



# Secure NGiNX Infrastructure Powered by AI

Wallarm AI-Powered Security Platform automates application protection and security testing. High-performance in-line protection for NGINX/NGINX+ powered websites, microservices, and APIs running on private and public clouds.

## Key Benefits

- \* Protects from OWASP Top 10 and 0-day attacks
- \* Used in blocking mode by 88% of the customers
- \* Low maintenance with AI-adapted automated security rules
- \* Minimal manual analysis powered by Active Threat Verification
- \* API abuse and bot protection
- \* Excellent accuracy/low false positives
- \* Integration with existing infrastructure and CI/CD pipelines
- \* Managed by DevOps tool chain

**Adaptive AI Platform**  
learns application context and detects patterns

**Attack blocking**  
Dynamically generate signature-free security rules

**Security Testing**  
Active attack recheck for threat verification

**NGWAF for API & web security**  
with ultra-low false positives and incident alerting

## Supported Platforms

Traffic filtering is performed by Wallarm nodes. Nodes can be installed on the application server, as reverse proxies or within the load balancer infrastructure with multi-platform support:

- \* **As a module**  
NGINX/NGINX+, Kong API Gateway
- \* **As a container or VM**  
Docker, VMware VM
- \* **Linux package**  
RHEL/CentOS, Debian, Ubuntu

## Public Clouds Support

AWS, MS Azure, Google/GCP, Heroku

## Native Support for API and HTTP Protocols

HTTP / 2.0, WEBSOCKETS, REST API, JSON, XML, SOAP

## Application Stack Agnostic

NodeJS, Go, Ruby / RoR, PHP, .Net, Java, Python SAP, Oracle BS, SharePoint

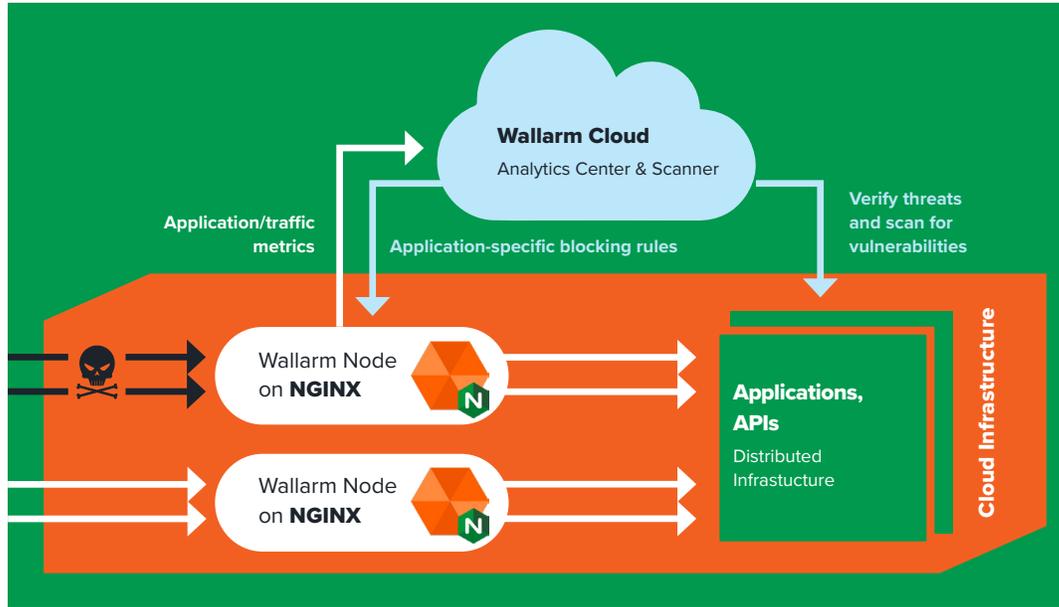


**Built for cloud-native enterprise applications**

- \* AI-powered accurate detection
- \* Unified management across all node clusters
- \* Low maintenance / no manual rule updates
- \* Incident alerting based on actual risk

**NGINX Plus Certified Module**

Customers are assured that Wallarm Next Generation WAF has passed a battery of certification tests, has available support, and is certified with the latest version of NGINX Plus.

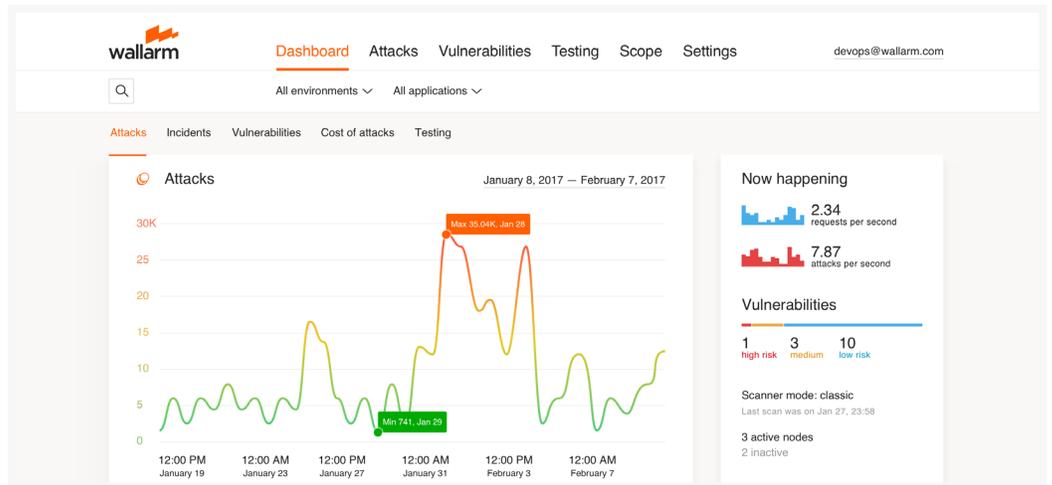


Wallarm is addressing quite a challenging problem of web application security in continuous integration environment. We like the approach the company is taking, and we'll be looking closely at their developments.

**Gus Robertson,**  
CEO at Nginx Inc.

Wallarm hybrid architecture is well suited for SaaS applications. The solution scales horizontally. Filtering nodes can be installed with load balancing nodes, such as NGINX Plus and can achieve similar scale with little overhead.

Initial statistical analysis of the traffic is performed locally by the nodes. Then anonymized app traffic statistics is sent to Wallarm Cloud for AI analysis to develop app specific blocking security rules which are downloaded to the nodes.



Protect and monitor your web application and APIs in real-time with zero false positives.

Get protected in minutes. Start your 14-day free trial today!

web: [wallarm.com](http://wallarm.com)  
twitter: [@wallarm](https://twitter.com/wallarm)  
phone: **(415) 940-7077**  
email: [request@wallarm.com](mailto:request@wallarm.com)

**SIGN UP FOR A FREE TRIAL!**