Application Security Platform Powered by AI

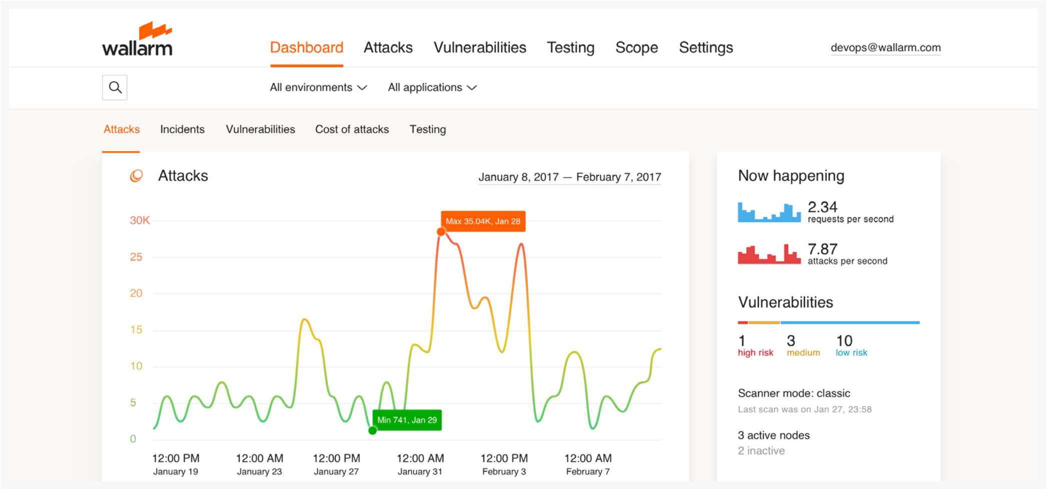
Wallarm is an application security platform which combines Active Threat Verification engine and a DevOps friendly NG-WAF. It applies machine learning to traffic to adaptively generate security rules and verifies the impact of malicious payloads in real time. The platform is uniquely suited for the modern application stack and CI/CD pipelines.

wallarm.com

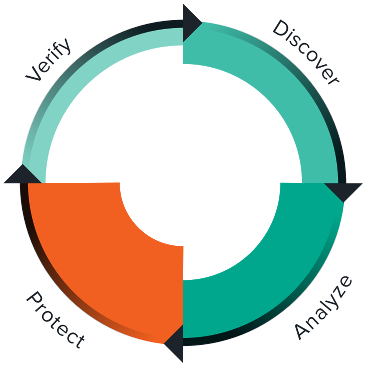
Adaptive application security

Key Benefits

- Adapts security rules with AI as application evolves
- Actively verifies threats to minimize manual analysis
- Protects from OWASP Top 10 and 0-day attacks
- Protects against bots and API abuse
- Lowers false-positives by customizing security rules to the application logic
- Integrates with existing infrastructure and CI/CD pipelines



Continuous Intelligent Security



In **Discover** phase Wallarm scans the entire network perimeter to identify exposed assets.

In **Analyze** phase Wallarm inspects incoming HTTP requests and applications responses. The platform continuously updates application specific security rules to keep pace with CI/CD pipelines.

This helps SecOps and DevOps teams meet best practices and **Protect** applications without a need for labor-intensive manual security rule administration.

Deep Packet Inspection capability coupled with advanced decoding parsers enables Wallarm to support nested protocols and modern APIs including support for JSON, AJAX, HTTP/2, WebSockets, Base64, ASP.NET VIEWSTATE, PHP serialization and their encapsulated variants like XML inside of the JSON and other similar protocols.

The platform is agnostic of the application stack: Wallarm protects applications written in Ruby, Node.js, PHP, .NET or other languages.

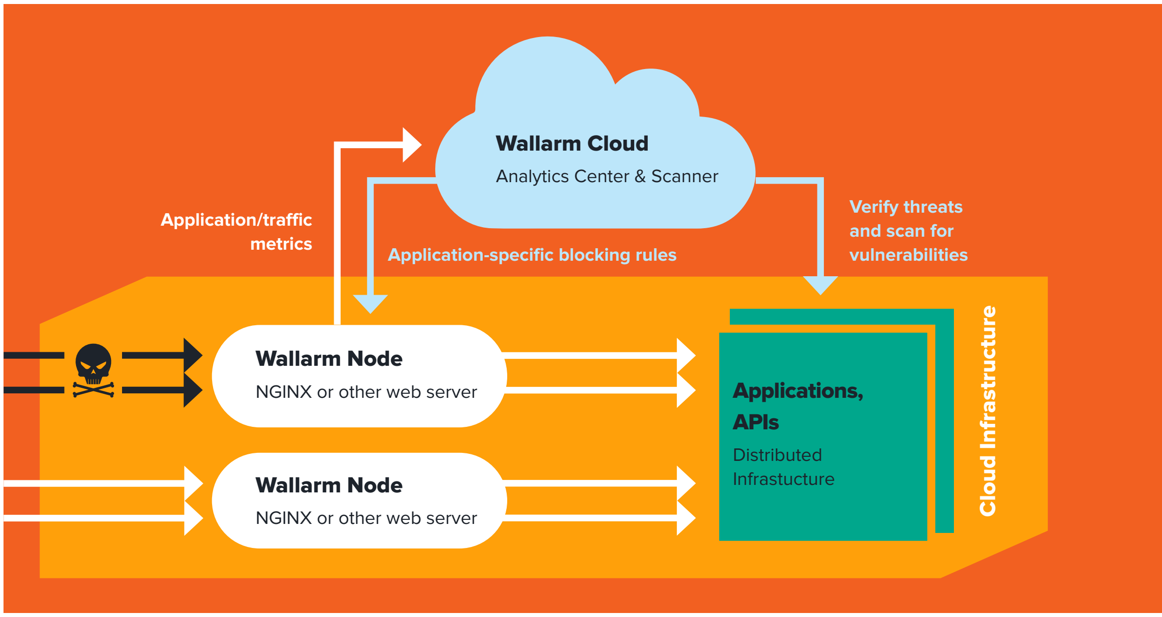
Verify phase combines similar malicious requests together into attacks based on target and payload. Then the active scanner (DAST) replays sanitized version of these attacks against the application, which reduces team efforts by only alerting on verified security vulnerabilities.

wallarm

wallarm.com

Adaptive application security

«With active threat detection, we are no longer over-swamped with tons of useless events. As all the payloads from malicious requests are analyzed with a cloud scanner, we don't need to do this manually. Adaptive security rules allowed us to use WAF in blocking mode which was almost impossible previously». Mike Chadwick, VP of Engineering of Acronis


Wallarm Cloud
Analytics Center & Scanner
Application/traffic metrics
Application-specific blocking rules
Verify threats and scan for vulnerabilities
Wallarm Node
NGINX or other web server
Wallarm Node
NGINX or other web server
Applications, APIs
Distributed Infrastucture
Cloud Infrastructure

Wallarm hybrid architecture makes it 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.

Supported platforms

Traffic filtering is performed by Wallarm's filtering nodes that can be installed on the application server, as a reverse proxy or within the load balancer infrastructure. It supports variety of platforms:

- Public clouds
  - AWS
  - Google
  - Azure
- As a module
  - NGINX
  - Kong API Gateway
- As a container or VM
  - Docker
  - VMware VM
- Linux package
  - RHEL/CentOS
  - Debian
  - Ubuntu

Wallarm Editions	Professional	Enterprise	Wallarm Plus
Centralized management	✓	✓	✓
Monitoring and blocking	✓	✓	✓
Adaptive security rules	✓	✓	✓
Bot protection / Behavioral Analysis	✓	✓	✓
Active Threat Verification / DAST		✓ 1K attacks / d	✓ 1K attacks /d
Event Storage	3 mo	12 mo / 10M	12 mo / 10M
Perimeter Discovery / Vulnerability Scanning	/28 subnet	/24 subnet	/24 subnet
Additional non-production instance	available	available	available
Built in NGINX Plus	available	available	✓

SIGN UP FOR A FREE TRIAL!

trial@wallarm.com

(415) 940-7077