Nemesida WAF

powered by Nemesida AI

A modern on-prem web application security platform that protects all forms web traffic, services and APIs against compromise attacks, L7 DDoS, account takeover, malicious bots and other OWASP TOP 10 threats.

nemesida-waf.com

High accuracy. Deep analysis. On-Premise.

- Nemesida WAF uses classical machine learning algorithms capable of detecting attacks with an accuracy of 99.98%
- Does not require constant maintenance and creation of exception rules
- Uses a variety of mechanisms for normalization of queries and their deep analysis (Deep Inspection)
- It is delivered as an installation distribution for Linux / FreeBSD, a virtual machine image or a Docker image
- It performs local training and recognition, does not require sending traffic to the cloud
- It scales perfectly, has no restrictions on the number of virtual hosts and traffic, and auxiliary components in the form of a vulnerability scanner and a virtual patching system will provide a high level of security
- Blocks various types of attacks: SQLi, RCE, XXE, OS Command Injection, XSS, CSRF, Path Traversal, Open Redirect, Web Shell upload & access, HTTP Response Splitting, Information leakage (backup access etc.), RFI/LFI, DDoS L7, password matching, flood and other parasitic traffic, as well as protects your API (OpenAPI/Swagger)

Nemesida WAF

IT'S CHEAPER TO PREVENT AN ATTACK THAN RECOVER FROM A DAMAGE

Website:
nemesida-waf.com

Email:
info@nemesida-waf.com