BT Assure
DDoS Mitigation UK

What is DDoS?

DDoS or Distributed Denial of Service is a common type of cyber attack which works by flooding a target device or application with high volumes of anomalous requests which swamp the device or application and so cause denial of service to legitimate users.

Common attacks target services hosted on high-profile web servers, such as banking, credit card payment gateways and online shopping sites, but they can and often do affect any IP based service. The end result can be devastating; downtime, lost revenue, and a tarnished brand.

The threat landscape is changing

There has been a recent increase in the number of these attacks. Not only are they increasing in frequency, but the nature of these attacks is getting more severe. The average attack now monitored by leading vendor Arbor is over 1 Gb/sec — enough to bring down the majority of company networks.

> BT, working together with Arbor, successfully mitigated a recent attack on a large UK retail organisation of 54 Gb/sec.

Recent advances in technology, coupled with better ease of use and a rise in mobile devices, have magnified the threat to organisations. DDoS attacks have even been outsourced to the average person, with mobile apps offering the user the ability to opt-in to a scheduled strike. They are also increasingly being used as a means of distraction, diverting attention and resources away from other malicious exploits happening at the same time.

The complicated nature of the server requests that flood in mean that no 'blanket' solution can be put in place. While run-of-the-mill security solutions such as firewalls can go part of the way in offering protection, a higher-level solution is needed in order to more effectively address the risks.

How can we help?

Our mitigation service for BT's networks comes in three bands: bronze, silver and gold. These vary according to the level of protection needed. At the highest level, we provide 24 hour security operations' centre support, proactive reach-out and intelligence reports on the status of the server.

Bronze:
- Entry-level service providing automated detection and mitigation
- No limit to the number of auto mitigations performed in a year
- Alerting services
- Weekly reports.

Silver (bronze, plus the following):

- Flexible, self-service monitoring and reporting options specified by the customer
- Up to 16 amendments to denial of service monitoring configurations and actions per annum at no charge
- A DDoS portal is included as part of the service, allowing the monitoring of thresholds and mitigation actions to be viewed alongside any events
- BT security experts available to assist at the customer's request.

Gold (silver, plus the following):

- Increased layer 7 capability giving combined cloud and CPE protection
- 24/7 proactive support from BT's highly trained security analysts and active reach out to the customer if BT suspect the customer to be the subject of an attack or planned attack
- Unlimited amendments to denial of service monitoring configurations and actions
- Cyber intelligence and threat assessment reports specific to customer.

Benefits of BT Assure DDoS Mitigation

BT has a single platform for detection and mitigation. This means we can automatically detect rogue traffic, with no human involvement and take action very quickly to protect our customer's network.

By using a cloud-based solution, the DDoS attack is mitigated before it hits the customer's network and, in some cases, even before it enters the BT network. This means limited or no impact on the customer's business and no compromised performance.

Assure DDOS mitigation is designed as a modular, subscription service, so different levels of protection can be added as required with no capital expenditure.

How does it work?

BT Assure DDoS mitigation technologies work by 'cleaning' the internet traffic, and sorting through the normal and malicious requests.

IP address ranges are entered into a Managed Object (MO), which sets the threshold for triggering automated mitigation. Traffic flows to the IP address as usual, but when an unusual quantity or type of traffic is detected, the protection system is activated. This then starts the process of 'cleaning' the traffic, separating the DDoS attack traffic from the normal requests. Any unsafe requests get directed to a Threat Management System, while the safe requests can continue on to the IP address they originally were destined for.

Once the thresholds have been breached, the mitigation takes place in milliseconds. The IP address under attack doesn't experience any downtime, and business can continue as usual, no matter the scale or frequency of attacks.
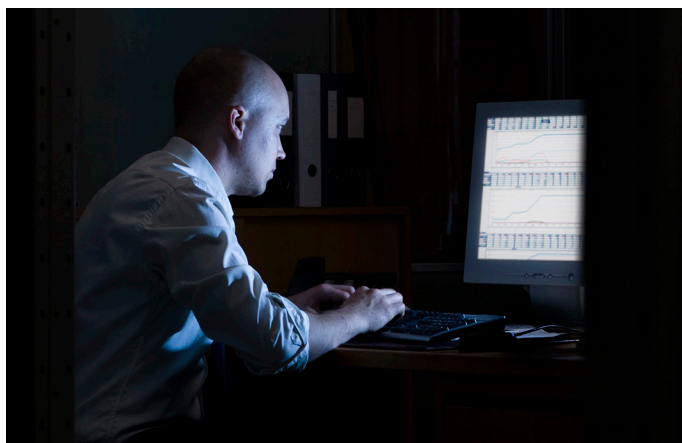
Why BT

We are the only supplier to provide a single platform for detection and mitigation. Our auto-mitigation service means extremely quick detection and protection for our customers.

BT's team of DDoS experts based in our UK state-of-the-art security operations centre have over seven years of experience dealing with attacks.

We have the unique ability to seamlessly integrate our DDoS offering with a BT-provided Internet Connect network. We're a one-stop-shop.

We have partnered with world-class DDoS vendor Arbor for the past seven years and, together, developed the comprehensive solutions that are offered to our customers today.

Offices worldwide