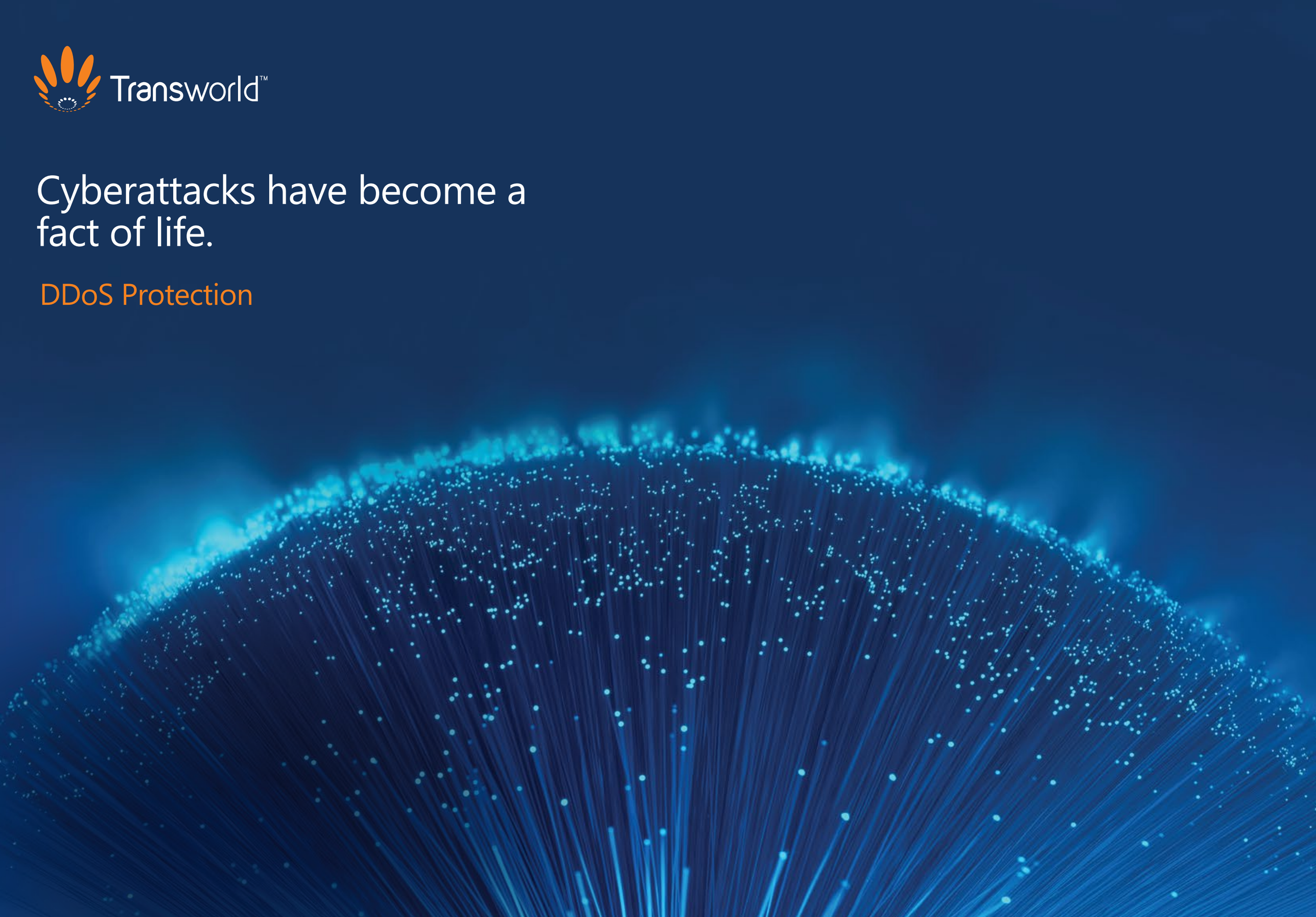
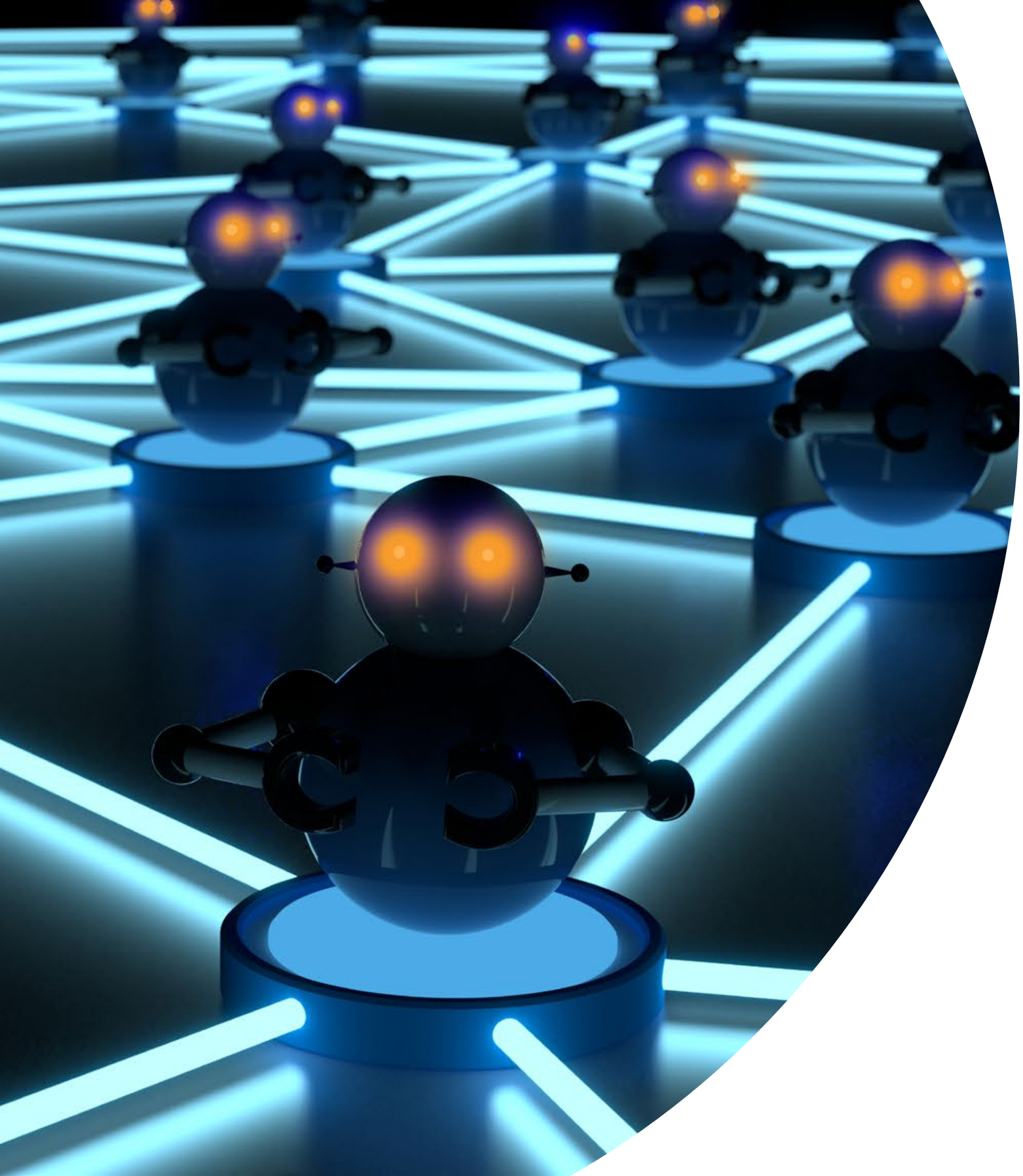
Transworld™

Cyberattacks have become a fact of life.

DDoS Protection



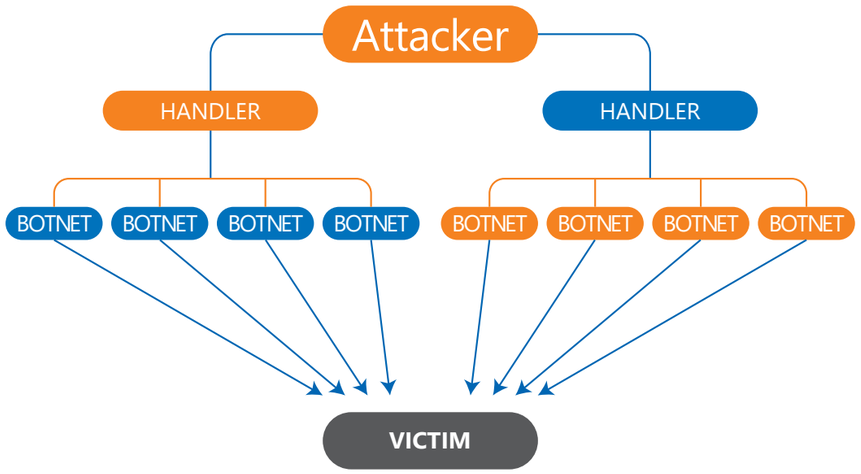


Transworld
DDoS Protection Service

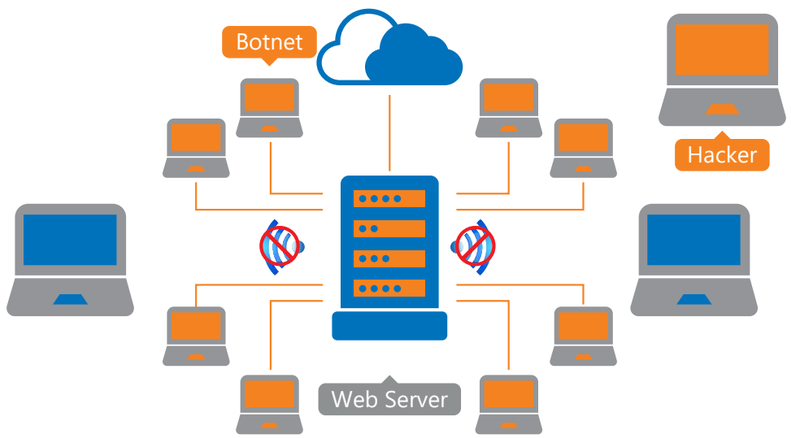
Any business entity that uses the Internet for its core business can no longer do business if their operations are down. This results in revenue loss. Some types of online businesses and financial institutions are more prone to DoS/DDoS attacks than others. However, everyone recognizes that without a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

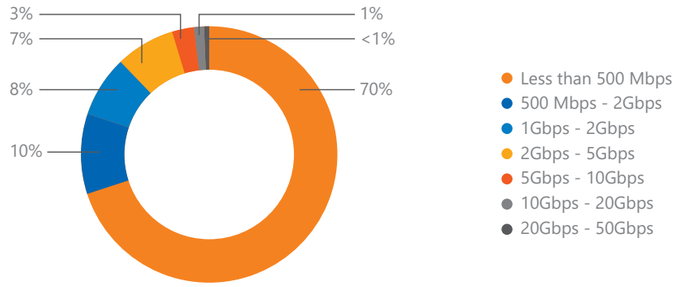
Application Layer DDoS Attacks

- 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.

Breakup

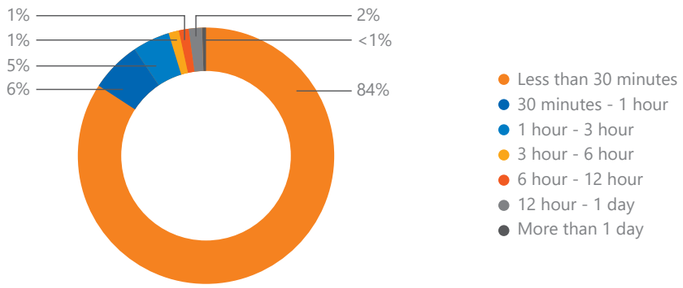
Attack Size Breakup

- 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.



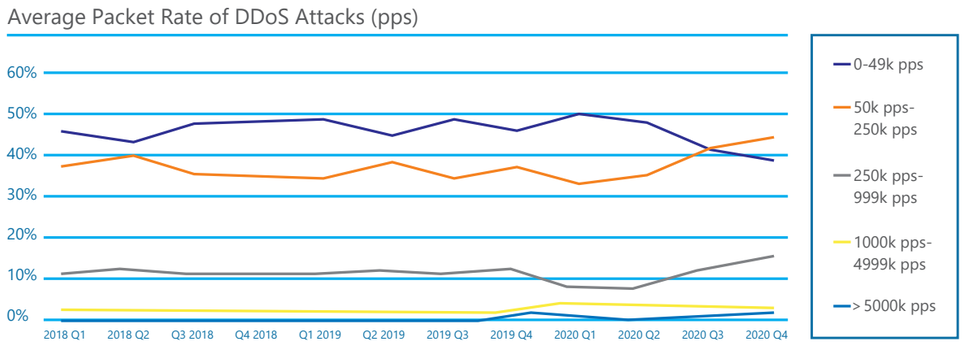
Attack Duration Breakup

- 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.

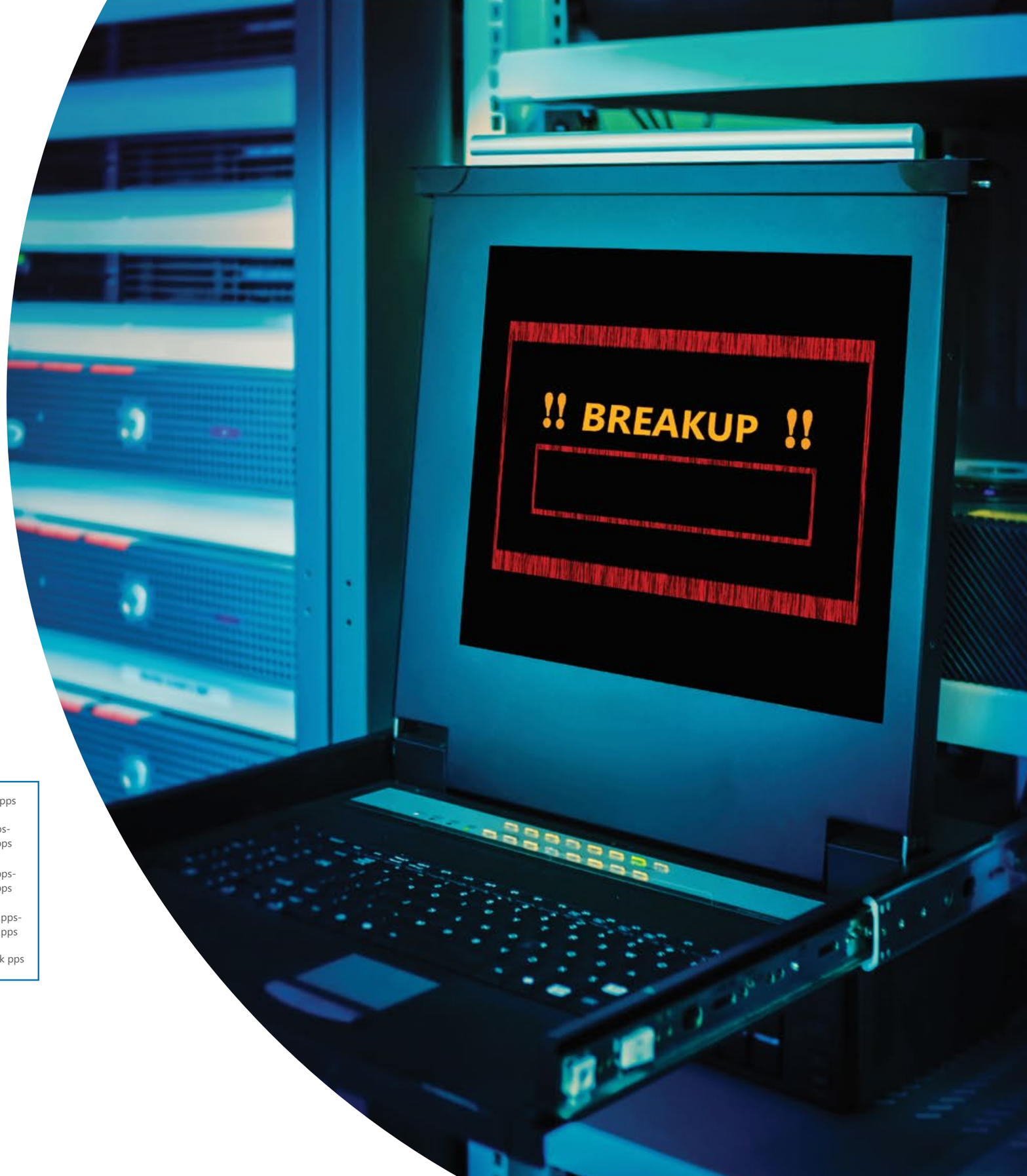


Key Trends

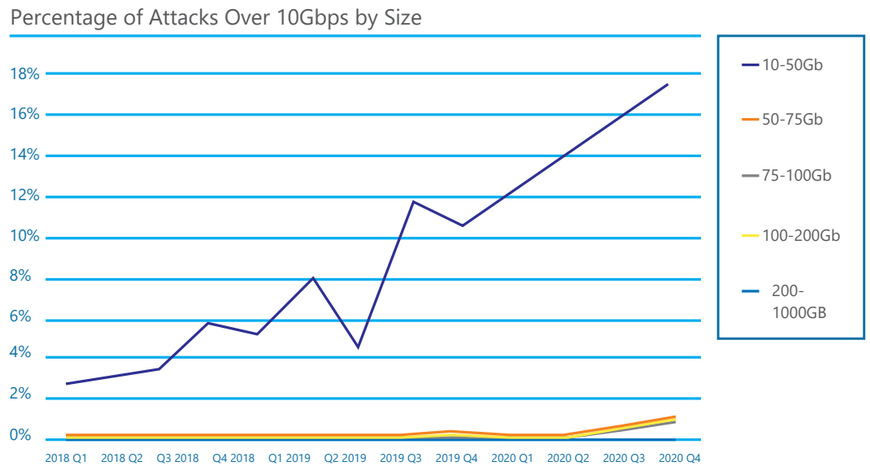
High Packet Rate Attacks on the Rise



17% increase in High Packet Rate Attacks

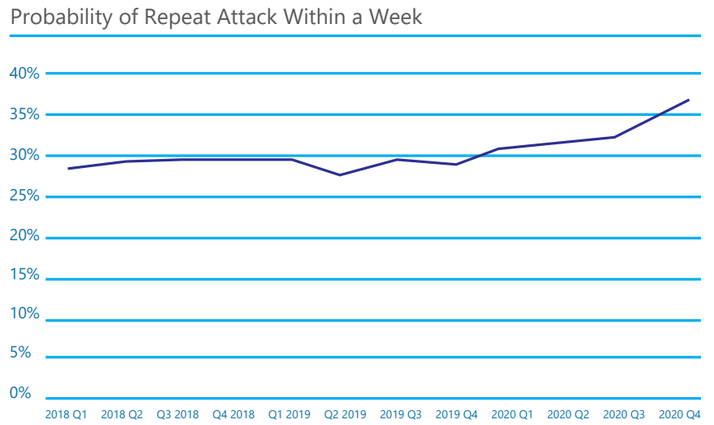


Increase in Attacks over 10Gbps



70% Growth in Attacks over 10Gbps

Increased Chance of Repeat Attack



68% Increased Probability of Repeat Attack within a Week

Challenge

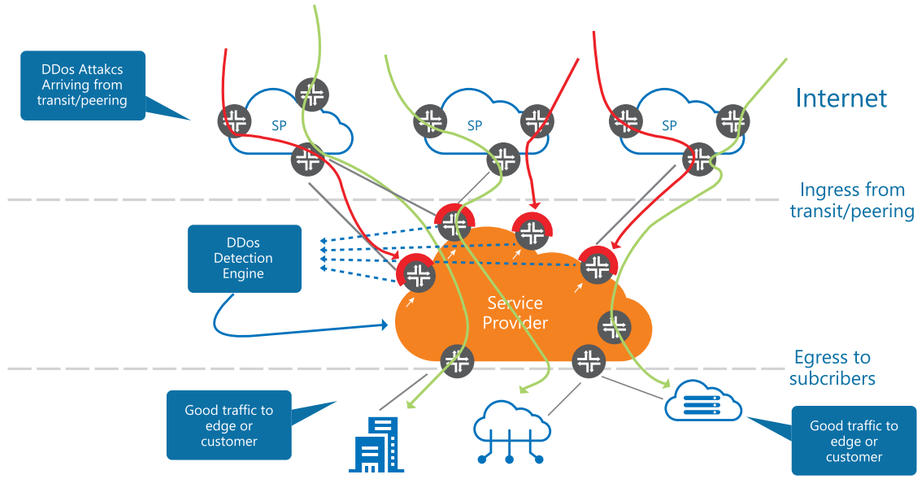
DDoS attacks are a significant part of today's threat landscape, and they continue to grow in magnitude, frequency, and sophistication. It is no longer feasible to address this growing problem with traditional out- of-band scrubbing centres and manual intervention on approaches.

Our Solution

TWA has acquired a revolutionary SDN based new defense against DDoS attacks. This unique SDN solution delivers line-rate detection and mitigation in real time at very large scale by leveraging always-on packet-level monitoring, AI analysis, and infrastructure-based enforcement. TWA has partnered with Juniper to provide this state-of-the-art DDoS defense SDN technology.

How it works

The solution represents a breakthrough in real-time volumetric DDoS defense offering unparalleled system capacity, security, and performance, scalable to tens of terabits of volumetric monitoring and mitigation.
The works together with TWA's routing platforms to filter out DDoS attack traffic at the edge of the network before even reaching TWA's infrastructure and the customers' network.
The solution offers a highly scalable monitoring capacity, and a mitigation capacity of 50 Gbps for enterprise customers and up to 200 Gbps for carrier customers. As an industry best practice, customer mitigation will be done up to the customers subscribed capacity.
The service is designed on what is termed as software defined network edge defense and works as follows.



DDoS detection engine continuously monitors traffic from all ingress points and if an attack is detected, the malicious traffic is removed right at the edge of the network in a distributed fashion. The benefits of inspecting traffic at the packet level with the power of infrastructure-based enforcement, enables real-time, automatic mitigation of DDoS attacks within seconds.

Benefits

- Removes malicious traffic at the network edge, the points where malicious traffic enters the network.
- Automates responses to stop DDoS attacks in seconds.
- Improves visibility with always-on packet-level monitoring, delivering detailed actionable intelligence before, during, and after an attack.
- Scalability to tens of terabits of volumetric monitoring and mitigation as the network expands.
- Packet-level inspection for accurate volumetric DDoS detection
- Automatic altering via machine analysis, for intelligent mitigation
- Closed-loop feedback to eliminate false positives.
- Unparalleled system capacity, density, security, and performance
- Industry- first inline data plane security with no compromise in throughput performance.

Transworld DDoS Reliability

- 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 24/7, 365 days a year, providing customers with a single point of contact, management and accountability.
- 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 centre, 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 Edge before forwarding the clean traffic to customer.
- Lower total cost of ownership against premise-based solutions.

UK
GERMANY
FRANCE
ITALY
TURKEY
EGYPT
SAUDI ARABIA
YEMEN
DJIBOUTI
OMAN
U.A.E
IRAN
AFGHANISTAN
CHINA
PAKISTAN
JAMMU & KASHMIR
Torkham
Islamabad
KPK
Lahore
PUNJAB
BALUCHISTAN
Gwadar
Karachi
SINDH
INDIA
BANGLADESH
MYANMAR
SRI LANKA
MALAYSIA
SINGAPORE
INDONESIA

Legend

- TW1 Cable System (Self Owned)
- SEA-ME-WE-5 (Consortium Cable)
- SEA-ME-WE-4 (Restoration)
- SEA-ME-WE-4
- MENA
- FLAG
- AAE 1
- TGN Gulf / Seacom
- Terrestrial Cable
- EIG
- Cable Landing Station
- Branching Unit
- Point of Presence (PoP)

Transworld™

Islamabad Office

Plot 24, Retalia Building G-6
Markaz, Islamabad.

T +92 (51) 2871623
U +92 (51) 111 111 891 (TW1)
F +92 (51) 2871625

Lahore Office

138 – CCA, Phase V,
D.H.A, Lahore.

T +92 (42) 35775105-7
U +92 (42) 111 111 891 (TW1)
F +92 (42) 35775108

Karachi Office

Dolmen City (Executive Tower)
6th Floor, HC-3, Block 4, Marine
Drive, Clifton, Karachi.

T +92 (21) 35824951-4
U +92 (21) 111 891 891 (TW1)

111 111 891 | www.tw1.com