

## Our Services

### DDoS Mitigation

Comprehensive protection  
against DDoS attacks.



## What is DDoS?

Distributed denial of service (DDoS) is one of the most serious threats facing companies on the Internet. DDoS attacks are typically launched by compromised PCs controlled by remote attackers to inundate a victim's network with the intent of crashing their web or application servers. DDoS can wipe out your web presence for months with incalculable financial costs and damage to your reputation.

Historically, DDoS attacks were carried out for extortion, but now that criminals offer DDoS services for hire, unscrupulous companies use them to take out their competitors' web presence. With DDoS being used against a wide range of companies, recent crime reports suggest that the total number of attacks is doubling year-on-year. The largest-scale attacks can flood your network with over 20Gbps, which can bring even the most robust environment to its knees. But high-volume attacks are not the only threat, the latest trend is to use lower-bandwidth application-level attacks that are designed to go under the radar of off-the-shelf DDoS appliances.

### Is DDoS mitigation for me?

Until about two years ago, companies outside of high-risk industries, such as media, finance, gaming and payment services, would probably not have been affected by DDoS attacks. But it is now cheaper than ever to launch an attack, and it can be very expensive for the victim to stop it. Now that all companies are at risk, you need to ask yourself how your reputation and finances would suffer if your website was unavailable. If website availability is important to you, then TelecityGroup's specialist DDoS mitigation service provides you with round-the-clock protection from denial-of-service attacks.

### How does it work?

When we detect a DDoS attack, your traffic will be routed through our system where it is 'scrubbed' clean. This approach keeps the malicious traffic out of your network and allows legitimate traffic through. The mitigation happens transparently and your service will be maintained throughout the attack. When the attack is over, the routing of traffic to your service will be returned to its normal path.

### Related services

DDoS is part of our Internet security portfolio and is related to services such as Intrusion Detection and Prevention (IDP) and Managed Firewalls. These are available on our fully-resilient Internet access service, called IP Multihome.

IP Multihome allows you to deliver your content through multiple carriers, providing superior performance and resilience. TelecityGroup gives you access to fully-redundant Internet connectivity without the expense and complexity of dealing with multiple carrier relationships. You receive a single bill for your transit and peering connectivity, and have a single point of contact for support.

Our Managed Firewall and IDP services complement DDoS Mitigation by providing further monitoring and protection of your web services. Firewalling provides stateful inspection of your allowed applications and will block unauthorized access to your services. IDP adds to this protection by inspecting and filtering your application traffic to remove exploit attempts.

### Why TelecityGroup?

For companies who rely on the Internet, a DDoS attack is a serious problem that could have far-reaching consequences. We are able to offer you comprehensive protection using market leading technology from Arbor Networks to protect against any attack without affecting your network or requiring any further investment in equipment.

We provide DDoS mitigation across all our London sites where your traffic is cleaned in our core networks. We are also part of a community-based approach to fighting DDoS attacks upstream, through the Arbor Fingerprint Sharing Alliance.

### Key benefits

- Optimised availability by proactively detecting and mitigating network-wide anomalies caused by DDoS attacks, botnets and other threats.
- Improved capacity planning and simplified compliance via real-time network analysis and historical reporting.
- Active monitoring and 24x7 support ensures maximum uptime and availability.
- Improved internal network protection through partnerships with leading service providers.
- Up-to-date immediate threat detection via active threat feed.
- Protection and visibility for your hosted networks.
- Simplified pricing & integration to complement your firewall, IDP and IPMH solutions.
- Monthly traffic reports as standard for the service. Additional reporting frequency and detail available.

### Wide range of available protection

DDoS attack types	Details
Generic flood attacks	Flood of traffic for one or more protocols or ports. May be spoofed or non-spoofed.
Fragmentation attacks	A flood of TCP or UDP fragments are sent to a victim overwhelming the victim's ability to reassemble the streams and severely reducing performance. May also be a result of misconfiguration.
Connection attacks	Connection attacks maintain a large number of half-open or fully open idle TCP connections.  Resource exhaustion in the TCP stack or application connection tables prevents the victim host from allowing new TCP connections to be opened to the victim.
Application attacks	Application attacks are designed to overwhelm components of specific applications.
Vulnerability exploit attacks	Vulnerability exploit attacks are designed to exploit a software flaw in the victim's operating system or application.

### Specifications

#### Multiple methods of threat detection and mitigation

We protect your critical IP services with a combination of attack detection and mitigation methods, including:

- Block known malicious hosts by using white and black lists. The white list contains authorised hosts, while the black list contains compromised hosts whose traffic will be blocked.
- Block application-layer exploits by using complex filters. We can use payload visibility and filtering to ensure cloaked attacks cannot bring down critical services.
- Defend against Web-based threats by detecting and mitigating HTTP-specific attacks. These mechanisms also help with managing flash-crowd scenarios.
- Shield DNS services from botnets that mask, amplify and deliver exploits to DNS infrastructure and services by employing DNS-specific attack detection and mitigation capabilities.
- Protect critical VoIP services from automated scripts or botnets that exploit packets per second and malformed request floods by employing VoIP/SIP-specific attack detection and mitigation capabilities.
- Control the zombie army by using specialised, always-on and learning zombie detection mechanisms that ensure compromised hosts are not attacking mission-critical infrastructure.
- Enforce baseline protection by building ongoing, always learning models of network behaviour. This information can be leveraged to ensure that abnormal traffic can be distinguished and blocked from the network at time of attack.
- Use GeoIP-based reporting and mitigation to identify and report on where traffic is coming from (by country, by city) and block traffic from illegitimate sources.

### Service Workflow

Detailed below are the key process steps in our DDoS mitigation service and an outline of how we react to an attack:

#### Connection to service

- Simple activation, no additional hardware required.
- Consultation to understand the risks associated with your platform.
- Bedding-in period to review and modify the configuration of the DDoS service.
- Runbook captures information relating to your environment, escalation points and procedures.

#### Reviews

- Reports produced every month for your review.
- Review milestones every 3 months.

### Service levels

We provide the following DDoS Mitigation service levels:

#### Attack notification

Within 15 minutes of attack identification.

#### Time to mitigate

Auto-mitigation will commence within 30 minutes.

#### Base lining

The initial 4 weeks after service activation during which time the specific customer service is analysed in detail and characterised to provide the baseline for attack detection.

#### Availability of DDoS mitigation infrastructure

99.95% target availability for DDoS infrastructure within TelemetryGroup's IP network, excluding scheduled maintenance periods.



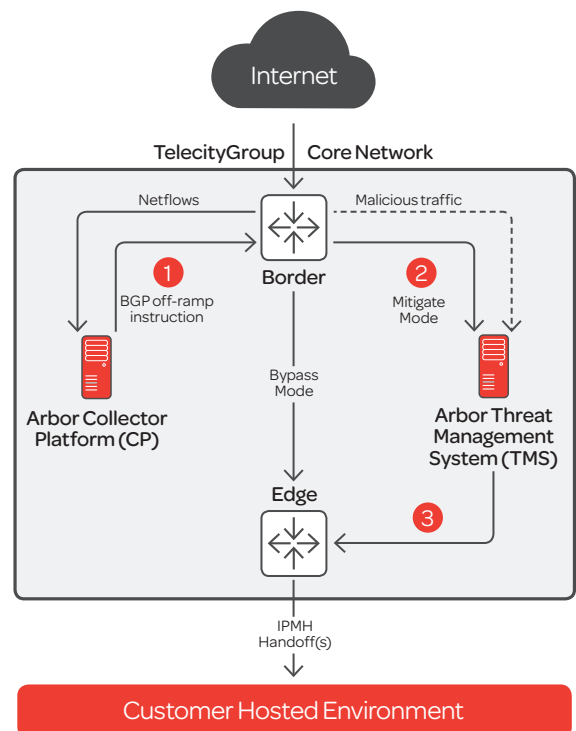
**Outstanding data centres.  
Expertise you can trust.**

Europe's leading provider of premium network-independent data centres.

[www.telemetrygroup.com](http://www.telemetrygroup.com)

### Detection and reaction to an attack

1. Attack is detected and exceeds the agreed thresholds;
2. We gather evidence of the attack and correlate it with other known information, such as that gained from monitoring your solution;
3. We perform impact analysis and validate the threat;
4. The runbook details the specific procedure to follow, such as 'clean traffic independently' or 'consult with you before taking action';
5. Produce report of the attack and the mitigation steps carried out.



### Contact TelemetryGroup

10th Floor  
6 Harbour Exchange Square  
London E14 9GE

+44 (0)20 7001 0101  
info@telemetry.com