CYBER

# DDoS Protection

## Advanced attack protection to ensure business continuity

DDoS (Distributed Denial of Service) attacks are increasing in sophistication and force.  Their scale and complexity threatens to overwhelm the internal resources of a business.  They can be devastating – resulting in downtime, lost revenue and a tarnished brand reputation.

Our Anti-DDoS offering conveniently sits in front of your existing 4D internet connection, proactively monitoring traffic to mitigate attacks from ever reaching your enterprise network.

## What is a DDoS attack?

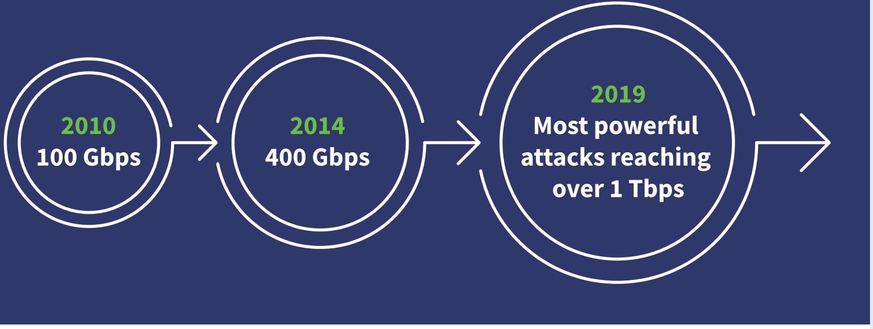
A malicious attempt to disrupt normal traffic of a targeted server, network or service.  Attackers overwhelm the target by generating large volumes of Internet traffic designed to flood your server or applications and bring them down – so causing denial of service to legitimate users.

Deployed as part of 4D's integrated cyber security offerings, our intelligent and scalable DDoS protection will make sure your business stays secure -  ensuring you only receive clean, attack-free traffic.

## Meeting a Changing Threat Landscape

DDoS attacks are growing ever more complicated and innovative in their targeting and techniques.

### BIGGEST ATTACKS RECORDED



2010
100 Gbps

2014
400 Gbps

2019
Most powerful attacks reaching over 1 Tbps

## Why 4D?

**4D Data Centres is an independently owned UK-based managed infrastructure provider with facilities in Gatwick, Surrey, Kent and London.  Since 2007, we've delivered colocation, cloud, cyber and connectivity services to hundreds of small and large-scale organisations.**

## 4D's Multi-layered Cyber Protection

Maintain business continuity with 4D's Cyber Security solutions

**Managed Firewalls**
Industry-leading perimeter protection

**DDoS Protection**
Safeguard your network and data

**Threat Monitoring**
Proactively minimise overall threat exposure

**Managed Backups**
Last line defence against system failure

## 91% of businesses have suffered network outages following a DDoS attack

The average cost to a UK business suffering downtime as a result of a DDoS attack is over £140,000.

### CHALLENGES

- DDoS attacks typically target services where there is an obvious need for 24/7 availability - high-profile web servers,  such as credit card gateways and online shopping sites, however they can affect any IP based service.
- DDoS attacks achieve effectiveness by utilising multiple  compromised computer systems as sources of attack traffic.
- DDoS attacks are often used as a distraction, diverting attention from breaches happening at the same time.

# Comprehensive Multi-layer DDoS Attack Protection

4D's always-on or on-demand DDoS mitigation service manages any type, size or duration of attack on your network or web apps – with near-zero latency.

If a new pattern of attack is developed and not filtered, our DDoS engineers adjust the protection systems to keep you safe.

## KEY BENEFITS

- ✓ Stop DDoS attacks BEFORE they reach your enterprise network and affect your business, using real-time attack detection and mitigation
- ✓ Defend against large-scale volumetric attacks – mitigate against attacks over 1 Tbps in size
- ✓ Engineered for both application & protocol protection - up to Layer 7 (Application)

## Service Features

### Flat-rate charging

Avoid the risks of fees attached to traffic spikes

### Large-scale attack protection

Safeguard against one of the biggest cyber threats

### 24x7x365

Dedicated account management and immediately available support

### Regular reporting

Threat visibility and blocked attacks to your network

## Service Options

Our flat monthly fee model has no additional bandwidth charges or usage costs.

| | Standard DDoS Mitigation | Full DDoS Mitigation* |
|---|---|---|
| Operate in-line with your existing IP transit from the 4D core | ✓ | ✓ |
| Clean traffic delivered up to your existing CDR on 95th Percentile | ✓ | ✓ |
| Number of attacks protected against per month | Up to 2<br>(Activated when an attack is discovered/ reported) | Unlimited |
| 'Always-On' Protection Option available | ✗ | ✓ |

*Note that Full Protection mitigation requires a minimum /24 of IPv4 space.

# Technical Specifications & Features

4D's DDoS Protection safeguards against a wide variety of common attacks.

| Common Types of Attacks | Examples |
|---|---|
| IP non-existing protocol attack | Flood with IP packets |
| Attack with fragments | Sending mangled IP fragments with overlapping, over-sized payloads |
| ICMP attacks | ICMP Flood, Smack, Smurf attack |
| TCP attacks | SYN Flood, SYN-ACK Flood, ACK Flood, FIN Flood, RST Flood, TCP ECE Flood, TCP NULL Flood, TCP Erroneous Flags Flood, TCP Xmas, Fake Session, SRC IP Same as DST IP |
| UDP attacks | General Random UDP Floods, Fraggle, DNS query, DNS Amplification (+DNSSEC), NTP Amplification, SNMPv2, NetBIOS, SDP, CharGEN, QOTD, BitTorrent, Kad, Quake Network Protocol, Steam Protocol |
| HTTP attacks | Slowloris (Apache / IIS Attack), R-U-Dead-Yet (RUDY), HTTP Object Request Flood |
| Other categories | Misused Application Attack and Slow Read attack |

| Technical Features | |
|---|---|
| Machine Learning | • Dynamic behavioural identification/progressive challenge algorithm determines whether an IP is dangerous or not.<br>• The output is used to populate the blacklist. |
| Blacklist / Whitelist | • Blacklisting removes flagged entries automatically.<br>• Whitelisting is applied to automatically approve and bypass behavioural identification. |
| IP Blocking | • Performed on border through ACLs (Access Control List) – configurable at customer request |
| TCP/UDP Generic Inspection & Filtering (Transmission Control Protocol/User Datagram Protocol) | • Achieved through an ACL by building inclusive/exclusive firewalls.<br>• Built with the standard communication in peer-to-peer, client- server, server-client relationships as reference.<br>• Any deviation from the standard communication will trigger filtering. |
| Deep Packet Inspection | • Both the header and the body of the packet are inspected in order to determine if it is safe.<br>• It keeps track of the frequency of the message being sent. |

The data floor at 4D's Gatwick Data Centre

## Take the next step

4D's Cyber Security Solutions supports cloud transformation, infrastructure and data management with an integrated approach to strengthen your overall security posture.

Discover why hundreds of organisations like yours trust us with their data and infrastructure security.