RedgeGuardian

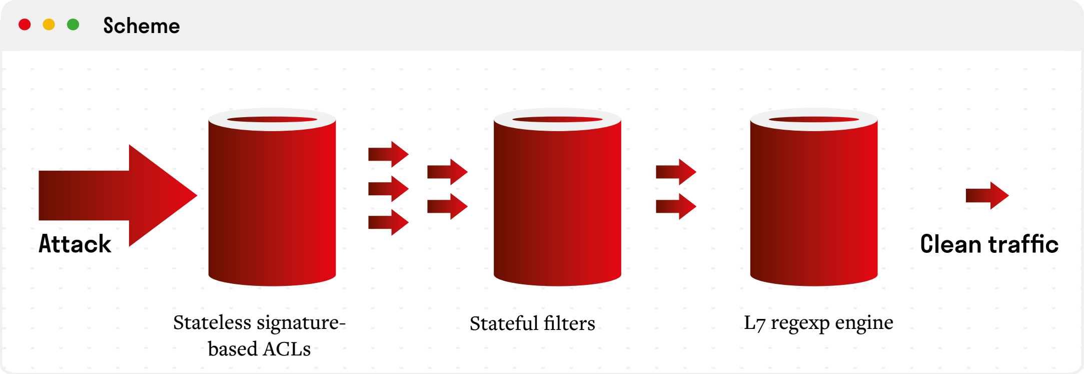
# DDOS MITIGATION CLOUD

A BGP anycast global scrubbing service. Gain ultimate protection for servers, infrastructure, and digital content.

## What is Redge Guardian?

Redge Guardian is a carrier-grade, software-defined DDoS mitigation platform, ready to handle fast-moving, terabit scale attacks, including IoT-based threats. Redge Guardian provides the first layer of network security and allows inspecting and filtering of 100M+ pps on a single node thanks to its unique data plane architecture. To date, such a performance level was only achievable on FPGA and ASIC-based platforms.

Redge Guardian allows defining of the traffic inspection pipeline comprising signature-based stateless filters, stateful filters, and a high-performance L7 regex module in order to fully protect the infrastructure against known and emerging threats. Such an approach yields the highest mitigation accuracy with the shortest activation time and does not affect legitimate user traffic.



The Redge Guardian Cloud traffic inspection pipeline comprises signature-based stateless filters, stateful filters and a high-performance L7 regex engine to fully protect the infrastructure against known and emerging threats.

## Key benefits

### State-of-the-art protection

Redge Guardian protects from the widest range of known and zero-day attacks, including reflected NTP/SSDP/memcached floods, DNS attacks, TCP floods and more. Redge Guardian starts mitigation within milliseconds and does not impact legitimate user traffic.

### Software-driven flexibility

Redge Guardian does not require custom hardware platforms - 100G+ performance can be achieved on a commodity x86 server. The deployment scenarios include inline, out-of-path or scrubbing center. Multitenancy support gives carriers an opportunity to monetize DDoS protection.

### Fully managed solution

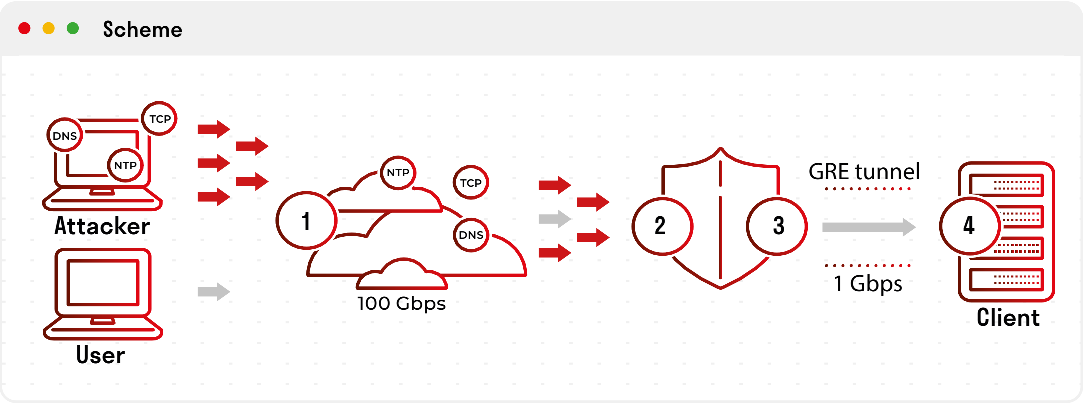
On-premises deployments are extensively supported by a dedicated Security Operations Team, which covers management, signature upgrades, fine-tuning and emergency response in case of zero-day attacks.

## Mitigated attacks

- ✓ Chargen reflected response flood
- ✓ DNS reflected response flood
- ✓ Echo reflected response flood
- ✓ IKE PAYLOAD-MALFORMED response flood
- ✓ IPMI/RMCP reflected response flood
- ✓ LDAP query flood
- ✓ LDAP reflected response flood
- ✓ Memcached reflected reponse flood
- ✓ MSSQL reflected response flood
- ✓ NetBIOS reflected response flood
- ✓ NTP reflected response flood
- ✓ QOTD reflected response flood
- ✓ RIP reflected response flood
- ✓ RPC Portmap reflected response flood
- ✓ Sentinel reflected response flood
- ✓ SNMP reflected response flood

- ✓ SSDP reflected response flood
- ✓ Steam query flood
- ✓ Steam reflected response flood
- ✓ TFTP reflected response flood
- ✓ UDP fragment flood
- ✓ UDP invalid packets
- ✓ TCP SYN/ACK/RST/ACK flood
- ✓ TCP fragment flood
- ✓ TCP invalid packets
- ✓ ICMP PING flood
- ✓ ICMP obsolete/legacy packets
- ✓ ICMP invalid packets (bad quote)
- ✓ ICMP fragment flood
- ✓ GRE invalid packets (destination address validation)
- ✓ IP invalid packets (checksum, fragment offset, packet length, spoofed source)

## How Redge Guardian works



1 Service activation advertises your prefix in BGP and redirects traffic to the nearest Redge Guardian scrubbing center.

2 In the scrubbing center, the attack is filtered according to the rules configured for the client.

3 The filtered traffic is delivered to the client via direct peering at the IXP or via GRE tunnel.

4 The Redge Guardian platform does not interfere with outgoing traffic from the client network.

## Anyone can be a target of a DDoS attack

Distributed Denial of Service (DDoS) attacks are on the rise, causing a huge threat to businesses and organizations that provide online services. Recent IoT vulnerabilities and the rise of new botnets have allowed attackers to enter the terabit-scale era, threatening even the largest businesses. No doubt, anyone can be a target.

## You can mitigate these attacks in a cost-effective way

Redge Guardian allows multi-terabit scalability, providing you with comprehensive, premium protection from DDoS attacks.
It is your best insurance policy and is individually preconfigurable and tailored to your needs.

## Features

### Deployment / management

| | |
|---|---|
| **Automated activation** | Support for sFlow v5, NetFlow v5/v9/IPFIX<br>Configurable activation thresholds |
| **Manual / external activation** | HTTP API call<br>SYSLOG messages<br>Management panel |
| **Minimal protected subnet size** | /24 (IPv4), /48 (IPv6) |

### Clean traffic delivery

| | |
|---|---|
| GRE tunnel | Optional key<br>Fragmentation before or after encapsulation |
| Direct peering | Available in Warsaw (Equinix WA1), Prague (CE Colo) and London (Equinix LD8)<br>n x 10G or n x 100G ports |

## They have trusted us:

NASK
CloudFerro
R22
dhosting.pl
e-point
efigence

## Get in Touch

redgeguardian.com

info@redge.com