wallarm

PRODUCT DATASHEET

Wallarm Cloud-Native WAAP Product

Unified API and Application Security for Any Environment

With a high pace of innovation and constantly evolving threat landscape, protecting apps and APIs is harder then ever. Shortcomings of traditional WAFs are impediments for digital transformation: deficient in detecting new threats, high cost of maintance, and lack of integration with the 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 apps and 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
Get protection beyond OWASP Top 10 for full coverage against emerging threats: account takeover (ATO), malicious bots, L7 DDoS, and exploitation of 0-day vulnerabilities.

Eliminate false positives
Scale protection without the burden of manual rules tuning typical with traditional WAFs. We provide near-zero false positives with grammar-based attack detection (not RegEx), threshold-based blocking mode and managed SOC so that over 88% of our customers use Wallarm in blocking mode.

Effective incident response and remediation
Leverage your existing DevOps and security tools with a variety of native integrations, webhooks or APIs. Stay informed with actionable alerts and configurable triggers in your existing solutions.

Key benefits:

High accuracy
88% of customers use Wallarm protection in full blocking mode and trust its accuracy.

Fast deployment anywhere
Cloud-native, multi-cloud, edge or on-prem – DevOps tems have protection up and running **in 15 minutes**.

Trusted by the best
Leader in the WAAP/WAF category by G2, and trusted by customers to protect over **20,000 applications.**

wallarm

Product Datasheet

Protect any web app or API

- REST, SOAP, graphQL
- Web Applications
- 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 Threats
- API-specific Threats
- Credential Stuffing
- API Abuse

Trusted Protection Against Full Spectrum Of Threats

OWASP Top-10
Protect against advanced threats and well known OWASP Top-10 attacks.

Block Disallowed Geographies
Serve only trusted regions. Block unwanted geographies to meet compliance requirements.

API Protection
Defend your APIs in seconds without relying on tedious manual configurations and outdated or inaccurate API specs.

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

Credential stuffing (ATO) and Brute Force
Stop behavior-based attacks by inspecting and correlating sequences of requests.

PCI DSS and Other Compliance
Meet compliance requirements by tracking sensitive data usage and enabling protection.

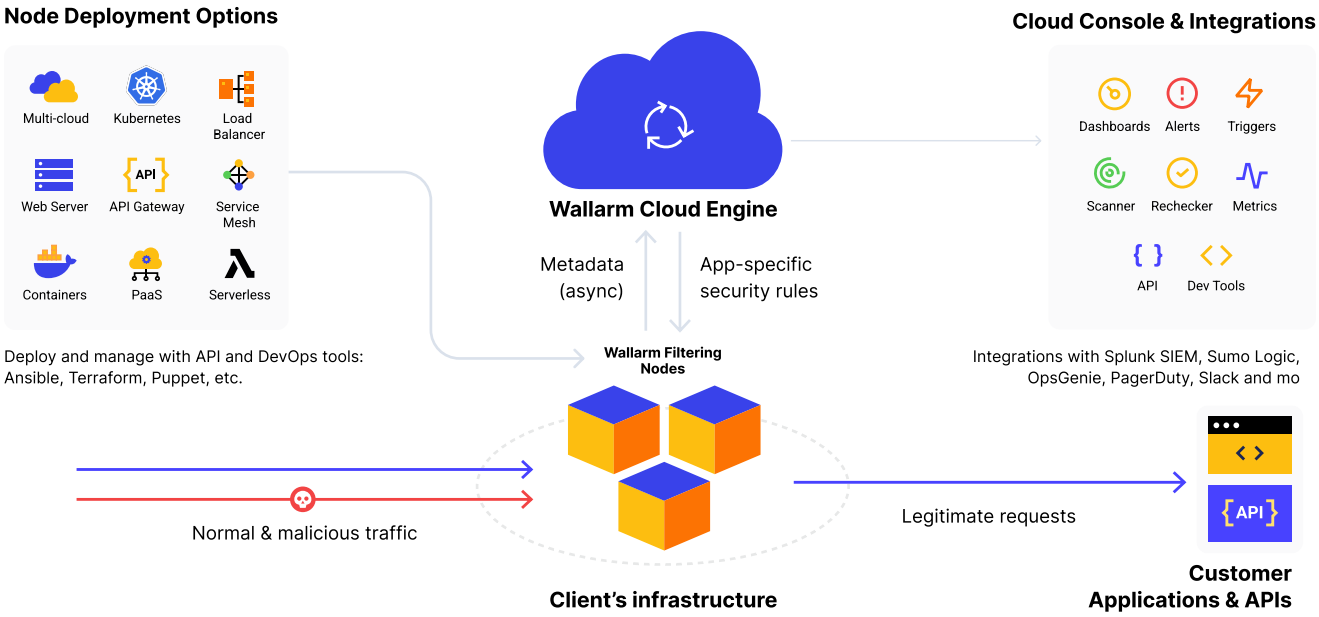
Virtual Patching
Drastically reduce 0-day risks by applying virtual patches to critical issues on the fly.

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 Next-Gen WAFs. 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.

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.

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.

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.

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).

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

Trusted by the Best

End-to-end web app and API protection

Trusted by Fortune 500 and the largest tech companies

#1 G2

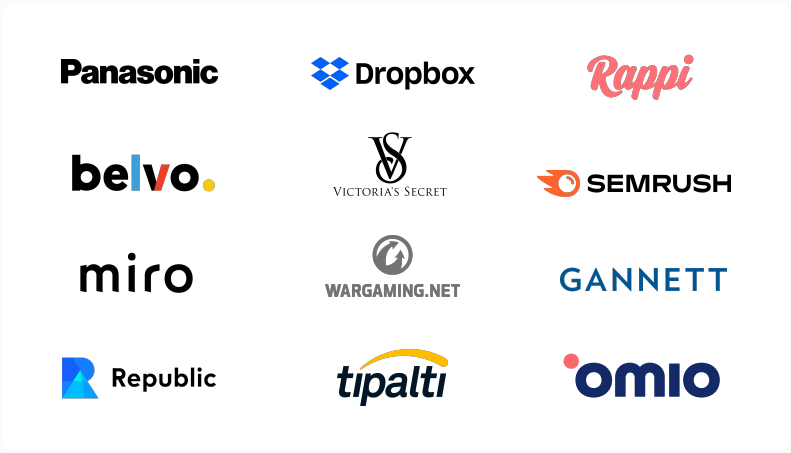
API Security Solution by customer reviews at G2

180B

API requests protected, daily

20K+

Protected APIs and web apps



To learn more about Wallarm, visit wallarm.com or contact the team at request@wallarm.com

The major requirements are the ability to auto-scale to support billions of requests per month and the ability to support new tech stacks, gRPC and graphQL protocols, and new attacks. While doing these we needed to have near real-time visibility into what's happening and how we can detect, analyze and defend against attacks on Miro applications.

Roman Bulbenko
Head of Application Security, Miro

miro