Comcast Business DDoS Mitigation Service

Comcast Business Ethernet Dedicated Internet (EDI) is enabled with threat defense and mitigation functionality to respond to DDoS volumetric and flood attacks.

Comcast Business DDoS Mitigation is a subscription-based network service that proactively detects DDoS attack traffic, alerts the customer when an attack is under way, and initiates mitigation to thwart the attacks. Comcast Business DDoS Mitigation Service provides real-time detection of volumetric and flood attacks such as UDP Floods, Web Flood, and DNS Application Floods.

Comcast Security Operations works closely with the customer to provision the service based on customer and network information, preconfigure countermeasure options and run acceptance tests to enable effective mitigation before service activation. Comcast monitors the customer network traffic for a specified set of IP addresses to be protected. When a DDoS attack is identified, an alert is sent to the customer via email and/or SMS to notify them of the attack.

During the mitigation process, Comcast diverts the customer's traffic, including DDoS attack traffic directed at the customer servers, to scrubbing centers distributed across the U.S. to filter and remove malicious traffic matching specific attack vectors. Simultaneously, the clean legitimate traffic is forwarded to the customer's network and servers through the use of a secure tunnel. Comcast Business DDoS Mitigation enables continued uptime of the customer's Internet business services during a DDoS attack.

DDoS Mitigation Service

Comcast Business DDoS service is designed for customers' security sensitivities, attack frequency, and time period. Customers are mitigated 24x7x365 in the Comcast Business Security Operations Center.

Your Unlimited service subscription provides an unlimited number of mitigation incidents in a monthly billing cycle, with no incremental mitigation incident fees charged.

Comcast automatically initiates mitigation when DDoS attack traffic levels exceed pre-set thresholds of high severity rates and duration. No customer intervention is required. When DDoS attack traffic drops below the thresholds, mitigation terminates automatically. After mitigation is terminated, all traffic is directed back to the Internet connections via normal paths. This solution is best when the customer would like peace of mind knowing Comcast will automatically mitigate DDoS attacks as they happen.

DDoS Mitigation Service Level Agreement

For a customer adding Comcast Business DDoS Mitigation to a new EDI service, the service delivery interval will be the same as the EDI service delivery interval. For a customer with existing EDI service, Comcast will configure and activate the customer's DDoS Mitigation service within 14 business days of submitting the order.

Mitigation interval – With On-Demand mitigation, the mitigation interval is the elapsed time from when the customer authorizes Comcast Business to enable DDoS mitigation to when Comcast initiates mitigation steps against any volumetric or flood attack traffic. With Automatic mitigation, the mitigation interval is the elapsed time from when a high severity alert is generated to when Comcast initiates mitigation of volumetric or flood attack traffic.

Benefits to customers

- **Enterprise grade –** Comcast utilizes this same DDoS mitigation platform to protect its own 23+ million customers and 1+ million IP's today

- **Simplicity –** Comcast manages threat mitigation from the network with no additional premise equipment required

Service	Detection	Alerting	Mitigation option	SLA (for mitigation start)
Unlimited	Proactive network- based real-time detection of volumetric and flood attacks	Automatic alert notifications of DDoS attacks.	On-Demand	Within 15 minutes
			Automatic	Within 5 minutes

- **Accountability –** Having Comcast manage the Internet and DDoS solution end-to-end means greater accountability and compatibility

- **Proactive detection and alerting –** Warns of DDoS volumetric and flood attacks in real-time

- **Peace of mind –** Helps thwart DDoS attacks before they impact Internet access and business operations

Service delivery option	Service delivery interval	Remedy
Add DDoS to new EDI Service	At time of EDI service delivery	No credit
	More than 24 hours after EDI service delivery	50% of the set-up fee
Add DDoS to existing EDI Service	Less than or equal to 14 business days	No credit
	More than 14 business days	50% of the set-up fee

- **Business continuity –** Ensures uptime during a DDoS attack

Service	Protection option	Mitigation interval	Remedy
DDoS Mitigation	On-Demand	Less than or equal to 15 minutes from customer authorization	No credit
		Greater than 15 minutes from customer authorization	1/30 of DDoS MRC
	Automatic	Less than or equal to 5 minutes from discovery of attack traffic	No credit
		Greater than 5 minutes from discovery of attack traffic	1/30 of DDoS MRC

COMCAST BUSINESS. POWERING POSSIBILITIES™

For more information please contact your Comcast Business Account Manager
or visit business.comcast.com/ethernet/DDoS.

COMCAST BUSINESS