Denial of Service Protection

Protect, Monitor & Defend

Summary

In recent years, Distributed Denial of Service (DDoS) attacks have evolved to become more prevalent and sophisticated.

DDoS attacks involve a multitude of systems on the Internet attacking a single target simultaneously to overload and prevent some or all legitimate requests from being serviced. Depending on the magnitude, the attack can cause downtime to internet services for you and your end users, impacting productivity, trust, customer satisfaction, brand confidence with potential financial implications.

Telstra's DoSP solution gives you the confidence to manage these unwanted attacks against your critical online assets and websites.

It provides a powerful and unique combination of protective measures for your business which includes:

- A monitoring, detection and mitigation system
- 24-hour, year round operational support and a dedicated hotline allowing for mitigation procedures to commence within minutes.
- The choice of Telstra initiated, customer initiated or automatic mitigation of attacks

Benefits

Safeguard Availability – Attacks are filtered before they reach your network to help protect against DDoS attacks.

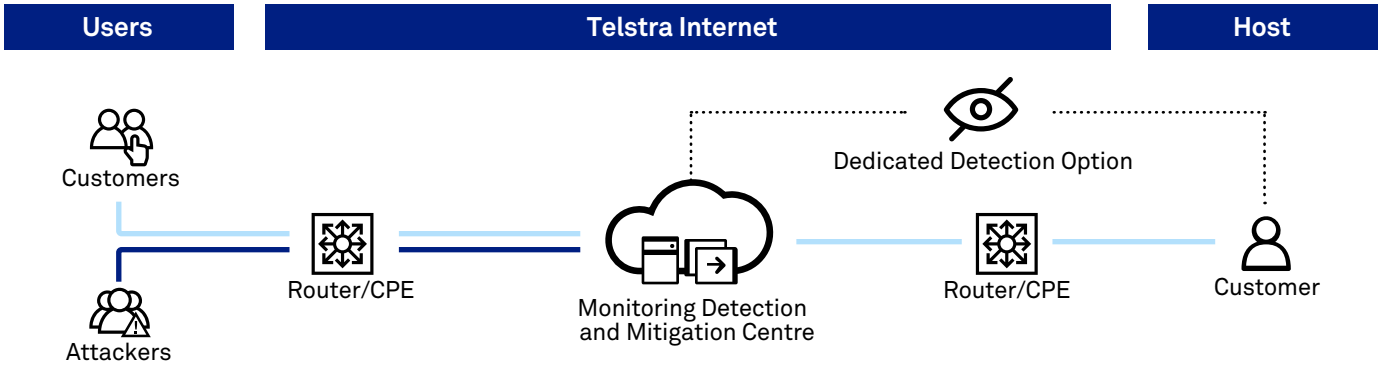
Reputational and Financial Protection – Help avoid the costs to your bottom line or to your customers' trust as a result of a DDoS attack.

Customer Portal – Allows you to monitor and protect your business and critical online services from a single portal providing peace of mind.

Simplicity – Protection against Denial of Service attacks without the need to purchase, deploy or install any additional hardware or hire specialist security staff.

Managed Solution – Proactive, near real-time management and monitoring to deliver cost-effective, customised 24/7 protection for the mitigation of distributed denial of service attacks targeted at your Internet connection.

A Telstra Network Security Service that monitors your traffic and when an attack is seen, activates a cleaning solution to mitigate the effect of the attack.



We provide two service options to meet your risk profile and regulatory needs:

- **Premium**: Monitors your internet link and internet facing on-premise equipment offering added protection for companies whose reliance on the internet is mission critical to their business. Customers have access to our trained security professionals whenever required.
- **Standard:** Monitors your internet link only. This would be suitable for companies who use the internet as part of their everyday business but not for vital operations. Customers also have access to our trained security professionals whenever required.

Key components

With Telstra's DoSP solution, specialised hardware and systems are deployed within Telstra's core network to support DDoS detection, attack mitigation, threat management and reporting functions.

The two main hardware components of the Telstra DoSP platform are Netflow Collectors and Mitigation Centres:

Netflow Collectors

The Netflow Collectors continuously monitor traffic levels at specific entry points to your network by using the Netflow protocol. DDoS alerts are generated when the traffic level exceeds the pre-determined baseline values at those traffic monitoring points.

Mitigation Centres

Telstra's Mitigation Centres are deployed globally within Telstra's domestic and global network infrastructure. If traffic filtering is required during a DDoS attack, your downstream traffic will be diverted to Mitigation Centres for cleaning purposes. 'Clean' traffic is then delivered back to your network via generic routing encapsulation (GRE) tunnelling technology.

A key feature of Telstra's DoSP solution is the global presence of traffic mitigation / scrubbing facilities which allow the DoSP Platform to mitigate a DDoS attack closer to its source (or sources) that significantly enhances its effectiveness.

24/7 Proactive Monitoring

DDoS alerts are monitored 24x7 by a dedicated team of cybersecurity analysts and specialists within our T4-certified Security Operations Centres (SOCs) based in Australia.

These SOCs provide proactive monitoring of your traffic to help protect your critical online services. Appropriate mitigation actions are then initiated based on the pre-agreed plan.

The DoSP solution can also be integrated with other Managed Security Services to provide additional visibility of your infrastructure, e.g. intrusion detection systems.

Complementary security products & services

Telstra Denial of Service Protection forms a key element of our wider security services portfolio, helping to protect our customers from malicious, distributed denial of service attacks and defending their critical online services. In addition to our DoSP solution, Telstra offers other complementary security solutions to our customers which include:

Telstra Internet Protection Web & Mail: Proactive, in-the-cloud protection against phishing, malware, ransomware and impersonation attacks.

Telstra Gateway Protection Advanced: Provides your business with an advanced cloud based secure Internet gateway, delivering virtualised Next Generation Firewall services.

Telstra Security Consulting Services: Helps protect your information assets from security breaches and threats by recommending the appropriate strategy, architecture, solution and services for your environment.

Managed Security Services: Telstra's Managed Security Services combine event data, analytics and discovery tools to give you visibility, detection and notification of security incidents in order to respond in a timely manner.

Contact your Telstra account representative for more details.

Australia

1300 835 787

telstra.com.au