Integrated web security solution built for NGINX Plus

130M

websites use NGINX to deliver traffic to applications

35%

of data breaches in 2014 targeted vulnerabilities in web applications

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.

Secure Application Delivery with NGINX+ and Wallarm

Get enterprise-grade load balancer and next generation WAF in one scalable software instance

Powering 1 in 3 of the world's busiest sites, NGINX is the secret heart of the modern web. It helps to deliver sites and apps with performance, reliability, and scale. With no additional software to install one can enhance application security by a painless switching to a special version of NGINX+ and Wallarm.

The demands of the modern web have inspired a new suite of tools and technologies that are overwhelmingly open source, cloud-friendly, and place a premium on adaptability, performance, and scalability. Of all of these new tools, none is more fundamental to the architecture of the modern web than NGINX.

From now on, in any infrastructure with NGINX used for application delivery and load balancing there is one small step away from getting web assets protected against possible data breaches and hacker attacks. You only need to switch from basic NGINX to a special build with Wallarm embedded.

With no changes to the traffic flow as well as in the way of deploying and scaling of NGINX instances, a complete security protection is added. It's a perfect choice for continuous integration environments since Wallarm was made with keeping in mind protection of frequently updated apps. This is why this approach is highly appreciated by DevOps, developers and security engineers.

Fast. Scalable. Efficient

wallarm

NGINX+

Why switch to Wallarm from another WAF?

- get rid of false-positives that block legitimate users with any change in the application
- discover vulnerabilities in each code deploy
- scale horizontally using NGINX-powered filtering instances

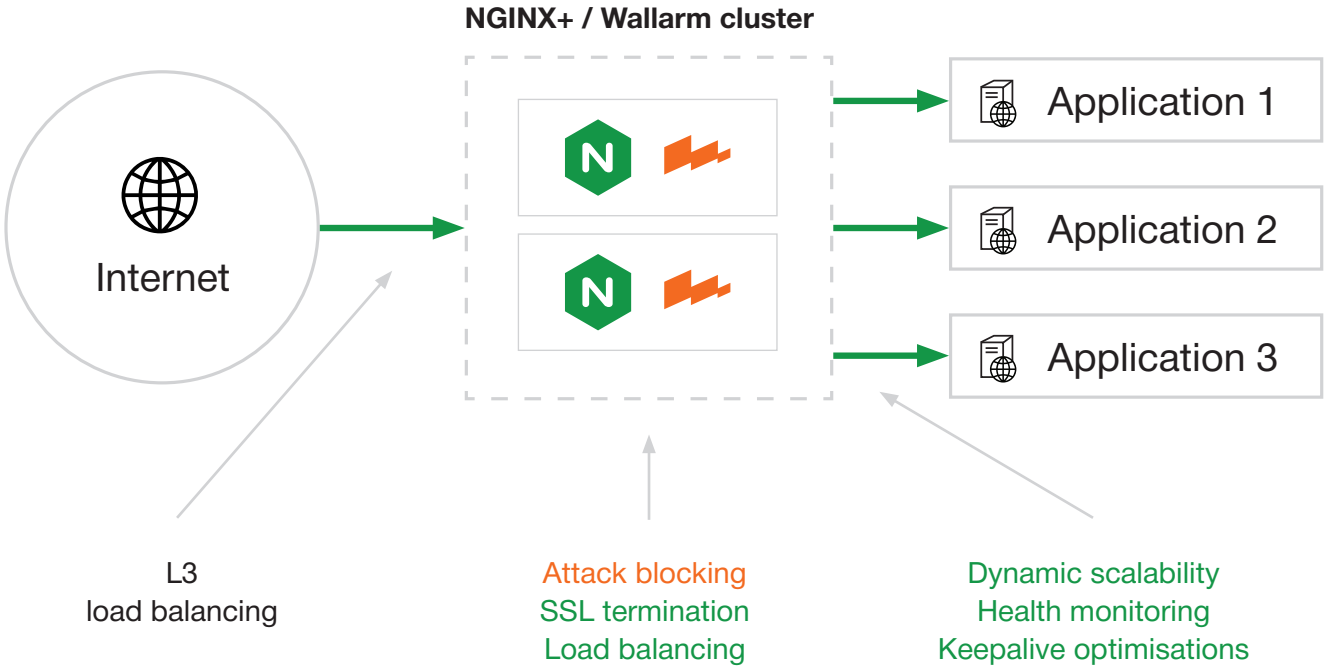
Enjoy NGINX Plus features

- HTTP and TCP load balancing
- session persistence
- health checks
- advanced monitoring

Wallarm/NGINX+ packages are available for CentOS, Ubuntu, Debian Linux and ready to deploy in cloud

Wallarm uses hybrid approach when traffic is filtered inside customer's infrastructure whereas advanced analytics is done in the cloud

It leverages the power of big data and machine learning to craft blocking rules specifically for every application. As a result, Wallarm detects even the most sophisticated attacks while keeping a false-positive rate extremely low. Traffic is filtered in real-time by scalable, efficient and easy to deploy Wallarm nodes based on NGINX+. This is why customers get advanced security with all the impressive features of NGINX/NGINX+.



For more information on integrated web security solution built for NGINX Plus please visit **www.wallarm.com/nginx-plus-wallarm**

wallarm

Wallarm is next generation web security solution designed to protect online businesses from application-level attacks

www.wallarm.com
+1 415-940-7077
@wallarm