wallarm | Built for Kubernetes

SOLUTION BRIEF

End-to-End API Security for Kubernetes Environments

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.

Advanced API Security and WAAP (Next-Gen WAF) Built for Kubernetes

With a high pace of innovation and constantly evolving threat landscape, protecting apps and APIs is harder then ever. Shortcomings of traditional security solutions are impediments for digital transformation: deficient in detecting new threats, high cost of maintenance, and lack of integration with cloud-native stacks. Wallarm provides modern protection for web applications and APIs (WAAP), in any customer environment — all via one integrated platform.

Robust protection for APIs wherever they are running

Wallarm elegantly deploys in any environment to protect thousands of exposed and internal workloads: in datacenter or cloud, multi-cloud or Kubernetes-based environment. So you can secure and manage your entire estate with one unified solution.

Stop Advanced Threats

Protect any apps and APIs (grapQL, gRPC, REST, SOAP and others) against well-known OWASP-Top-10 and advanced threats, such as Injections, BOLA, and authentication failures.

Sensitive Data Protection

Understand sensitive data usage, including PII, financial & health data, credentials and more —so you can ensure compliance with applicable regulations / standards and reduce risk of improper exposure.

Manage Growing Attack Surface

Discover all your APIs, including Shadow APIs, Rogue APIs, Zombie APIs, and deprecated endpoints—so you can improve control of your attack surface and reduce risk.

Use Accounts Protection

Prevent Account Takeover (aka Credential Stuffing) and other behavior-based attacks and API abuse which can lead to large-scale breaches.

CLOUD NATIVE COMPUTING FOUNDATION

Why Wallarm

- **Fast deployment anywhere.** Cloud-native, multi-cloud, edge or on-prem – DevOps tems have protection up and running **in 15 minutes**.
- **High accuracy. 88% of customers use** Wallarm protection in full blocking mode and trust its accuracy.
- **Complete protection.** One unified solution to protect all your assets, including APIs and apps, exposed and internal.

#1 API Security Solution by customer reviews

Panasonic · Victoria's Secret · miro · Gannett · Dropbox · tipalti

wallarm

Solution Brief

Protecting any internal and external app or API

- graphQL, REST, gRPC, SOAP
- Web Applications
- Microservices
- Serverless

In any cloud-native environment

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

Against any threats

- OWASP Top-10 Threats
- API-specific Threats
- Credential Stuffing (ATO)
- API Abuse and Bots

Complete Protection Against Full Spectrum Of Threats

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.

Cloud-Native WAAP

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

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

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

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

Distributed Rate Limiting – Define thresholds and prevent automated tools (such as bots and L7 DDoS) from overwhelming your workloads.

Advanced API Security and Discovery

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

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

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.

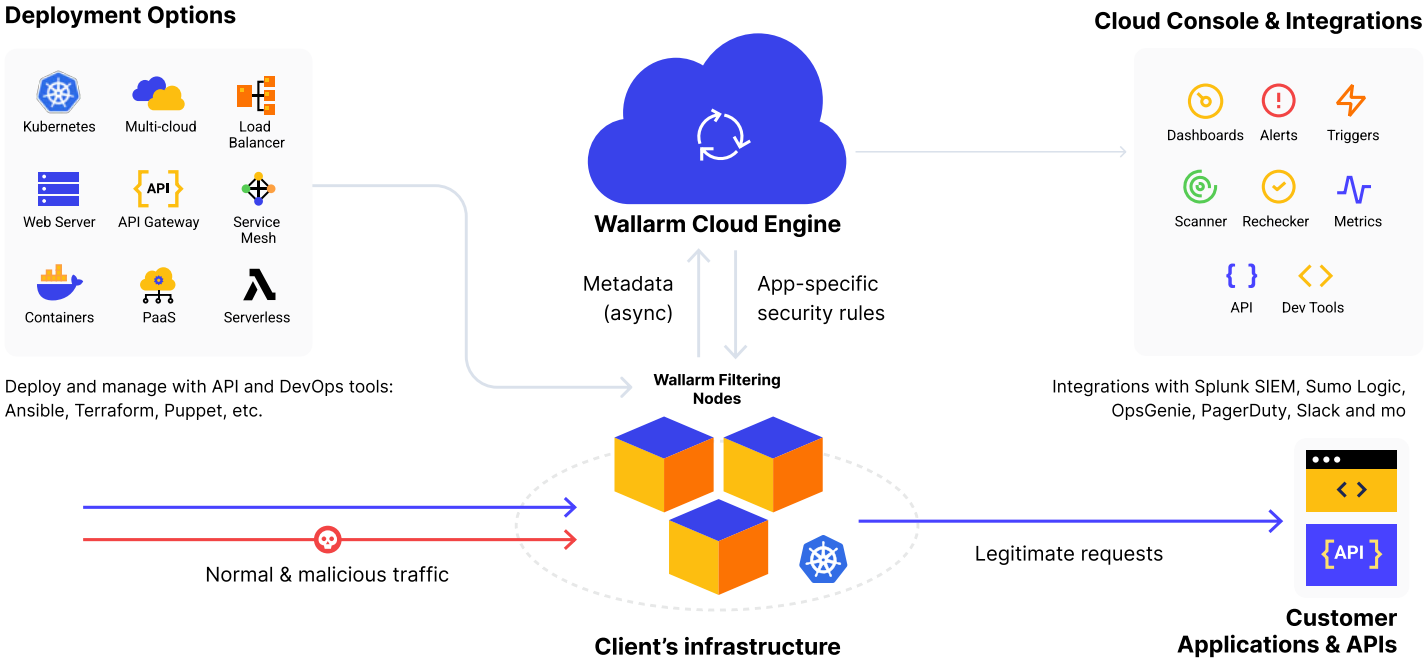
Track Sensitive Data Usage – including PII, financial & health data, credentials, etc. to ensure compliance.

We needed a solution that is ready for our massive microservices architecture and can be managed over API. Wallarm turned out to be the best fit to protect our backend APIs across multiple regions.

Gustavo Ogawa, Head of Security, Rappi

Rappi

Wallarm Cloud-Native Technology



Architected for privacy. 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.

Innovative attack detection. Innovative attack detection. Deep Request Inspection and grammar-based attack detection are core Wallarm technologies. Attack detection doesn't rely on RegEx and eliminates the maintenance hurdles typical of security solutions. Results include industry-best levels of both false positives (incorrectly blocked requests) and false negatives (missed attacks).

Reliable and scalable. Wallarm nodes have a fail-open design and are optimized for performance and near-zero latency. Integrate protection into your existing environment and DevOps/IaaC toolchain and scale protection up and down—the same way as you manage rest of your infrastructure. Wallarm inspects traffic of all protocols (APIs)—without prior configuration and specs.

Unified console and integrated workflows. Wallarm Console provides unique visibility and actionable insights into malicious traffic across the entire footprint. The same data is available through out-of-box integrations, webhooks, and API—so that you can build your incident response procedures and SOC operations leveraging your existing DevOps and security tools.

Where we find Wallarm to be a distinguished security partner for us is in their superb support and false positive management, two things you can't go without when application security is key and no compromise on coverage or resilience is acceptable.

Alexander Getsin, Senior Information Security Architect, Tipalti

tipalti

Fast Deployment Everywhere

The unique architecture enables you to quickly install in diverse environments by mixing different deployment options—and yet manage everything with one unified console.

Kubernetes or container-based infrastructure

Deploy Wallarm site-wide with the Ingress Controller or with the flexibility of an Envoy-based sidecar proxy for select services to enable both north-south and east-west traffic analysis.

Cloud and multi-cloud

Jump-start deployment with pre-built images available in cloud providers' marketplaces, like AWS, GCP, MS Azure, or IBM Cloud. Get Wallarm up and running in any public or private cloud, or any combination of them.

Native integration with web servers, load-balancers and API Gateways

Native integration with load balancers (e.g., NGINX, Envoy) or API Gateways (e.g., Kong) avoids added complexity and inspects traffic with near-zero latency.

Private data center

Wallarm API Security platform is architected to provide the same web app and API protection in your private cloud and datacenters as in public clouds, or any combination of them.

Out-of-band deployment

For faster POV or when deploying inline is not an option, Wallarm can analyze your web app and API traffic by tapping to cloud-native technology (such as VPC mirroring in AWS).

At the edge / Cloud WAAP (SaaS)

A simple change of DNS record will route application traffic thorugh the distributed network where Wallarm runs on the edge. This enables deployment as fast as 15 minutes and the benefits of a cloud service (such as CDN, cache, and others).

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