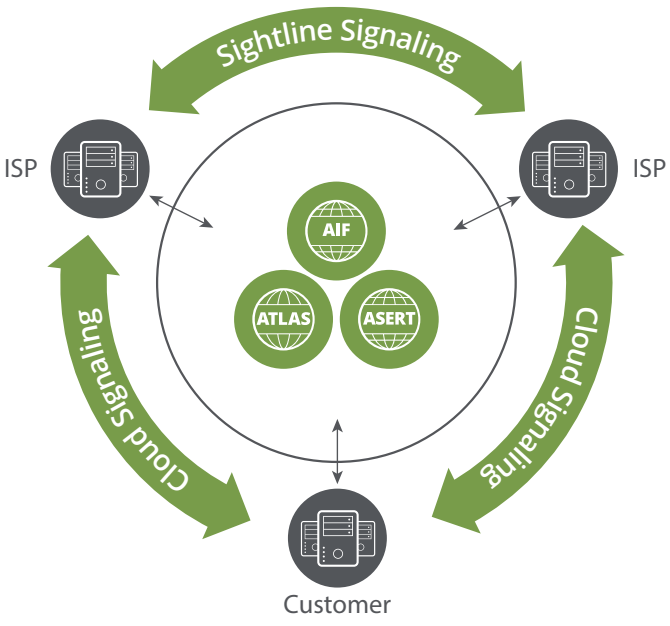
Service Provider Collaboration

DDoS attacks are rising so much that for the first time in history, the annual number of observed DDoS attacks crossed the 10 million attack threshold, with NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) seeing 10,089,687 attacks over the course of 2020. Furthermore, as the pandemic lockdown took effect last spring, cybercriminals launched 929,000 DDoS attacks in May, the single largest number of monthly attacks we've ever seen.



The Challenge

These increases in DDoS attacks have impacted how Internet Service Providers (ISP) think about DDoS and how they can assist their customers plus collaborate with other ISPs both upstream and downstream in mitigation efforts since they are closer to the source of the attacks and see the traffic first.

Plans such as 'Flowspec Peering' between tier-1 US operators, and the Internet Engineering Task Force's (IETF) DDoS Open Threat Signaling (DOTS) program attempted to develop collaboration programs that require installing provisioned infrastructure or sharing attack data to a central database. These programs uncovered the reluctance in the industry to install infrastructure or share data. Most of the reluctance came from the executive suite based on the business decisions. Initiatives like this though, demonstrate that the whole industry wants to fight DDoS together.

The Collaboration

Dealing with this level of attack should not fall on the backs of the ISPs alone but requires collaboration among all stakeholders in the battle against DDoS attacks. NETSCOUT® has been a trailblazer in efforts to coordinate DDoS protection and collaboration within our customer ecosystem. For over 20 years, NETSCOUT's Arbor DDoS defense products have been deployed in a majority of the world's ISPs and many enterprise networks. Arbor DDoS protection products enable collaboration amongst ISPs and their customers to fight the global threat of DDoS attacks together. This collaboration falls into three categories.

1. ISP-to-ISP Collaboration
2. Customer-to-ISP Collaboration
3. Sharing of Threat Intelligence

ISP-to-ISP Collaboration

To assist with attack collaboration among ISPs, NETSCOUT's Sentinel provides a unique, fully integrated, internetwork-signaling mechanism called Sightline Signaling, which allows network operators to share attack attributes and coordinate defenses spanning network boundaries ultimately enabling their peers to collaborate at an unprecedented level to collectively stop DDoS attacks nearer their source. Our Sightline Signaling feature in Sentinel provides the similar capabilities to the risky and clunky Flowspec peering efforts but in a safe, automated way. One ISP may see DDoS traffic that is attacking their network customers but originates or passes through an upstream ISP. They can then signal the upstream ISP through Sentinel to alert them that the identified attack traffic is coming through their network while providing attack details and attack countermeasures.

Customer-to-ISP Collaboration

To assist with Customer-to-ISP collaboration, NETSCOUT's Arbor Edge Defense® (AED), which is deployed on the customer premises, provides a Cloud Signaling feature so customers can share attack attributes with their upstream ISPs. The upstream providers can use the identified attack attributes to create countermeasures within their systems and further share those countermeasures with their peers. The Cloud Signaling feature can also coordinate collaboration from the on premise AED with cloud DDoS services to knock down volumetric attacks closer to their source.

Sharing of Threat Intelligence

To help feed the ecosystem and the DDoS defense community as a whole, both Sightline and AED deployments send anonymous attack stats back to NETSCOUT's ASERT and ATLAS® (Active Threat Level Analysis System), providing information about observed DDoS attacks and other forms of cyber threats experienced by these organizations. No one has the global-threat-intelligence presence that NETSCOUT employs to provide awareness for our customers and the DDoS protection community as a whole. This awareness is generated through Omnis® Threat Horizon, Threat Reports, Blog Posts, Threat Advisories and a continuous feed of Threat Intelligence that arms all Arbor DDoS protection products.

- **Omnis Threat Horizon** – A global cybersecurity situational awareness platform, NETSCOUT's Omnis Threat Horizon provides highly contextualized visibility into global-threat-landscape activity that's tailored for each organization's specific vertical and geographic profile.
- **Threat Reports** – NETSCOUT's bi-annual Threat Intelligence Report offers our customer unique insight into worldwide DDoS attack activity and other cybersecurity threats.
- **ASERT Blog** – ATLAS Security Engineering and Response Team engineers and researchers are part of an elite group of institutions that are referred to as 'super remediators' who represent the best in information security. This team delivers world-class network security research and analysis for the benefit of today's enterprise and network operators via a number of vehicles none more accessible than the ASERT Blog.
- **Threat Advisories** – If something that ASERT deems important or dangerous to our customer's networks, cloud or on-premise, we will issue advisories to them related to identification and mitigation.
- **ATLAS Threat Intelligence Feed** – This data can also be returned back to the customer ecosystem in the form of the ATLAS Intelligence Feed® (AIF). The AIF arms the Arbor DDoS protection products with highly curated and current threat intelligence that enables customers to protect themselves from the latest DDoS and other cyber threats.

Summary

As the global DDoS threat landscape grows and attacks become more frequent and complex, worldwide network operators, their peers and their customers have to adapt to meet the new requirements for identification and mitigation of these new attacks. Collaboration between all of the Internet entities looking for protection against these global attacks is the key to this adaptation.

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_016_EN-2103 09/2021