Transworld™

DDoS Mitigation

Corporate Office
Retalia Building, 2nd Floor,
Plot No 24, G-6 Markaz, Islamabad.
Tel: +92 (0) 51 2871 623-4
Fax: +92 (0) 51 2871 625

Lahore Office
138 CCA Phase 5 Defense Housing Authority Lahore.

Karachi Office
Dolmen City, (Executive Tower) 6th A Floor,
HC-3, Block-4, Marine Drive, Clifton, Karachi.
Tel: +92 (0) 21 3582 4951-4

111 111 891 | www.tw1.com

Transworld DDoS Mitigation Service

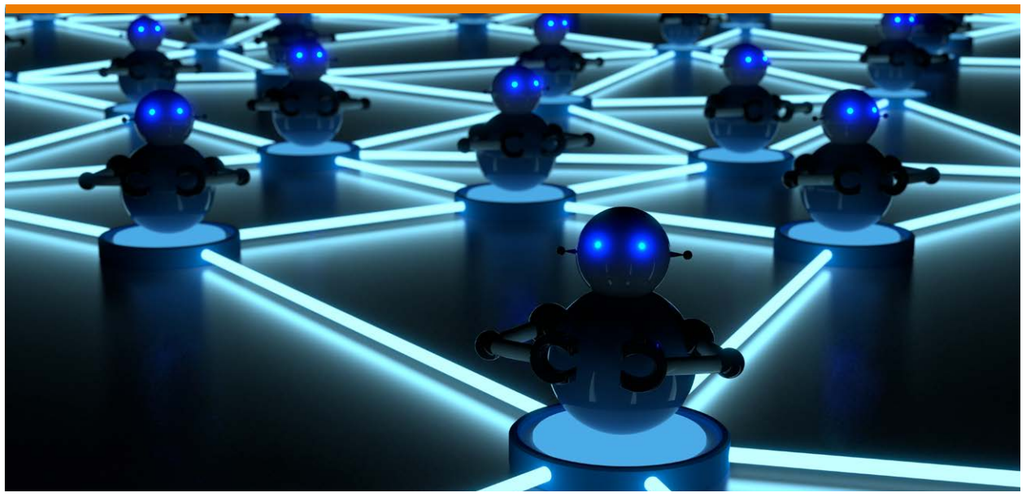
Any business entity that uses the Internet for its core business can no longer do business if their operations are down. This results in revenue loss. Some types of online businesses and financial institutions are more prone to DoS/DDoS attacks than others. However, everyone recognizes that without a stable and secure business momentum their critical data and revenue is under threat.

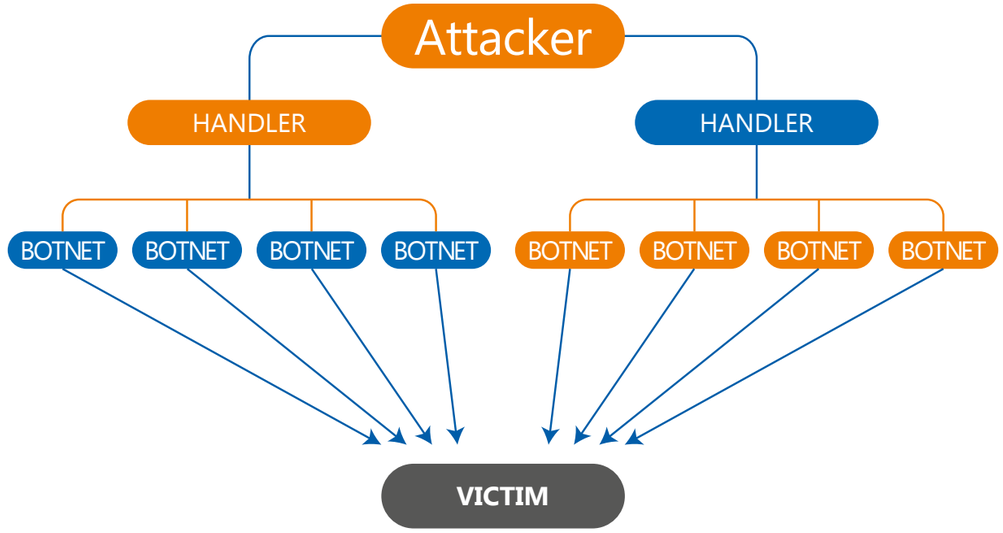
Introduction to DDoS Attacks

Cyberattacks have become a fact of life, with data breaches of high-profile businesses and organizations making headlines practically on a daily basis. One common type of cyber threat is a denial of service (DoS) that—as its name implies—renders websites and other online resources unavailable to intended users.

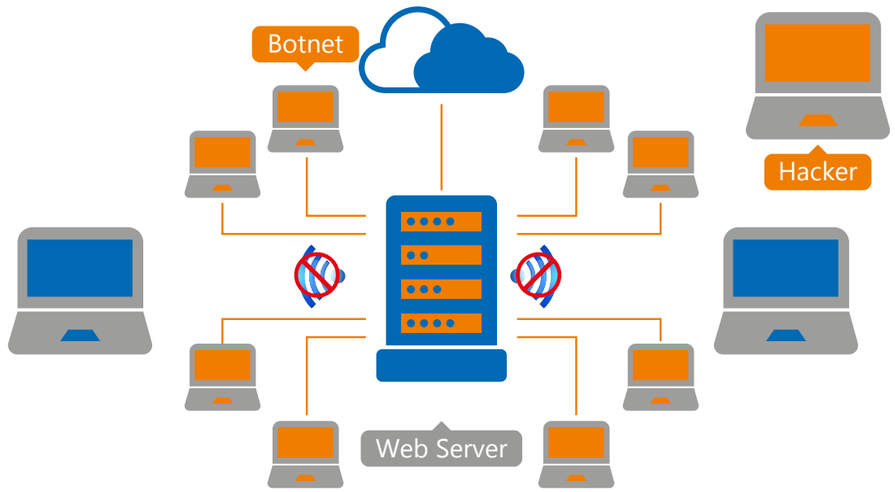
DDoS attack is an attempt to make a computer/ network user unavailable over internet. A common attack method requests to open huge number of connections from multiple hosts. The target host cannot cope with such a large number of session requests and simply stops responding; rendering it useless. The DDoS attack also swamps a customer's Internet connection, blocking traffic from legitimate sources.

A common attack method is for an attacker to use thousands of compromised Internet connected computers to form a 'botnet'. This simultaneously sends multiple requests to open a network session with a host or network device owned and operated by the attack target. As the attack grows, the traffic generated by the botnet aggregates and begins to swamp the target's Internet connection and host's machines; effectively disconnecting them from the Internet and rendering them useless.





DDos Attack



The attack involves saturating the target machine with requests, such that it cannot respond to legitimate traffic or responds so slowly that it renders it unavailable.

Types of DDoS Attacks

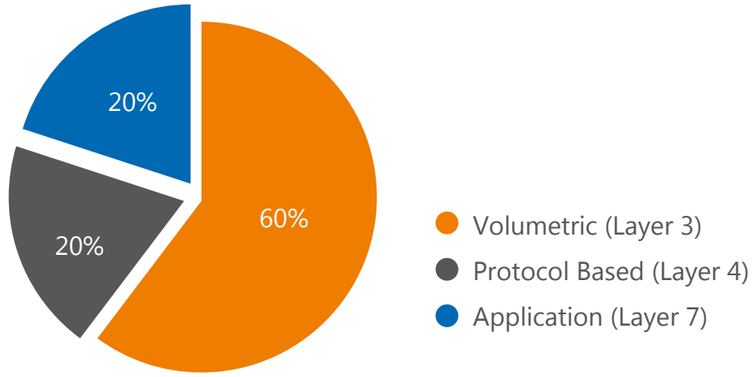
NETWORK LAYER DDoS ATTACKS

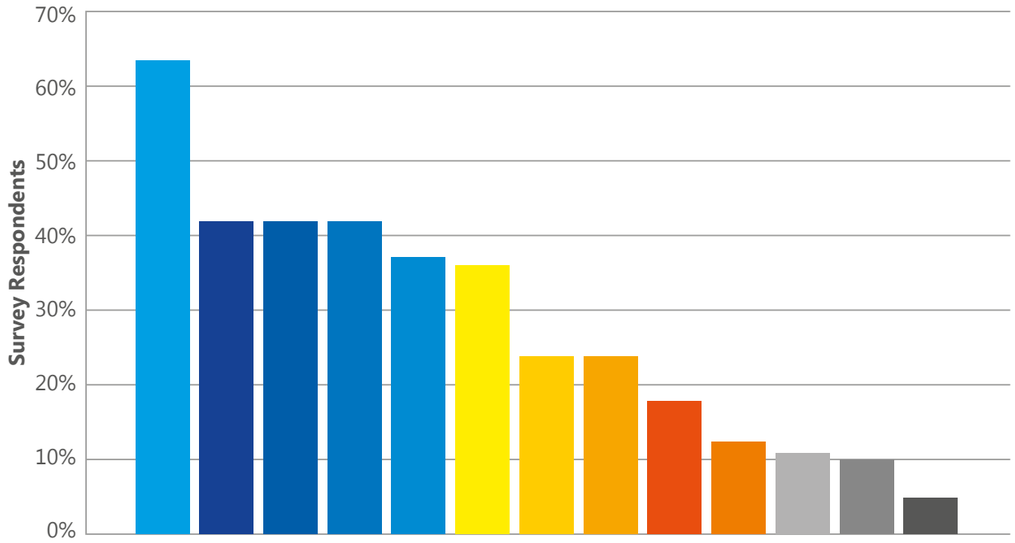
- Volumetric attacks use multiple infected systems to flood the network layers with a substantial amount of seemingly legitimate traffic.
- Smaller network packets result in faster packet-forwarding rates and higher peak DDoS traffic
- Protocol based or State-exhaustion attacks target the connection state tables in firewalls, web application servers, and other infrastructure components.

APPLICATION LAYER DDoS ATTACKS

- Slow, Stealthy and require less volume than network layer attacks to succeed.
- Attackers attempt to bring down a service by sending seemingly harmless HTTP or DNS requests which are commonly used.

Percentage of DDoS Attacks





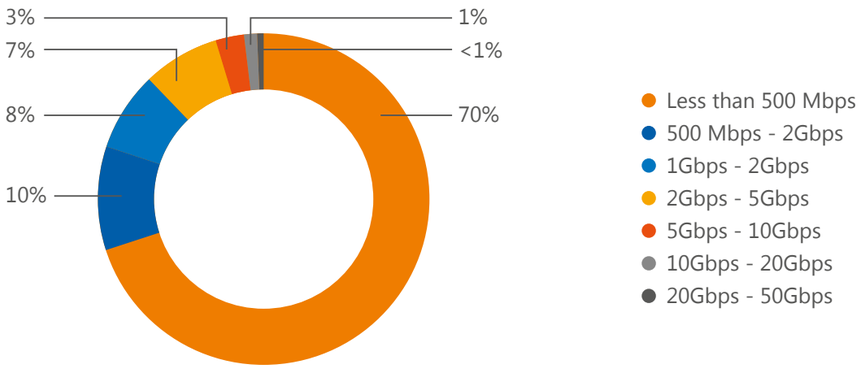
63% End-user/subscriber
42% Financial Services
42% Hosting
42% Government
37% E-Commerce
36% Gaming
24% Education
24% Gambling
18% Utilities
12% Manufacturing
11% Law Enforcement
10% Healthcare
5% Other

Source: Arbor Networks

Breakup

ATTACK SIZE BREAKUP

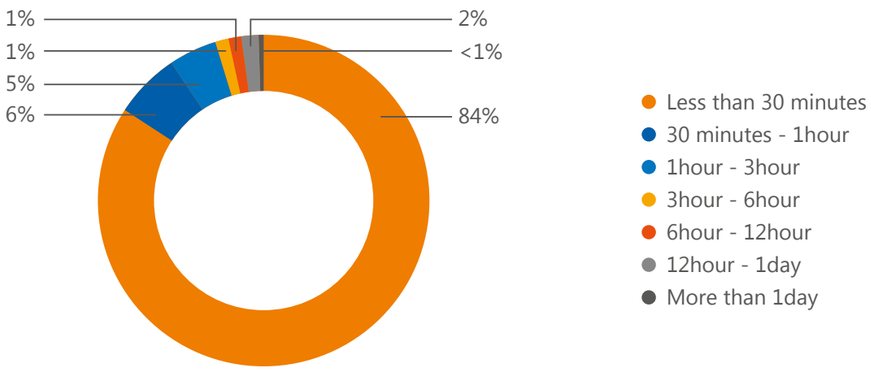
- Most of the DDoS attacks are still relatively smaller in size. Around, 88 percent are less than 2 Gbps.
- Attacks between 500 Mbps and 2 Gbps in size are easily capable of saturating the Internet connectivity of many enterprises.



Source: Arbor Networks

ATTACK DURATION BREAKUP

- 91 percent of attacks lasted less than one hour. The average duration of an attack in 2016 was 55 minutes
- More than 44 percent of application layer attacks lasted more than an hour while just 12.2 percent of network layer ones did.



Source: Arbor Networks

Service Description

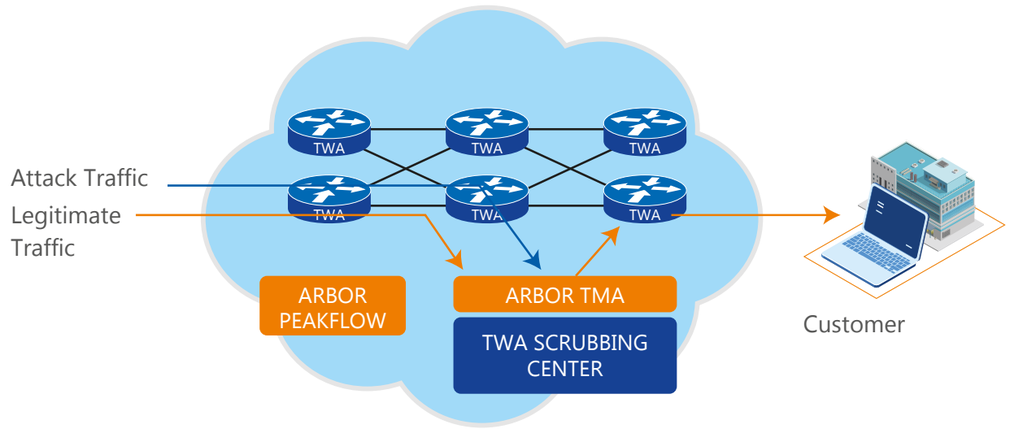
GENERAL DESCRIPTION AND POSTIONING

Transworld's DDoS Mitigation Service is a managed service that provides customers Internet connections and Internet facing hosts with Mitigation against the threat of DDoS attacks. During an attack a customer's traffic is redirected through our DDoS Mitigation platform which intelligently identifies and drops malicious attacks such as traffic in our core network before it reaches a customer port where it will cause the most damage.

Historical techniques for dealing with DDoS attacks, such 'black hole' routing, stopped all traffic from reaching the DDoS attack target. Whilst 'black hole' routing is effective at protecting a site or data center it can also achieve the same result as the DDoS attack because it blocks all traffic, good and bad.

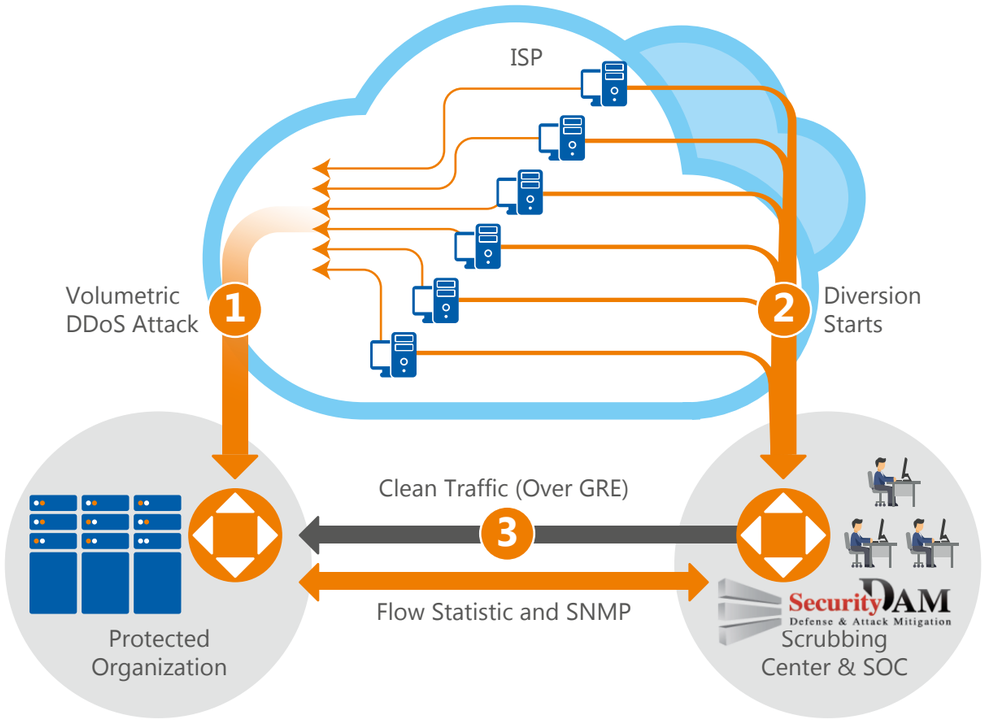
Transworld's DDoS Mitigation Service uses Attack Detection and Attack Mitigation Systems located at Transworld's Internet gateway, to analyze, identify and discard malicious DDoS attack traffic generating from Internet before it reaches a customer's port. By filtering the malicious traffic in our backbone, the customers Internet connection and hosts do not become saturated with DDoS attack traffic and can remain operational.

Transworld's DDOS Mitigation Service is currently focusing on country's Financial Institutions, high-end corporates/MNCs, and CDN to ensure their highest availability for high uptime dependent business.



ON-DEMAND SERVICE OPTION

When an attack is detected, the customer contacts and requests Transworld Technical Assistance Centre (TAC) to enable DDoS mitigation service, by quoting their DDoS Mitigation Service ID (SID). By customer's consent, the task will be carried out, ensuring that Mitigation is not activated and traffic is not re-directed due to non-malicious activity known to the customer, such as large file transfers, a special event.



How DDoS Mitigation Works?

DDoS Mitigation is a process which redirects Internet traffic destined for a customer's host or network infrastructure through a Threat Management System (TMS).

The Threat-Management System analyzes the customer's traffic flow through peak traffic rates, attack signatures and packet inspection techniques. These techniques involve protocols, IP addresses, port numbers and other data which helps identify and drop malicious DDoS attack traffic.

Under normal operating conditions customers' traffic will flow to/from the Internet via the most direct path across Transworld's IP backbone.

ATTACK DETECTION AND SERVICE ENABLEMENT

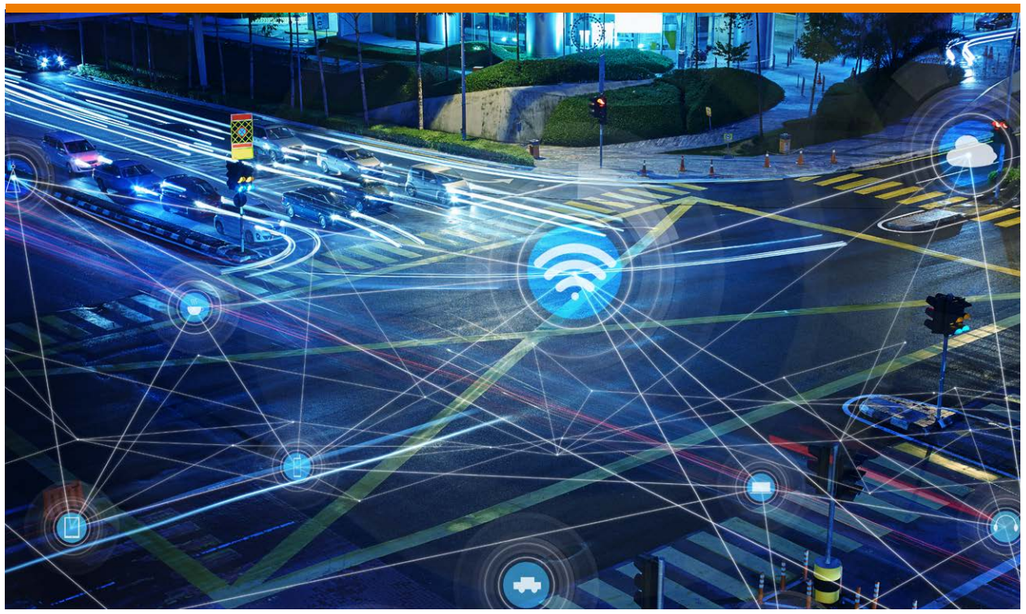
Transworld offers two types of DDoS Mitigation services:

- *On-Demand service option* - "On-Demand" service option – requires the customer to call into the Transworld Technical Assistance Center to request mitigation.
- *Always-On service option* – for prefixes that are permanently advertised, customer traffic constantly monitored for any attack and diverted automatically -towards the scrubbing network for mitigation.

  (Note: This does not require the customer to call into the Transworld Technical Assistance Center to request Mitigation.)

- 24 x 7 management and monitoring via Operations Center
- Access to performance and event reporting with online attack reports and historical data for Volumetric and application layer attack mitigation
- Mitigates against known forms of layer 3-7 attacks
- 15 to 30 minute time to Mitigate for most known forms of attack for On-Demand service option
- 5 to 15 minute Time to Mitigate for most known forms of attack for Always-On service option

When DDoS Mitigation has been enabled, a customer's traffic is redirected through Transworld's IP backbone so that it flows through our DDoS Mitigation Platform. The customers traffic flow is analyzed using complex filters to detect network layer anomalies that could be associated with a high bandwidth 'flood' attack or 'cloaked' application layer attacks. Once detected the malicious traffic is discarded by the Attack Mitigation System in our IP backbone where there is plenty of bandwidth without interrupting the flow of legitimate traffic destined for a customer's Internet port.



Mitigation Procedure

ON-DEMAND SERVICE OPTION

If Transworld detects a volumetric attack, we will contact the customer's designated authorized person to advice that an attack is occurring and confirm if it is acceptable to enable DDoS Mitigation.

From opening a trouble ticket DDoS Mitigation is enabled within 30 minutes. Once enabled a customer's traffic is redirected through the TMSs in our IP backbone.

Mitigation will remain in place for 24 hours. If at the end of that timeframe:

- **Attack persists** – the mitigation will remain in place for another 24 hours. If attack continues, customer affected IP will be black-holed.
- **Attack has ceased** – the mitigation will be removed, customer's traffic returned to normal path, and the customer will be notified by email.

ALWAYS-ON SERVICE OPTION

Customers have their mitigation permanently enabled to their prefixes which means that they want to be permanently monitored and automatically re-routed towards the mitigation infrastructure in case of DDoS attack.

Reporting

Post-attack reports are available on request that will provide the customers with a per attack summary and attack statistics.

This will provide customers with a view of their traffic and associated attack statistics, including:

- Alerts Summary
- Attack Summary

Managed Objects

Transworld's DDoS Protection Service provides customers with protection against DDoS attacks based on IP addresses. These details are captured in a customer specific network-based software element on our DDoS Protection Service called a 'Managed Object'.

Each individual Managed Object can be configured to protect blocks of IP address.

Mitigation Terms

Customer can subscribe up to 5Gbps DDOS attack/malicious traffic per attack; clean traffic will be maximum subscribed bandwidth for any attack. Traffic will be mitigated up to the subscription and shall be automatically set for black-hole if subscription limit increases.

Attack on each /32 IP address will be treated as single attack instance. Customer may subscribe for single instance OR multiple simultaneous instances depending on commercial agreement.

Default duration for attack mitigation will be 24 hours which can be extended based on commercial agreement.

If customer subscribed capacity is exhausted, customer affected IP will be black holed.

Service Implementation & Support

Transworld's DDoS Protection Service is managed by our TAC on a 24x7x365 basis. The customer is not required to change any of their existing infrastructure to make the service operational.

DDoS attacks can occur very quickly and require a very fast response from Transworld's Operations teams.

NOTE: If at any point there is a risk that Transworld's own network could be compromised Transworld reserves the right to shut down the customer's port(s) until it is safe to reconnect the customer. This action could be undertaken whilst other measures are implemented (e.g. enabling black holing).

Key Benefits

- Customers Internet Service remains operational even when being attacked, maximizing the availability of the customer's website, on-line services and applications.
- Transworld's DDoS Mitigation discards malicious traffic within its IP backbone before it reaches the customer where it would do the most harm.
- Provides customers with a key service that positively contributes to a customer's business continuity planning (BCP) processes.
- Affordable insurance against the threat of DDoS attacks.
- Integrated with Transworld's Internet Services, all of which is managed by Transworld's TAC/NOC 24x7x365, providing customers with a single point of contact, management and accountability.
- Ensure business continuity by protecting access to critical resources.
- Improve network and application uptime.
- Safeguard customer experience and business reputation.
- Protect last-mile bandwidth and avoid costly overprovisioning.

Advantage

- Being a Tier-1 Internet Gateway Operator, Transworld is in a strategic position to monitor and effectively mitigate any DDoS attack against its Customers.
- Whilst 'black hole' routing is effective at protecting a site or data center, it can also achieve the same result as the DDoS attack because it blocks all traffic, good and bad.
- Premise-based devices leave last-mile bandwidth vulnerable, TWA DDoS service removes attack traffic within TWA's IP Core before forwarding the clean traffic to customer.
- Lower total cost of ownership against premise-based solutions

Conclusion

The threat to availability represented by DDoS attacks cannot be overlooked. No business continuity plan is complete without taking into account the need to maintain the availability of critical online data. Customers can now successfully detect, classify and mitigate DDoS attacks with TWA's anti-DDoS solutions.

Given today's threat landscape, companies simply cannot afford to disregard these solutions as part of their business continuity and risk management planning. The risk is too severe.

Sources:

1. Interroute.de 2. Incapsula.com 3. SatteliteToday.com 4. Arbor.com