Telia Carrier

DDoS MITIGATION

PROTECT YOUR INFRASTRUCTURE FROM INTERNET-SCALE DDOS ATTACKS

DDoS mitigation directly on the world's best-connected Internet backbone, ensuring scalable and continuous host-level protection against DDoS attacks.

ATTACKS ON YOUR INTERNET-CONNECTED SERVICES

Distributed denial-of-service (DDoS) attacks aim to disrupt organizations by targeting their websites and servers. Using botnets, attackers overwhelm organizations with fake traffic, making websites and services unavailable to legitimate users. The results can be both financially and reputationally damaging for organizations.

SOPHISTICATED ATTACKS ON THE RISE

DDoS attacks are growing in frequency and sophistication - and often described as one of the Internet's most powerful and dangerous weapons. Attackers continuously look for ways to outsmart evolving mitigation techniques with more distributed, complex, and powerful attacks.

MITIGATION TECHNIQUES THAT CONTINUALLY ADAPT

Telia Carrier uses carrier-grade mitigation technology that intelligently and automatically adapts to variations within every attack, but also the ever-changing threat landscape across the global Internet.

The mitigation methodology we use is straightforward yet effective. Customer traffic passes through our DDoS mitigation platform for real-time analysis to selectively block malicious traffic, while legitimate traffic is free to pass through.

FINE-GRAINED TRAFFIC CONTROL ON THE BACKBONE

We use BGP flowspec as a granular mechanism that enhances our existing DDoS mitigation technologies. BGP flowspec enables the faster exchange of information with Internet routers and our DDoS mitigation platform.

24/7 PROTECTION

Our DDoS mitigation service provides an ideal layer of protection by continually monitoring all potential threats across our backbone infrastructure - anything that could jeopardize service availability and business continuity for us and our customers.

- Constantly updated threat intelligence backed by industry leading vendors.
- Dedicated SOC staff working to protect your network (and ours).

CUSTOMER TESTIMONIAL

"Telia Carrier's network security team confidently took control of the DDoS attack and immediately deployed a solution to restore our services. Through first-hand experience, we understand more than ever how serious a DDoS attack can be, which is why we put our trust in Telia Carrier to mitigate future attacks".

- CEO, leading US Wireless Internet Service Provider

BENEFITS IN BRIEF

SCALABILITY

We provide a high-capacity solution throughout our global IP backbone that can be scaled to add more Managed Objects (MOs) and mitigation capacity supporting our customers growing protection needs.

PRECISION

Our service applies surgical mitigation techniques to mitigate attacks automatically. Malicious traffic is already dropped within our backbone before it reaches our customers' Internet connections, allowing our legitime traffic to pass.

BACKBONE STRENGTH

We have deployed advanced mitigation techniques with BGP flowspec, enabling more granular control of traffic on our global backbone, which connects 65% of global Internet routes. As a result, we have a more dynamic way of protecting our backbone and, consequently, our customers against large-scale volumetric DDoS attacks.

Telia Carrier

DDoS MITIGATION

TECHNICAL HIGHLIGHTS

Defence against the largest attacks

- With the sheer scale of AS1299 and edge capacity exceeding 280Tb
- Use of AS1299 as a scrubber with Flowspec
- 5 geographically spread scrubbing centres

Attacks are stopped before they overload your Internet connection. Having attack traffic cleaned by your upstream means you are not limited by the capacity of your Internet connection.
Fast time to mitigate - using the power of AS1299's global backbone, we are able to redirect traffic towards the nearest scrubbing location in record time - and less than 3 minutes.
Tailor your service - we offer you the ability to deviate from standard protection thresholds and mitigation settings - you can opt for our fully automatic service (recommended) or decide yourself whether you want us to mitigate or not.

MULTI-HOMED DDOS SERVICE

With the multi-homed DDoS service, we leverage best-in-class detection and mitigation system. The service works like the base-level service with a couple of additional functions:

- Netflow (or sFlow) data from customer edge routers is sent to our detection system allowing us to see attack traffic even if the data does not flow through AS1299
- When an attack is detected, we not only create an internal redirect, but also issue more specific eBGP announcements to the Internet to bring that traffic on to AS1299

Once successfully mitigated, all BGP announcements are withdrawn and traffic returns to normal. This is done in a fully automated way, with no manual intervention needed.

USE CASES

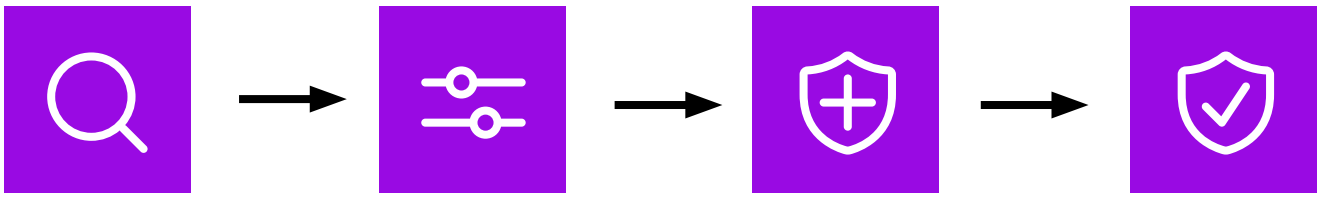
BUSINESS CONTINUITY

DDoS has an immediate and profound impact on businesses. We have designed our DDoS mitigation service to scale across the global Internet for each tier. We can absorb highly distributed attacks and allow data centers, servers and Internet connections to operate normally even when under attack.

COST-EFFICIENT SECURITY

We designed our pricing model to adapt to the risk profile of each customer, making it more economical than in-house edge solutions that can cause additional bottlenecks during DDoS attacks.

HOW THE DDOS SERVICE WORKS - BASICS



DETECTION
Our detection system monitors traffic flows and looks for suspicious traffic.

DIVERSION
When an attack is detected towards one of our protected customer prefixes, we steer that traffic to our nearest scrubbing locations.

FILTERING
Our scrubbers then use advanced filtering to drop all malicious traffic and let legitimate traffic continue towards its intended destination.

MITIGATION
Once the attack has stopped, our system withdraws the redirections and all traffic flows return to normal.

TYPICAL ATTACK TYPES :
Reflection Amplification Flood Attacks (TCP, UDP, ICMP, DNS, mDNS, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service); Fragmentation Attacks (Teardrop, Targa3, Jolt2, Nestea); TCP Stack Attacks (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, other combinations of TCP Flags, slow TCP attacks); Application Attacks (HTTP GET/POST Floods, slow HTTP Attacks, SIP Invite Floods, DNS Attacks, HTTPS Protocol Attacks); SSL/TLS Attacks (Malformed SSL Floods, SSL Renegotiation, SSL Session Floods); DNS Cache Poisoning; Vulnerability Attacks; Resource Exhaustion Attacks (Slowloris, Pyloris, LOIC, etc.); Flash Crowd Protection; Attacks on Gaming Protocols.