Telia Carrier

DDoS MITIGATION

DEFEND 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 growing 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 accurately block attack 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.

ALWAYS-ON MITIGATION

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

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 to support 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, passing through only legitimate traffic.

BACKBONE STRENGTH

We have deployed advanced mitigation techniques with BGP flowspec, providing more granular control to handle traffic on our global backbone, which connects 60% 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

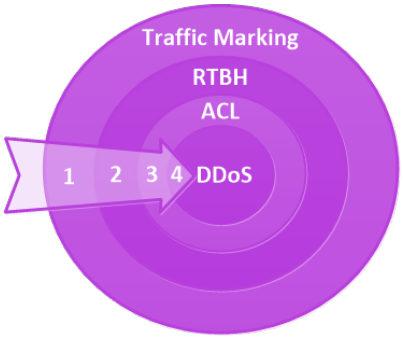
TECHNICAL HIGHLIGHTS

We provide mitigation against evolving attack vectors:

- Volumetric
- Protocol
- Application

We apply a Four-Tier Mitigation Model to offer complete protection from DDoS attacks.

1. Tier-1 Malicious Ingress Traffic Marking and Policing (Infrastructure protection)
2. Tier-2 RTBH Technique
3. Tier-3 ACL Port Level Service
4. Tier-4 DDoS Protection



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 continue to operate 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 in DDoS attacks.

HOW THE SERVICE WORKS