wallarm

CLOUD NATIVE
COMPUTING FOUNDATION

Secure Kubernetes Infrastructure Powered by AI

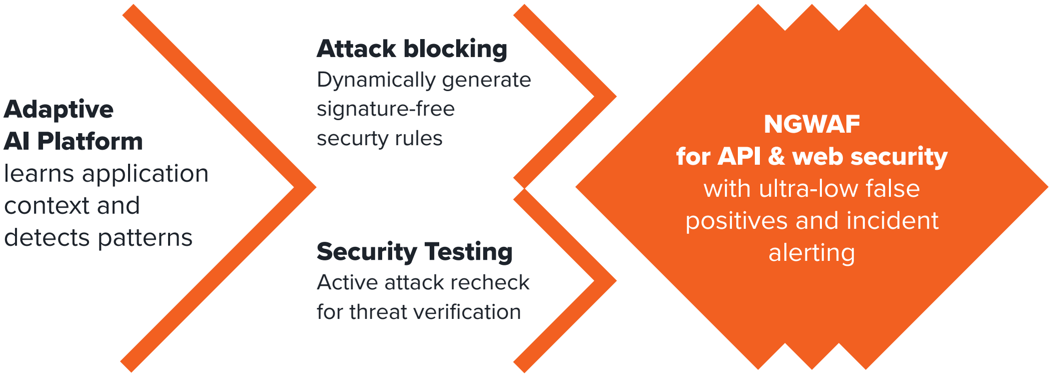
Wallarm AI-Powered Security Platform automates application protection and security testing. Installed directly on an Ingress controller, Wallarm protects websites, microservices, and APIs powered by Kubernetes and running on private and public clouds.

wallarm.com

Adaptive application security

Key Benefits

- Protects from OWASP Top 10 and 0-day attacks
- Integrates natively with the Kubernetes infrastructure
- 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 securty 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 an instrumented Ingress controller
- 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 wallarm

wallarm.com

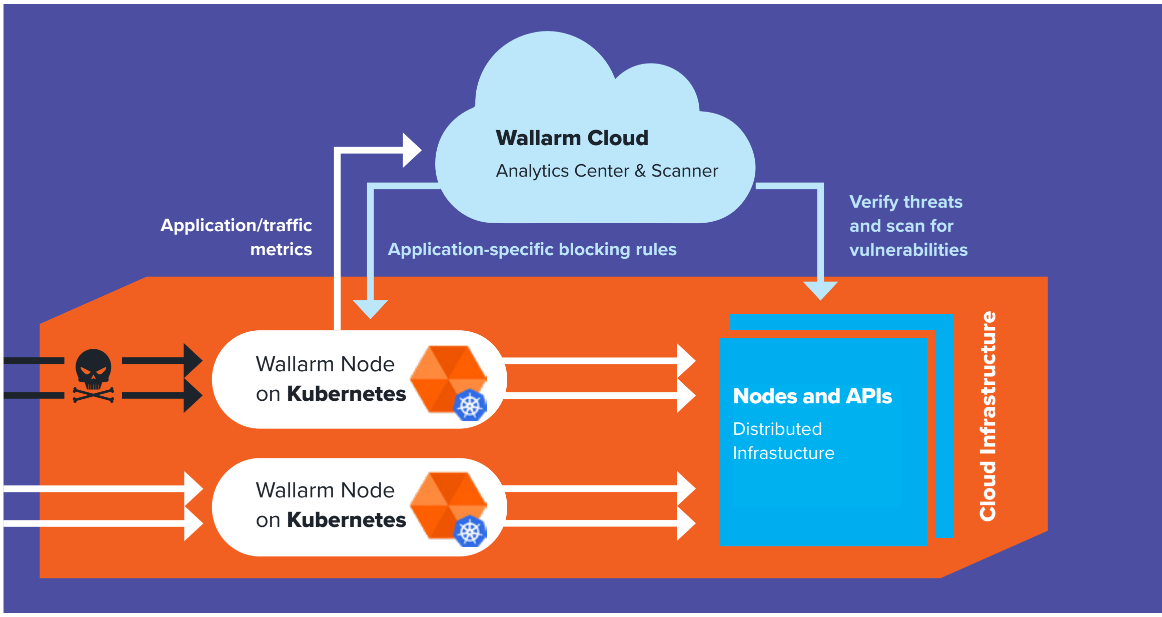
Adaptive application security

Built for cloud-native enterprise applications

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

Wallarm on Ingress controller

Customers are assured that Wallarm Next Generation WAF enfoces security with minimum of overhead , has available support, and works with the standard Kubernetes distributions: https://kubernetes.io/.

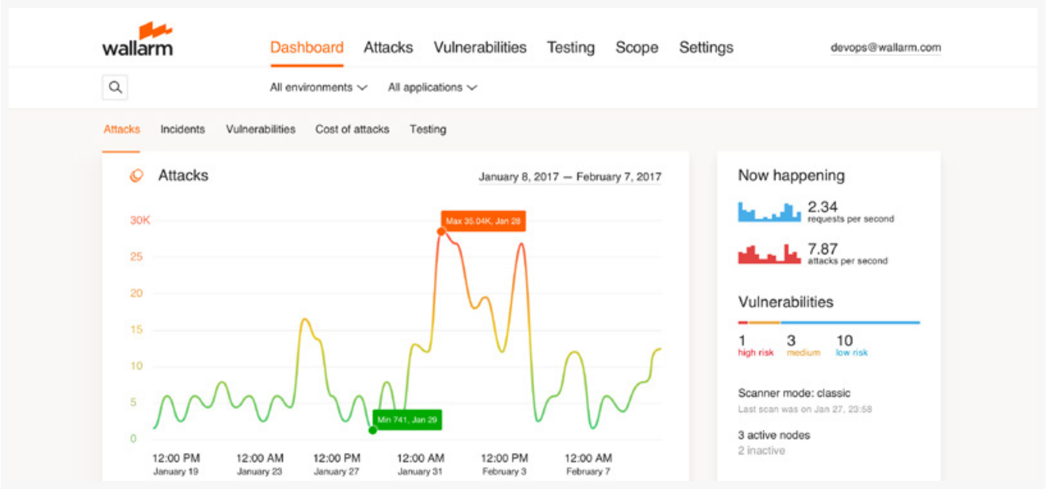

Wallarm Cloud
Analytics Center & Scanner
Application/traffic metrics
Application-specific blocking rules
Verify threats and scan for vulnerabilities
Wallarm Node on Kubernetes
Wallarm Node on Kubernetes
Nodes and APIs
Distributed Infrastucture
Cloud Infrastructure

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.

Wallarm is addressing quite a challenging problem of web application security in continous 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.



Now happening

2.34 requests per second

7.87 attacks per second

Vulnerabilities

1 high risk 3 medium 10 low risk

Scanner mode: classic

Last scan was on Jan 27, 23:58

3 active nodes

2 inactive

SIGN UP FOR A FREE TRIAL!

request@wallarm.com **(415) 940-7077**