

DDoS Mitigation Service

Stop the largest DDoS attacks & protect your web applications everywhere.

What is a DDoS attack?

A distributed denial-of-service (DDoS) attack is a cyberattack in which a malicious agent tries to force a machine or network resource offline. By disrupting the services of a host connected to the internet, it makes this service unavailable to its intended users.

For a DDoS attack to be successful, the attacker needs to send more requests than the victim's server can handle. There are three main types of attack vectors:

- **Volume-based/volumetric attacks:** These use connectionless protocols such as UDP (User Datagram Protocol) to congest infrastructure and consume all the available bandwidth.
- **Protocol attacks:** These seek to overwhelm specific devices, which may include web servers, firewalls or load balancers. These connection-based attacks typically work by exhausting resources on a device, such as the number of concurrent sessions a device can handle.
- **Application layer/layer 7 DDoS attacks:** Attacks of these types target specific applications or servers by establishing a connection to legitimate resources that consumes all service resources.

Product overview

THG Ingenuity Cloud Services provides an on-demand reactive service, ensuring that if an attack happens, we will take action to prevent any customer downtime. When purchasing an on-demand reactive delivery service, traffic will only be routed through the DDoS mitigation.

	NO PROTECTION	ON-DEMAND PROTECTION
Description	This option provides zero level of protection, upon any attack you will be blackholed. This means your service could be down for up to 24 hours.	Our reactive offering provides customers with the full security that if an attack is to happen, we will take action and prevent customer downtime.
Small targeted attacks	✗	✓
Larger targeted attacks	✗	✓
Layer 3/4 attacks	✗	✓
Volumetric attacks	✗	Up to 10Gbps in bound clean traffic that is scrubbed.
Price	N/A	£15.00/\$22.00 per month per server

DDoS Mitigation Service

Stop the largest DDoS attacks & protect your web applications everywhere.

Service scope & pricing

In normal circumstances, the clean traffic delivery does not trigger over-usage fees for periodic or intermittent bursts, though we may review this on a case by case basis. On-demand reactive customers are subject to the fair usage policy, and if a customer receives more than one attack per month, there will be additional charges. These attacks will be measured through a sliding scale – two small attacks (under 20Gb) and one large attack (over 20Gb).

Mitigation capabilities

This system is designed specifically to deal with DDoS attacks, and it's far more than just a crude rate-limiting system. It has advanced capabilities to detect, recognize and filter out common DDoS attack types, including the following:

VOLUMETRIC	PROTOCOL	REFLECTIVE
TCP & UDP floods	Malformed or truncated packets	NTP amplification
UDP fragmentation	Invalid IP segmentation	UPnP
TCP SYN floods	Bad checksums and illegal TCP flags	DNS amplification
ICMP floods	Invalid TVP/UDP port numbers	Connectionless LDAP amplification
Use of reserved IP Space	Bad checksums and illegal TCP flags	DNS amplification

Data Center Locations

Our DDoS protection is spread across the following THG Ingenuity Cloud Services data center locations:



SALT LAKE CITY



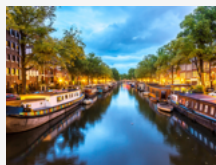
DALLAS



NEW YORK



NEW JERSEY



AMSTERDAM



FRANKFURT



+1 888 395 0752



+44 800 011 6011

ingenuitycloudservices.com

THG / INGENUITY
Cloud Services