# Mitigation at the Edge, Reducing Cost and Risk

When it comes to DDoS, network operators have traditionally deployed mitigation infrastructure at a few key peering points and data centers. They 'diverted' traffic towards these locations for customers or infrastructure under DDoS attack. This is changing in some networks, with a clear push toward mitigating attacks earlier, at the network edge. Usually, this means combining intelligent mitigation and infrastructure mechanisms, so that any given attack can be mitigated efficiently and effectively.

## Challenge

Network architectures have changed as operators drive to improve customer service while reducing cost and complexity. ISPs are pulling content into their networks at the edge, deploying caches, and minimizing the number of hops content traverses within their networks. And, they are doing the same with value-added service infrastructure – pushing it nearer to the customer. These shifts in architecture make the idea of back-hauling attack traffic across the network to centralized mitigation infrastructure much less practical.

At the same time, many network operators are now experiencing multiple, concurrent large-scale attacks on a daily or weekly basis. The number of attacks has increased dramatically with 16% growth in frequency between 2018 and 2019. In 2019 alone, NETSCOUT® monitored 8.4 million DDoS attacks. That's 23,000 attacks per day or 16 per minute.

Back-hauling DDoS traffic for multiple large, concurrent attacks across the core for cleaning is no longer considered ideal, as it can result in congestion and service interruption, leading to poor or inconsistent customer experience.

## Risk

Changes in network architecture, increases in traffic levels and network utilization, and the increased frequency of DDoS attacks all pose risks to a consistent user experience. Some OTT service providers even publish metrics ranking network operators based on their ability to deliver their OTT services.

Poor or inconsistent customer experience drives customer churn, a major threat to revenue stability and growth for network operators of all types.

## Solution

Arbor's Sightline and Sentinel provide automated DDoS attack detection in as little as 1 second. Arbor Sightline provides multiple mechanisms to identify DDoS attacks of different types and provides detailed attack classification, traceback, analysis and forensics data within its user interface. Arbor Sightline's DDoS detection capabilities are trusted by most of the largest network operators around the world.

Many of the routers and switches network operators have deployed support BGP Flowspec. This technology allows a packet filter or rate-limiting rule to be advertised over BGP, the routing protocol used to control Internet traffic. Flowspec is a very scalable way of mitigating DDoS attacks. It leverages network infrastructure, where the attack traffic can be described succinctly using network layer parameters e.g. IP addresses, ports, packet sizes, etc. However, not all routers and switches implement Flowspec in the same way, especially when it comes to feature support and scale. Furthermore, Flowspec cannot mitigate all attacks, especially those that are sophisticated.

Intelligent mitigation is required to mitigate sophisticated attacks. The Arbor Threat Mitigation System (TMS) provides intelligent traffic inspection and DDoS mitigation for volumetric, state-exhaustion and application-layer attacks.

In order to mitigate sophisticated attacks as effectively and efficiently as possible and as near to their network entry point as possible, network operators need to combine mitigation mechanisms. Doing this requires both an orchestration capability and a flexible, software-only business model to facilitate the deployment of Arbor TMS at the network edge as either a dedicated appliance or running virtually in the edge router. Arbor Sightline With Sentinel provides the automation, orchestration and management of the mitigation mechanisms and collates the results via comprehensive reporting in one simple interface.

Moving beyond this, Arbor Sightline With Sentinel also enables network operators to collaborate, allowing them to share attack information so that attacks can be mitigated across network boundaries, again with feedback being exchanged. This allows for trusted coordination between organizations and provides the robust reporting and accountability that enable these DDoS peering arrangements.

## Summary

Arbor Sightline With Sentinel provides network operators with a single-pane-of-glass overview for network monitoring and reporting, threat detection and mitigation. It automates and orchestrates intelligent, infrastructure and inter-network mitigation capabilities, delivering the next-generation of DDoS protection for next-generation networks.

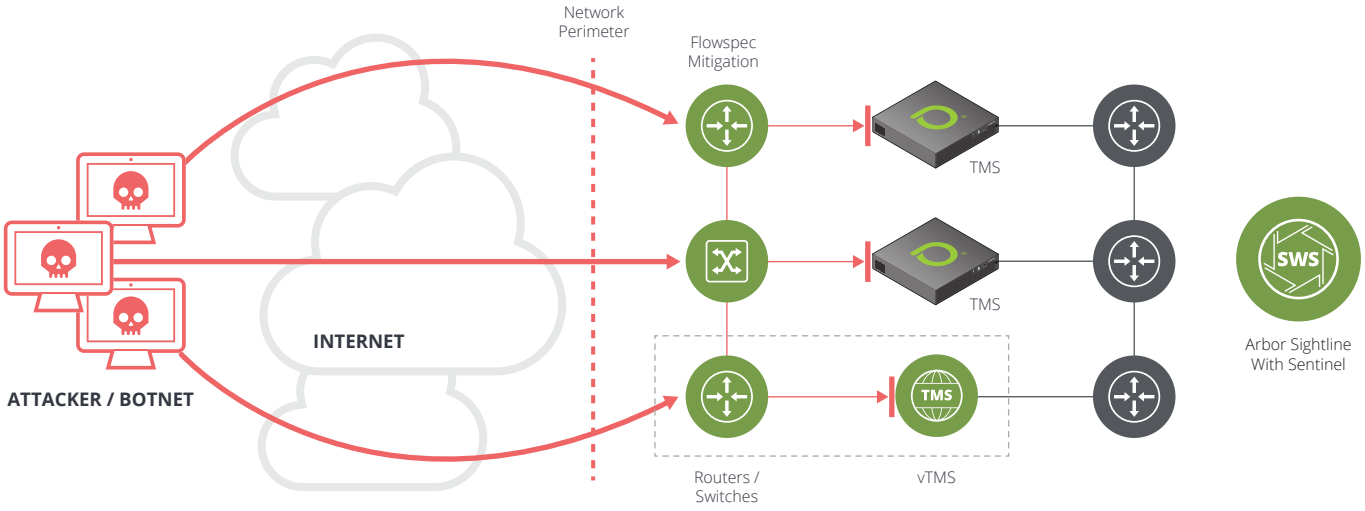


**Figure 1: Arbor Sightline With Sentinel, Mitigation Without Borders.**

NETSCOUT

**Corporate Headquarters**
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

**Sales Information**
Toll Free US: 800-309-4804
(International numbers below)

**Product Support**
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us



SECUC_004_EN-2002 05/2020