JT DDoS Mitigation

Product Overview

Distributed Denial of Service (DDoS) attacks are when hackers use a global network of compromised devices to flood your internet connection with so much traffic that your normal internet traffic gets jammed up and can't get through, shutting down your services.

Attackers also try to overwhelm your firewalls and network, so they fail under the huge weight of traffic, disrupting your network availability, or as a distraction whilst they try to hack in to your infrastructure elsewhere.

Ongoing protection, which evolves as you do

The JT DDoS Mitigation Service blocks network-based DDoS attacks before they come near a customer's network. The service can absorb volumetric attacks of over 4.3 Tbps and uses a multilayered solution designed to remove all known and evolving types of DDoS attacks, providing customers with only clean bandwidth.

JT's dedicated Cybersecurity team use sophisticated Cyber Threat Intelligence to tune and optimise the service, to ensure it always delivers stateof-the-art protection.

JT's DDoS Mitigation Service is part of eleven regional DDoS Scrubbing Centers', working with over 200 Points of Presence removing DDoS traffic from clean traffic as close to its source, as possible. This ensures your good traffic is not disrupted on any part of its journey across the internet and bandwidth is only consumed by clean traffic.

1.3 Tbps

of traffic targeted a site in the largest DDoS attack ever recorded.

14.5 million

DDoS attacks are anticipated to double to 14.5 million by 2022

JT

Always On

JT DDoS Mitigation service blocks DDoS attacks in the cloud before they reach a customer's network ensuring that the customers links are completely protected.

The JT DDoS Mitigation Service can easily be added to a customer's existing connection and includes the following features:

- Direct integration with the JT global internet network
- Generic DDoS mitigation and protection
- Volumetric network protection
- 'Always on' service, building traffic profiles based on real-time traffic flows
- Line rate Network Behavioural Analysis and anomaly detection
- Highly scalable attack mitigation
- Extremely low 'false positive' and 'false negative' ratios
- Eleven regional scrubbing centres

1.5 million

IoT devices were recruited into the Mirai Botnet virus and used as a DDoS weapon.

To find out more contact us at:

T **Jersey**: +44 (0) 1534 882 345
Guernsey: +44 (0) 1481 882 345
E business.solutions@jtglobal.com
W www.jtglobal.com/businesscontinuity