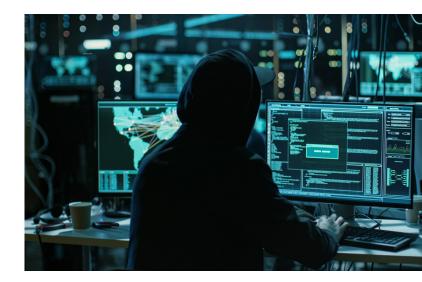# DDoS Protection

Boost resilience against complex DDoS threats

with our robust defence system

What is a DDoS attack?

A DDoS or distributed denial-of-service attack is an attempt to disrupt the flow of regular traffic to a network, targeted server or service by overwhelming it with a large number of malicious traffic. DDoS attacks look to exploit the control of computers and other internet-connected devices to form a botnet network. This traffic will then bombard a system with thousands of requests until the service eventually crashes and cannot resume normal service. The rise in the number of DDoS attacks is showing no sign of slowing down, with attacks continuing to grow in size, scale and sophistication. So what can you do?

DDoS Defence System

As websites and applications are increasingly at risk of DDoS attacks, businesses should look to deploy a dedicated DDoS defence system where possible.

DDoS protection is a system of practices and technologies that can help protect you from being knocked offline by DDoS attacks. Utilising hardware, algorithms and advanced software to monitor incoming traffic to an application or website, any traffic that is deemed illegitimate will be filtered out and denied access.
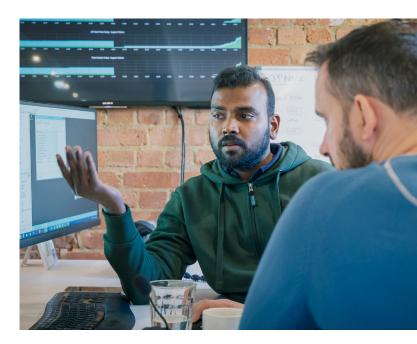
DDoS protection options will generally guard against attacks up to a certain amount of traffic per second. For example, most standard protection options for organisations will protect against attacks ranging anywhere from five to ten gigabytes of data per second, with more robust and secure protection options guarding against attacks of 100 gigabytes per second or more.

We are **serious** about **service.**   We **deliver** business **outcomes.**   We are **your cloud experts.**

How much protection does your site need?

The amount of DDoS protection will naturally fluctuate from business to business. When deciding how much you need, it is worth having a good understanding of the amount of traffic coming to your site during a regular period of operation as well as during peak times. If your website or application regularly receives a large amount of traffic, a basic level of protection may not be enough to suit your needs.

If you are unsure about how much protection your website or application may need, it is always advised to discuss this directly with your hosting provider.

DDoS Protection with Hyve

As part of our commitment to security, Hyve offers an extensive DDoS protection service that ensures the security of your mission-critical infrastructure.

Built on four key areas; detection, diversion, verification and forwarding, Hyve's DDoS defence system inspects incoming traffic and identifies any flaws or a large number of suspicious connections. When an attack is detected, our system transfers the malicious traffic to a scrubbing and filtering site and allows legitimate traffic to hit the site as normal. The diverted or malicious traffic is sent away for treatment, and once cleaned, it will be routed back to the server.

Features of Hyve's DDoS Protection System

- Detects and mitigates network-layer DDoS attacks and more advanced application-layer attacks

- Substantial, multiple bandwidth feed capacity data centres

- Low latency even during times of attacks

- Protects against outbound attacks caused by viruses or malware