DDoS Mitigation Service

Defend against attacks to help keep your data and network secure

Distributed Denial of Service (DDoS) attacks are among the most common types of cyberattacks.

Bad actors take advantage of the capacity limits of network and server resources — such as the infrastructure enabling an organization's website — and overload them. DDoS attacks send malformed, high-volume requests to your application, server, and network resources, aiming to exceed its capacity to handle the traffic, prevent proper function, and take it offline for legitimate users.

DDoS attacks can result in potential revenue losses if there is downtime. They also can lead to reputational damage due to customer service issues and remediation.

In the first half of 2023, NETSCOUT's DDoS Threat Intelligence Report observed a staggering total of nearly eight million DDoS attacks, a 31% increase year-over-year. This represents a remarkable 44,000 DDoS attacks per day.

44K
DDoS Attacks per day

Source: NETSCOUT DDoS Threat Intelligence Report

Other industry sources have reported the following:

~13M
DDoS attacks worldwide in 2022[1]

10X
Increase in attack frequency since 2005[1]

$218K
The average cost of a DDoS attack in the U.S.[2]

Help Safeguard Your Digital Assets

Businesses need robust DDoS mitigation strategies for their network. Comcast Business DDoS Mitigation Service is a comprehensive managed service designed to help safeguard your online infrastructure. Whether you are a medium-sized business, school, or large enterprise, Comcast Business DDoS Mitigation Service is scalable and tailored to meet your needs with customizable detection and mitigation templates that help protect against attacks of all sizes and types.

1. 2022 Netscout DDoS Threat Intelligence Report
2. Corero Whitepaper - The Need for Always-On, Real-Time DDoS Security Solutions

COMCAST BUSINESS

Proactive Detection and Response

At the heart of Comcast Business DDoS Mitigation Service is an advanced monitoring system that continually analyzes network flows to detect and proactively respond to DDoS threats. In the event of an attack, our service automatically scrubs malicious traffic. Comcast Business does not redirect traffic to the cloud or use Generic Routing Encapsulation (GRE) tunnels that may limit throughput. This technique helps preserve bandwidth capacity and avoid latency issues.

Geo Blocking and Allow List features provide customers with precise access controls. Plus, our advanced detection algorithms help minimize false positives. Threshold adjustments ensure that legitimate traffic remains unblocked during a DDoS attack.

Enhanced Analytics Supports Informed Decision Making

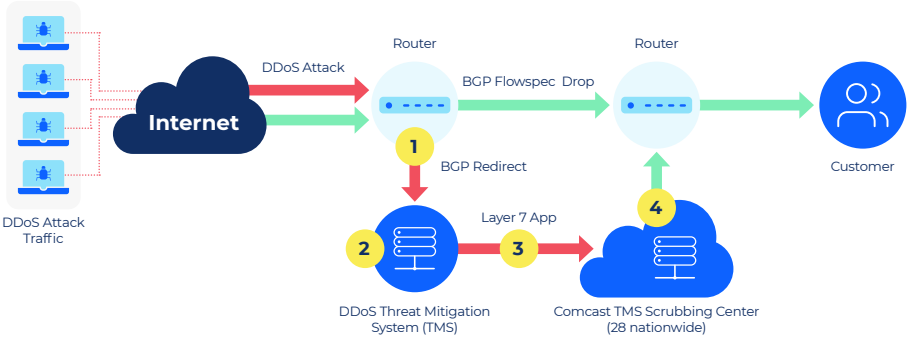
Comcast Business DDoS Mitigation Service goes beyond detection and mitigation by providing insights and analysis for each attack, including reports for customers. Customers can also track attacks by severity, type, volume and mitigation details, plus obtain historical data with additional insights into threat activity.

Robust Coverage and Support Lets You Focus on Your Business

Comcast Business maintains a network of high-capacity, geographically dispersed, and redundant scrubbing centers co-located with our nationwide network infrastructure. DDoS Mitigation Service helps protect systems connected over Comcast or third-party circuits regardless of the size, duration or geographic origin of DDoS attacks.

Our team of cybersecurity experts – with extensive experience mitigating DDoS attacks – is available 24/7 to provide customer support. We also empower customers with self-service configuration, reporting, and alert management.

How it Works



1 DETECT	2 DROP	3 DIVERT	4 DELIVER
• Flow monitoring & BGP FlowSpec enabled on edge routers • Anycast advertises nearest TMS appliance • TMS monitors flow monitoring session data • TMS detects attack in near real-time	• Proactive alert sent to customer • BGP FlowSpec enabled on router • ~80% of DDoS attacks are Layer 3-4 • FlowSpec drops Layer 3-4 Network Traffic at Network Edge • Zero latency impact	• If TMS detects DDoS attack against Layer 7 app services: • Traffic forwarded to TMS Scrubber using BGP redirect • TMS Scrubber cleans malicious DDoS traffic	• Cleaned traffic delivered to customer • BGP redirect to Comcast EDI circuit

Why Choose Comcast Business DDoS Mitigation Service

Advanced Solution

- Proactive threat monitoring
- Rapid attack mitigation
- Allows legitimate traffic during a security event
- Distributed DDoS scrubbing centers nationwide

Enhanced Analytics

- In-depth attack analytics and reporting
  - Severity
  - Type
  - Volume
  - Mitigation details
- Historical insights data

Flexible

- Scalable, customized security
- Allow Lists and Geo Blocking for fine-tuned access control
- User-friendly – optional self-service configuration
- Email or SMS alert notifications
- Works with both Comcast and non-Comcast circuits

Service & Expertise

- 24/7 customer support
- Backed by team of cybersecurity experts

COMCAST BUSINESS

Support For All Circuit Types

	DDoS Mitigation Service	
Capabilities & Requirements	Comcast Circuits	Non-Comcast Circuits
Automatic or optional on-demand (monitor only) mitigation	●	◐ Automatic only
Helps protect Comcast Business EDI circuits	●	
Protects Non-Comcast DIA circuits		●
24/7 phone support and troubleshooting	●	●
MyAccount configurable SMS & Email Notifications	●	●
MyAccount self-service configuration	●	●
MyAccount logs, analytics & reporting	●	●
No additional equipment required	●	
Requires Border Gateway Protocol (BGP)		●

Get peace of mind with Comcast Business DDoS Mitigation Service.

Focus on your core business activities while we take care of your DDoS defense.

Detect, Respond, Recover

Comcast Business DDoS Mitigation Service aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and helps customers maintain business availability.

DDoS Mitigation Service

Detect:

- Scrutinizes network flows for abnormalities that can indicate an ongoing attack
- Quickly detects and alerts on potential volumetric, state exhaustion, and application layer DDoS attacks

Respond:

- Email & SMS Alerting notifies customers of attack
- Allows valid traffic flows seamlessly while reducing false positives

Recover

- Real-time DDoS Mitigation for Layer 3, 4 and 7
- Only clean traffic returned to customer

COMCAST BUSINESS