Medianova Cloud WAF

"Security at the Edge"

OWASP Core Rule Set and Managed Rules

Protect your web assets against common attack types such as;

- SQL Injection
- Cross-Site Scripting (XSS)
- Local / Remote File Inclusion
- PHP Code Injection
- Java Code Injection
- Shellshock
- Unix / Windows Shell Injection, and more

Customized Rules

Create custom rules for tailored defense and prevention of false-positives using;

- User agent
- Request protocol
- Request URI
- Client IP
- Referer
- Request method, and more

Continuous Updates on Rulesets

Maintain effective protection against emerging attacks and vulnerabilities with;

- Ongoing updates, and
- Access to the most recent threat intelligence

Monitoring-only WAF Operation Mode

Enhance your security posture without disrupting your workflow with "Monitoring-only" mode. Choose your WAF operation mode based on your security requirements.

- Monitoring-only
- On
- Off

Geo-blocking

Block requests from specific geographies in case of an attack.

Rich Analytics

Monitor the security of your website and take the required steps to strengthen it with;

- Detailed Threat Statistics
- Top Client IPs of Attacks
- Top Request URIs of Attacks
- Activity Logs
- Top User Agents of Attacks

High Protection Capacity

Secure your web properties with a protection capacity proportional to Medianova's global edge network (50+ data centers).

IP Blacklisting and Whitelisting

Block requests from specific attacking IP addresses with IP blacklisting.

Integration with Other Medianova Services

- Dynamic CDN (Aksela)
- Anycast DNS
- Load balancing

Flexibility of Deployment

Use our cloud-based WAF solution standalone or complementary to other on-prem WAF solutions for extended security.

Seamless and Agile Onboarding Process

Activate your Cloud WAF instantly and get in touch with our team any time through private Slack channels.

MEDIANOVA

www.medianova.com