DDOS MITIGATION SERVICES

Northland COMMUNICATIONS

Now offering! DDoS Mitigation services to extend security and protection to our dedicated Internet customers that will offset distributed denial-of-service (DDoS) attacks.

What is DDoS Mitigation?

DDoS mitigation is the process of successfully protecting a target from a distributed denial-of service attack. A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. A DDoS attack on a company's website, web application, APIs, network, or data center infrastructure can cause downtime and prevent legitimate users from buying products, using a service, getting information, or any other access.

Firewall vs. DDoS

Firewall cannot do the job of protecting your network alone. Cybersecurity threat protection strategy requires a DDoS solution that detects and blocks DDoS traffic—in front of the firewall—within Northland's core network, before we even send the traffic to you. DDoS protection complements a firewall, and allows clean, legitimate traffic to flow through normally, without any impediment.

DDoS Attacks are on the Rise

DDoS Mitigation offers a highly-scalable attack mitigation service that helps you tackle today's sophisticated and high volume DDoS attacks. It works across your enterprise environment to alleviate the burden on your network and perimeter systems, and helps maintain continued availability to your customers.

KEY FACTS + BENEFITS

Uptime: This service helps keep customers connected with a 99.999% uptime by its live monitoring systems to alert potential attacks.

50%

of DDoS attacks lead to significant service disruption.

Comprehensive visibility: Leverages data analytics to report and alert for clear, actionable intelligence on the DDoS attack activity happening across the network.

Monitored traffic: All Internet traffic is monitored due to Northland's network design versus with competitors', data sampling is used as a detection.

76%

of DDoS attacks are made with less than 1GB of data.

Reduced operating costs: Automated DDoS response significantly decreases human intervention and false positives for reduced operational costs.

Real time mitigation:
Service will mitigate and alter traffic flow in real time versus larger network data sampling where the attack could be missed.