and other automated behavioral attacks are increasingly abusing the essential nature of your APIs – which can lead to ATO & credential stuffing attacks, disrupt end-user experience and put business-critical services at risk.

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.

End-to-End Approach for the Application and 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 (OWASP API Security)
- Block bots and L7 DDoS
- Safeguard sensitive data use
- Upload and enforce API specifications to detect and block non-compliant API requests

Respond

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

Test

- Automate API security testing in CI/CD
- Discover misconfiguration issues
- Remediate API vulnerabilities during development

Integrated Application and API Security Platform

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

API Attack Surface Management

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

Advanced API Security

- API Discovery, Posture Management
- API Security Testing
- API Abuse Prevention

Cloud WAAP

- OWASP Top-10
- API Protection
- Credential Stuffing, Distributed Rate Limiting

Integrated App and API Security Platform

> **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

API Attack Surface Management (AASM)	Advanced API Security	Cloud-Native WAAP
Domain and Subdomain Enumeration AASM systematically identifies all host domains and subdomains under an organization's purview, .ensuring no aspect of the network goes unnoticed.	**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.	**Unified Protection** Secure and manage your entire app and API estate across any environment with a single solution – to improve security coverage and workflows while reducing overhead.
Security Misconfiguration Identification AASM actively scans for security misconfigurations within API setups, a common source of vulnerabilities.	**Assess API Risk** Track and remediate risky API endpoints, especially those handling sensitive and PII data – to prioritize API security efforts and minimize compliance & breach risks.	**Stop Emerging Threats** Defend against OWASP Top-10, malicious bots, L7 DDoS, ATOs, 0-day exploits and other growing risks – to get full spectrum protection for web applications and APIs.
API Leak Detection Actively detecting and promptly informing on inadvertently leaked API secrets is another vital feature, closing a critical gap in API security.	**Guard Against API Vulnerabilities** Apply real-time mitigations without relying on 3rd party tools – to prevent 0-days and limit potential damage with a seamless & efficient workflow.	**Eliminate False Positives** Scale protection automatically using grammar-based attack detection without relying on manual rules (RegEx) – to reduce workload and improve efficiencies.
API Discovery, App and Risk Assessment and Protection Catalogs all APIs, evaluating and classifying risks. Helps organizations identify possible attack paths and fortify their security. Checks the protection of each API, offering details on current security strategies and effectiveness.	**Boost your API Security** Protect against OWASP API Security Top-10 risks, other advanced API threats, and API abuse – to strengthen your security posture and reduce service & security impacts on customers and internal users.	**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.