Secure

Managed DDoS

24Seven

Connectivity without compromise

Managed DDoS

Protecting your business against enterprise security threats

Protecting your business against enterprise security threats and DDoS attacks that become more frequent and complex, every day.

DDoS attacks are different from most security threats. Traditional systems cannot protect businesses against large scale attacks, which are now, more than ever, a greater threat for any type of business and organisation, with motivators such as organised crime, politics or hacktivism.

Our Managed DDoS product includes scalable and efficient anti-DDoS solutions for a wide category of businesses, detecting and successfully mitigating advanced attacks, which have exploited applications, web servers and DNS vulnerability, hit-and-run or botnet type of attacks.

Product benefits and features

- M24Seven owned 'Anomaly Detector' ecosystem, **completely eliminating potentially dangerous traffic** and allowing only legitimate traffic in your network during an attack
- **Diverse and robust mitigation** – personalised platform and protection through Corero and Radware, two of the most important suppliers of DDoS mitigation systems
- **Speed** – mitigation is done in a matter of seconds as our systems use complex algorithms to analyse live traffic
- **Scale** – both capacity and other locations on our map can be added easily, because we have built the solution having in mind that we need this to be scalable. The hardware itself is modular, plug and play, and the software is built to run in our M24Seven Internal Cloud, for maximum redundancy and scalability
- **Multiple locations** – the DDoS mitigation platform is built to clean all the traffic at the very edge of our network, to make sure no DDoS, no matter how large it is, can affect any of your services

Business benefits:

Protecting uptime and Data Integrity :
Our Managed DDoS service works like an insurance policy against high level attacks. When organisational performance is threatened by system interruptions or instability.

Pre-empting:
M24Seven provides support for automatic and rapid detection of threats at the most granular level, facilitating early warning and the ability to characterise attacks in time. This allows us to help you avoid financial loss caused by interrupting the web activity and systems that would otherwise be brought down, often for a long period of time.

Enhanced Support:
Comprehensive reports on browsing habits of employees or other users to fulfill HR requirements and allowing you to control access to certain websites, including social media.

Types of attacks we can prevent:

With our behavioral DoS mechanism, we're able to protect your internet assets from even the largest and most advanced DDoS attacks.

Category of DDoS Attack Type	
Volumetric DDoS Attacks	• TCP Flood Attacks • UDP Flood Attacks • UDP Fragmentation Attacks • ICMP Floods • HTTP/Service Flood • Connection Flood
Reflective DDoS Attacks	• NTP Monlist Response Amplification • SSDP/UPnP Responses • SNMP Inbound Responses • Chargen Responses • Smurf Attack • Fraggle Attack DNS • DNS Amplification
Resource Exhaustion DDoS Attacks	• Malformed and Truncated Packets (e.g. UDP Bombs) • IP Fragmentation/Segmentation AETs • Invalid TCP Segment IDs • Bad checksums and illegal flags in TCP/UDP frames • Invalid TCP/UDP port numbers • Use of reserved IP addresses
Other DDoS Attacks	• Command and Control Operations • Tunnel Inspection (GRE, MPLS etc.) – GRE, MPLS etc. • NTP Monlist Requests • Blacklisting & Whitelisting of IP • Known malicious IP Addresses (botnets, scanners, anonymisation services, phishing sites, spammers) • Customised Protection with – Blacklisting of IP Addresses – Port address range filters (provides protection for generic TCP/UDP port based attacks) – Rate Limiting Policies • Flex-Rule – Programmable filters based on the Berkley Packet Format (BPF) syntax. These can be programmed to address a variety of attack categories volumetric, reflective through to attacks leveraging specific payloads (Teamspeak, RIPv1, netbios). • Smart-Rule – Heuristics based engine leverages heuristics and behavioral analysis to track and rate limit L1-L4 attacks

You may also be interested in:

Data backup
Managed Firewalls
Content Filtering

24Seven
Connectivity without compromise

For our Sales Team call 0800 066 2739
For our Support Team call 0161 822 2580
Alternatively email our friendly team at hello@m24seven.com
www.m24seven.com