

Medianova DDoS Protection



Origin Shield

Introduce an extra layer of security for your origin and limit its exposure to possible DDoS attacks with our Secure Cloud.



IP Blacklisting and Whitelisting

Block requests from specific IP addresses that attempt to attack, with IP blacklisting.



IP Protection

Mitigate the likelihood of DDoS threats preemptively by concealing your origin IP address before an attack can be initiated.



Rate Limiting

Block suspicious requests that exceed predefined thresholds within a time frame.



Always-on DDoS Protection

Protect your web assets against common attack types such as;

- DNS Query Floods
- SlowLoris
- HTTPS GET
- HTTPS POST, and more

Minimize downtime with our always-on DDoS mitigation, without the need for an extra activation.



High Protection Capacity

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



Integration with Other Medianova Services

- Web Application Firewall
- Load Balancing



Anycast DNS Infrastructure

Mitigate DDoS attacks with our Anycast DNS network that distributes thousands of requests across multiple servers that might overwhelm a single server.



Geo-blocking

Prevent malicious requests from specific geographies in case of an attack.



Flexibility of Deployment

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