Protect your organisation from a concerted malicious attack

Distributed Denial of Service (DDoS) attacks are designed to flood your server or applications and bring them down. They can be devastating – resulting in downtime, lost revenue and a tarnished brand reputation. Our intelligent protection service will make sure your business stays secure. We can monitor traffic and requests 24/7 to automatically detect rogue traffic and snuff out the danger before it hits your network.

DDoS attacks typically target services hosted on high-profile web servers, such as banking, credit card payment gateways and online shopping sites. But they can affect any IP based service – and they're on the rise.

The spread of mobile technology has magnified the threat. DDoS attacks have even been outsourced, with mobile apps used to opt-in to a scheduled strike. More worrying is that DDoS attacks are often used as a distraction, diverting attention from breaches happening at the same time.

The complex nature of the server requests that flood in mean there's no 'blanket' solution. While firewalls and other standard security procedures can offer some protection, a higher-level solution is needed in order to more effectively address the risks.

Meeting the changing threat landscape

Our Managed DDoS Security works by 'cleaning' the internet traffic, and sorting through normal and malicious requests.

We enter IP address ranges into a Managed Object (MO) and set the threshold for triggering automated mitigation. Traffic flows to the IP address as usual, but when any unusual 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 or are cleansed at the edge of BT's network, while the safe requests can continue on to the IP address they originally were destined for. Once the thresholds have been breached, the mitigation can take place in minutes. The IP address under attack doesn't experience any downtime, and business can continue as usual, no matter the scale or frequency of attacks.

Mitigating the threat of a DDoS attack

- **Single platform for detection and mitigation –** so we can automatically detect rogue traffic and take action to protect your network.
- **Cloud-based solution –** attacks are identified before they hit your network so they have limited or no impact on your business and performance.
- **Modular design –** our subscription service lets you add different levels of protection as required with no capital expenditure.

From automated detection to 24/7 proactive support

Our mitigation service for BT's networks comes in four bands – bronze lite, bronze, silver and gold – depending on the level of protection you need. 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 Lite

- automated detection based on exceeding link capacity
- once set up a single on demand mitigation service for up to 72 hours maximum
- 1 hour mitigation response time within UK business hours
- easy upgrade path to bronze, silver or gold to automate and extend mitigation protection

Bronze

- automated detection and mitigation
- no limit to the number of auto mitigations performed in a year
- alerting services
- reports available via DDoS portal

Silver (Bronze, plus the following)

- flexible, self-service monitoring and reporting options specified by you
- up to 16 amendments to denial of service monitoring configurations and actions per year at no charge
- DDoS portal for monitoring thresholds and viewing mitigation actions alongside any events
- security experts available to assist when requested

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
- active reach out if we suspect you are the subject of an attack or planned attack
- unlimited amendments to denial of service monitoring configurations and actions

Managed DDoS edge defence

BT has the capability to deploy a CPE device inline on the customers premise to combat application layer / low and slow attack vectors.
Through its integration with BT's network based DDoS detection and mitigation it allows for a dual pronged approach and bolsters a company's layered approach to security, thus providing a comprehensive solution providing co-ordinated protection against all types of DDoS attack.

- Stateless analysis filtering engine
- Automated and advanced DDoS protection
- Outbound threat filter for non-DDoS threats
- Visibility, control and alerting
- Real-time and historical attack forensics and reporting
- "Out-of-the-box" blocking with custom protection recommendations

Why choose BT?

We are the only supplier to provide **a single platform for detection and mitigation.** And our auto-mitigation service provides **extremely quick detection** and protection.

Our **team of DDoS experts,** based in our UK state-of-the-art security operations centre have over seven years' 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 comprehensive solutions for our customers.

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.

What could Managed DDoS Security do for you?

Visit bt.com/security

Offices worldwide.

January 2020