Network Protection Around The Clock

Proactively block unwanted threats on your network with protection at the core.

Key benefits

- Network based detection of potential threats.
- Network based DDoS mitigation services enables you to minimise the impact of DDoS attacks by providing protection at the core. Attacks can be addressed quickly to reduce site downtime.
- Network protection around the clock.
- Enables business continuity by allowing legitimate transactions to be processed.
- Stay ahead of threats with proactive alerts and comprehensive reporting processes.
- Security costs remain manageable, as network based solutions require no hardware or software at your premises.

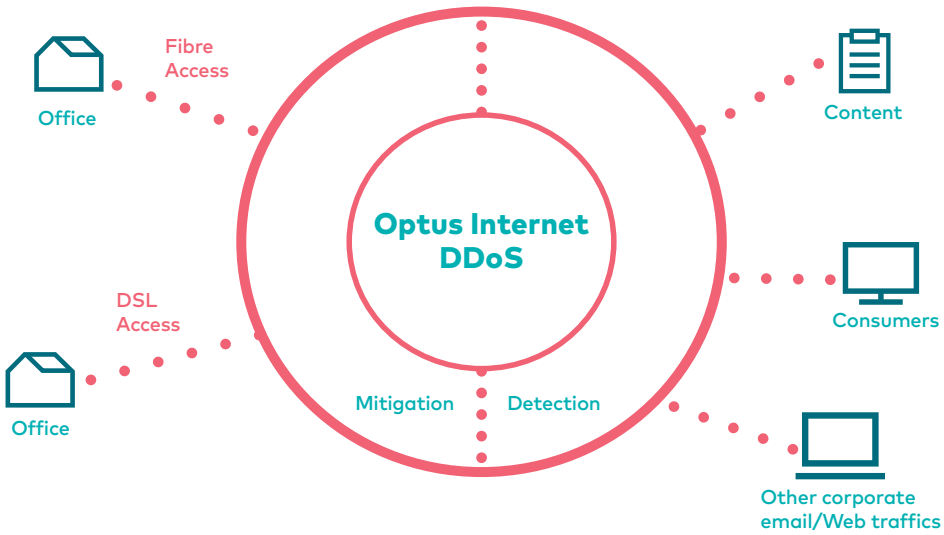
Optus Internet DDOS enables you to optimise the availability of services and applications on your network by proactively blocking unwanted threats.

A DDoS (Distributed Denial of Service) attack is a malicious attempt to consume finite networking capacity and computing resources to deny availability of these resources to its legitimate users. Firewalls, Intrusion Detection Systems and Access Control Lists are popular techniques/systems used for information security. These systems, however, are not designed for malicious DDoS attack.

Optus Internet DDoS is an optional feature of Optus Evolve Internet which offers flow analysis for your traffic, identification of potential DDoS attack on your network/ computing devices and mitigation of the threat at the edge of Optus network.

Investigate DDOS attacks

Optus Internet DDoS provides access to a secure portal which enables you to see ongoing and historical mitigations. The portal also provides valuable insight into your traffic including information about the origin of inbound and outbound traffic.



OPTUS

Optus Internet DDoS mitigation overview

The Optus Internet DDoS service has the following key components:

- Sampling traffic from Optus routers.
- Collecting all traffic records for your Internet service or services (sub-network).
- Analysing the traffic to and from your sub-network to determine whether unusually high traffic is being seen and if so alerting Optus Operations and your organisation by email.
- Analysing the traffic to determine whether any of the traffic has a known protocol-misuse and if so alerting Optus Operations and your organisation by email.
- Diverting attack traffic to 'cleaners' which remove the malicious traffic.
- Routing the clean traffic back onto your Optus Evolve Internet service.
- Regularly updating the system's ability to detect and clean new volumetric attacks with the latest attack signatures.
- Portal access to enable you to view and manage mitigation actions.

Notes:

- Optus Internet DDoS is only available on Optus Evolve Internet services.
- The default configuration is for mitigation to be automatically initiated after attack traffic has been detected for 3 minutes. The Cleaners will generally become effective within 5 minutes of attack traffic first being detected. Once the attack has finished mitigation is turned off.
- Only the detection of malicious attack traffic will trigger automatic mitigation. Your organisation will be notified by email of high traffic and if it is believed that the high traffic is due to an attack you can request Optus to divert the traffic to the Cleaners.
- Defence against volumetric DDoS attacks is provided. Optus collaborates with its partners to provide alternative solutions including defence against 'low and slow' and application level attacks.
- Only attack traffic originating overseas is cleaned. In excess of 95% of DDoS volumetric attack traffic originates overseas. Nationally originating traffic is not diverted to the Cleaners.

GMO_N 400 0816 KIT