MANAGED SECURITY SERVICES : MULTI-LAYER DDOS

DETECT, PROTECT AND THRIVE

SHIELD YOUR IT SETUP AND YOUR BUSINESS AGAINST DDOS ATTACKS

Distributed Denial of Service (DDoS) attacks have become more common — and more sophisticated. Hybrid DDoS detection systems are now essential if you're to effectively protect your enterprise from this new wave of threats.

- Deal with multi-layer attacks — with seamless integration of cloud and on-premise DDoS protection
- Keep internet-facing applications running — with proactive protection
- Stay safe from global botnet threats — with attack countermeasures
- Stay one step ahead — with real time security updates
- Take control of your IT — with immediate forensics and attack reports

SAFEGUARD YOUR APPLICATIONS AND YOUR BUSINESS

Sophisticated Distributed Denial of Service (DDoS) attacks are now targeting multiple layers of the enterprise. The most common attack targets the application layer, threatening critical applications like HTTP, HTTPS DNS, VoIP and SMTP. These attacks use less bandwidth than volumetric attacks and are harder to detect.

Meanwhile other attacks target servers and devices including firewalls, IPs and load balancers, exploiting their need for timely responses. A multi-pronged bombardment like this can put your enterprise at risk, threatening loss of revenue, lower productivity and even a tarnished reputation.

A POWERFUL PARTNERSHIP TO DELIVER MULTI-LAYERED PROTECTION

TATA COMMUNICATIONS

ARBOR NETWORKS
The Security Division of NETSCOUT

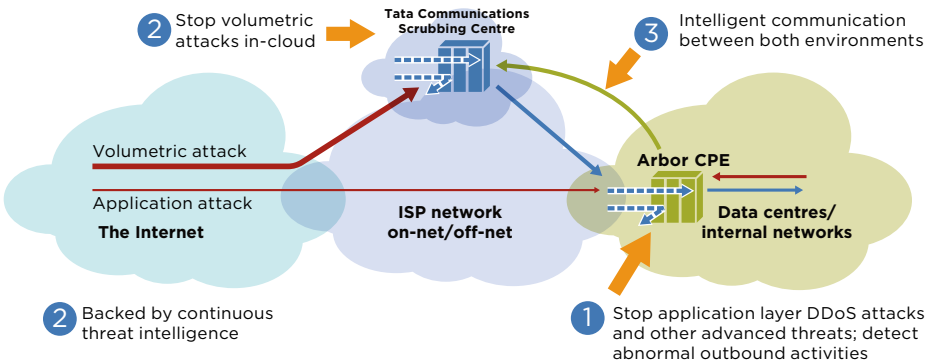
Tata Communications and Arbor Networks have together introduced a multi-layered DDoS protection solution that defends you from complex application layer attacks. By adding Tata Communications' cloud-based technology to Arbor's on-premise device, the architecture delivers real-time detection and mitigation, protecting critical assets like the data centre and using cloud signalling to raise the alarm during a volumetric attack.

The solution only blocks malicious traffic, while legitimate traffic continues to flow as normal. Real-time security updates, forensics and attack reports bring you more control over how you respond to attacks than ever before.

WITH THE STRENGTH OF ARBOR NETWORKS

- **Out-of-the-box protection:** Availability Protection Systems (APS) detect and block DDoS threats in real time
- **Full suite of countermeasures:** To neutralise the vast majority of global botnet threats
- **Encrypted SSL/TLS flood mitigation:** A FIPS compliant SSL decryption module comes built in with APS, to battle SSL-based encryption attacks
- **Real-time threat updates and forensics:** visibility over 120 Tbps of the world's internet traffic means we can provide timely, automatic security updates to keep you one step ahead — while attack reports and forensics detail attacks and trends

LAYERED DDoS ATTACK PROTECTION



"SLA-backed DDoS detection and mitigation is available globally with regional scrubbing facilities deployed across the Tata Communications' backbone. This is arguably the leading provider of DDoS mitigation services in Asia with very large server farm capacity for data scrubbing, and SLAs providing less than 30ms throughput delays."

– CURRENT ANALYSIS

HARNESS THE POWER OF TATA COMMUNICATIONS' CLOUD

- **Protect last-mile bandwidth —** with a network-based defence that removes attack traffic on Tata Communications' global IP backbone
- **Optimal protection —** Cloud Signalling™ functionality connects the on-premise APS device with the cloud-based Tata Communications solution
- **Minimal latency and high availability —** thanks to a wide network of 21 scrubbing farms on Tata Communications' network
- **Handle any amount of attacks —** irrespective of the source location, our scrubbing farms are never more than one AS hop away
- **Fully managed by us —** with certified and experienced security professionals monitoring and managing client services 24/7/365

For more information, visit us at www.tatacommunications.com

Contact Us | **Share**