

Wargaming and Wallarm WAF: Appsec statistics that make the difference

Wargaming is an award-winning online game developer and publisher headquartered in Nicosia, Cyprus. Operating since 1998, Wargaming has grown to become one of the leaders in the gaming industry with 5,500 employees and offices spread all over the world. Over 200 million players enjoy Wargaming's titles across all major gaming platforms. Their flagship products include the massively popular free-to-play hit World of Tanks and the strategic naval action game World of Warships.



20 years of game development experience



15+ released titles gaining millions of fans worldwide



5500 employees over 18 global offices



200M over last 10 years – largest global gaming audience



Datacenters by **G-Core**

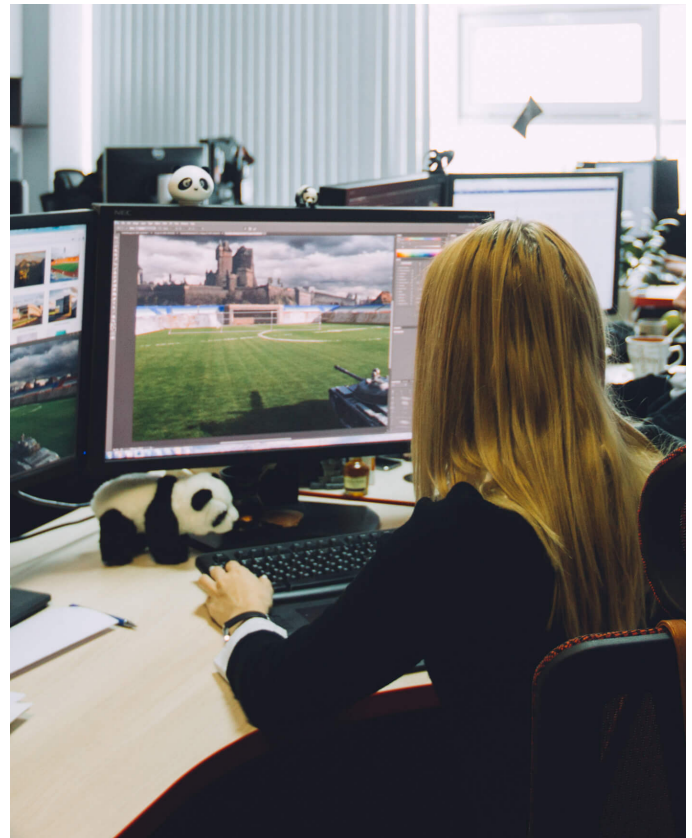
Why Wallarm WAF?

In 2015 Wargaming participated in Wallarm WAF Beta testing. When the testing period was finished, Wargaming became one of the first enterprise commercial clients of Wallarm.

After some years of using the platform, Wargaming conducted a competitive comparison. The result

was that appliance-based WAF solutions were less expensive, but not suitable for Wargaming due to the business model and infrastructure construction with more than 50 regions of operation.

On the other hand, there was no convenient way to change the WAF service partner, since all deploys, plants were tightly connected to NGINX. Moreover, for the amount of traffic Wargaming resources get – other service partners, for example, Cloudflare, cost incomparably more than Wallarm WAF. Nevertheless, competitive analysis of WAF market is conducted each year.



What is under Wallarm WAF protection?

First of all, due to GDPR, loss of personal data of the customers and gamers may cost the company a lot. So, almost every node with traffic is protected by Wallarm. Wargaming has about 3000 nodes with web-applications. Wallarm WAF protects websites, APIs, and applications – big gaming services, catalogs, shops. In different services, and teams, multiple APIs and different standards are used.

Deployment

Wargaming uses a hybrid mode of WAF protection: some of the nodes operate in blocking mode, others only in monitoring mode.

Most useful features of Wallarm WAF for Wargaming



Statistics in dashboards

Wallarm gives stat on the aggressiveness of the internet. These statistics are used for internal forecasts and help predict web-associated activities, highs, and downs to distribute resources in a more efficient way.



Scanner

Immediate internal scanning of such a number of resources is not a trivial task. Furthermore, a quick analysis of this load of raw data is almost impossible. Wallarm analyses the load of data and indicates only the vulnerabilities that need attention. Active scanner informs about, for example, the expiration of PHPs and alerts about open ports. Detected vulnerabilities are being fixed. This is a kind of insurance for Wargaming infrastructure.



HOW IT WORKS

We scan the infrastructure by our own Security team monthly to see issues that were missed by an automated scanner. Nevertheless, there've been reverse cases. Once Wallarm detected a vulnerability of an open Registry earlier than our team did it.

– **Ivan Agarkov**, Services Infrastructure Security Director, Wargaming

