NETSCOUT®

Global Logistics Company Prevents DDoS Attacks While Ensuring Worldwide Package Delivery, Despite Pandemic Onslaught

The Situation

One of the largest transportation and logistics companies in the world with locations in multiple countries and territories worldwide, delivers over 1.3 billion parcels per year and has over 300,000 employees throughout the world.

This organization had historically used multiple service providers to protect their globally distributed datacenters, depending on the regional availability of such services from the providers. They contacted NETSCOUT® in 2019 to help them simplify their DDoS mitigation infrastructure by replacing the different service providers with one single provider-agnostic service that could also cover all global locations. This enabled them to have a single SLA with 1 company rather than the multiple provider option, which was extremely difficult, complex and expensive to manage. In times of attack, an organization

needs clarity and a consistent platform to protect themselves rather than different SLA's with multiple vendors in all locations. Overall, the NETSCOUT Arbor Cloud™ Service was less expensive than the combined multi-Service Provider solution, and with one single point of contact for delivery of the service plus the mitigation of attacks, they moved to NETSCOUT with confidence. Simply put, they found Arbor Cloud to be the preferable solution in the market.

The Details

The company fell victim to a series of complex targeted DDoS attacks at the end of December 2019 which spilled over into January 2020. A particular application service was impacted so much that it threatened to halt all the of the company's flights from taking off worldwide affecting all packages to be delivered.

They engaged with the NETSCOUT Account team and NETSCOUT was able to offer immediate cover with NETSCOUT Arbor Cloud. NETSCOUT Arbor Cloud SOC (Security Operations Center) reacted in "emergency mode" and mitigated the attacks.

On the heels of that attack and primarily due to the COVID-19 pandemic, they then recognized an increase in VPN traffic because of employees working from home accessing internal applications via VPN. So now their newly refreshed Arbor Product Portfolio needed an upgrade to manage the escalation in traffic. So, they added 6 x AED 2600s, 2 x 2800s and Cloud services to cope with the bandwidth overload. In addition, NETSCOUT provided a subscription license model for their AED and Cloud portfolio to ease the short-term pain in a cost-effective fashion.

The Results

The increased DDoS management and mitigation capacity provides the organization and their employees using VPN the confidence that they will be protected from DDoS attacks that can disrupt their business activity and even damage the organization's reputation while temporarily working from home. The organization was pleased with the flexibility of the AED license configuration and the ability of NETSCOUT to execute on a global procurement effort quickly and to the organization's crisis timeline.

> Due to NETSCOUT's flexibility in licensing, global presence and ability to react swiftly, the customer was able to meet their crisis goals quickly and efficiently.

SECURITY

Intelligently Automated, Best Practice Hybrid DDoS Protection, Backed by Global Visibility and Threat Intelligence

The facts are clear – DDoS attacks continue to rise in size, frequency and complexity. Modern-day DDoS attacks are a dynamic combination of:

1. Volumetric
2. TCP State Exhaustion
3. Application-layer attack vectors

Industry-best practice for DDoS defense is a multi-layer, or hybrid approach that takes into account the different types and targets of DDoS attacks. Just as important, the solution must have an intelligent form of communication between these two layers backed by up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks.

In-Cloud Protection

Arbor Cloud™ is an ISP agnostic, in-cloud, fully managed DDoS Protection service. Employing 14 scrubbing centers located throughout the US, Europe and Asia, Arbor Cloud provides over 11 Tbps of global mitigation capacity. Enterprises can seamlessly integrate their on-premise Arbor Edge Defense (AED) protection with Arbor Cloud to obtain comprehensive DDoS attack protection. Service Providers can also use Arbor Cloud for extra mitigation capacity and expertise.
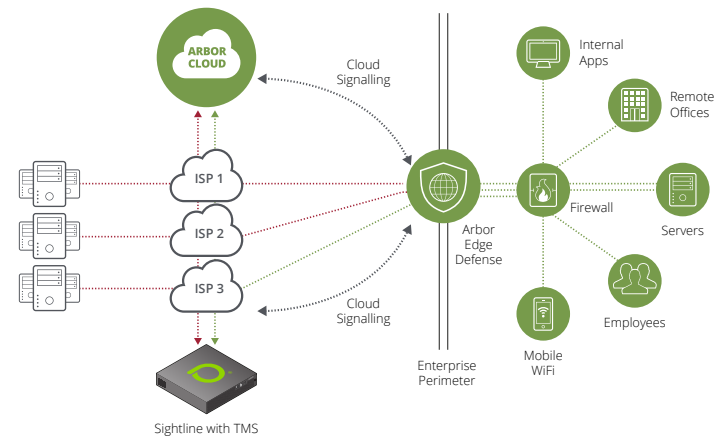
On-Premise Protection

For larger networks and more experienced DDoS attack mitigation teams, Arbor Sightline and Arbor Threat Mitigation System (TMS) provide pervasive network visibility and DDoS attack detection. Upon attack detection, Arbor Sightline can automatically re-route attack traffic to the Arbor TMS for surgical mitigation of all types of DDoS attacks. For smaller networks, Arbor Edge Defense (AED) is an always-on, in-line, DDoS attack detection and mitigation solution which can stop inbound DDoS attacks. For larger DDoS attacks, AED's Cloud Signaling™ will intelligently link to Arbor Cloud.

Global Visibility and Threat Intelligence

Arbor Security Engineering & Response Team (ASERT) leverages a 20-year, worldwide deployment of Arbor products and third-party intelligence – otherwise known as ATLAS® – to gain unmatched visibility into global threat activity. The global insight derived from ATLAS/ASERT continuously arms all Arbor products and services in the form of features, integrated workflows and the ATLAS Intelligence Feed (AIF).

Arbor Products	
Arbor Cloud DDoS Protection Products and Services	• A fully managed, tightly integrated combination of in-cloud and on-premise DDoS protection. • 24/7 managed DDoS protection with 14 scrubbing centers around the world providing over 11 Tbps of mitigation capacity.
NETSCOUT Arbor Edge Defense	• Always-on, in-line, detection and mitigation of DDoS attacks ranging from sub 100 Mbps to 40 Gbps. • Can stop inbound and outbound DDoS attacks, malware, and C2 communication.
Arbor Sightline & Threat Mitigation System (TMS)	• Arbor Sightline provides pervasive network visibility and DDoS attack detection. • Arbor TMS provides out-of-path, stateless, surgical mitigation at up to 400 Gbps per 2U device.
Arbor Sightline with Sentinel	• Intelligently optimize mitigation based on infrastructure capability to block attacks in the most efficient and scalable way. • Share attack data and request mitigation help from other networks. • Detailed reporting to see exactly what is being dropped, where, and why.

NETSCOUT®