NETSCOUT®

Arelion Employs NETSCOUT Arbor DDoS Protection Products

This Ensures Its Global Customers With Secure Access to Arelion's #1 Ranked Global Internet Backbone

## OVERVIEW

The Challenge

Improve the efficiency of network security across the #1-ranked global Internet backbone, empowering enterprise and Internet Service Provider customers with resilient, high-performance connectivity services.

The Solution

- NETSCOUT® Arbor Sightline™
- NETSCOUT® Arbor Threat Mitigation System™ (TMS)
- NETSCOUT® Arbor Sightline with Sentinel
- NETSCOUT® Adaptive DDoS Protection
- NETSCOUT® ATLAS® Intelligence Feed (AIF)

The Results

An increase in network visibility that results in added protection for business-critical services, no matter whether it is at the largest service provider or a multi-homed enterprise.
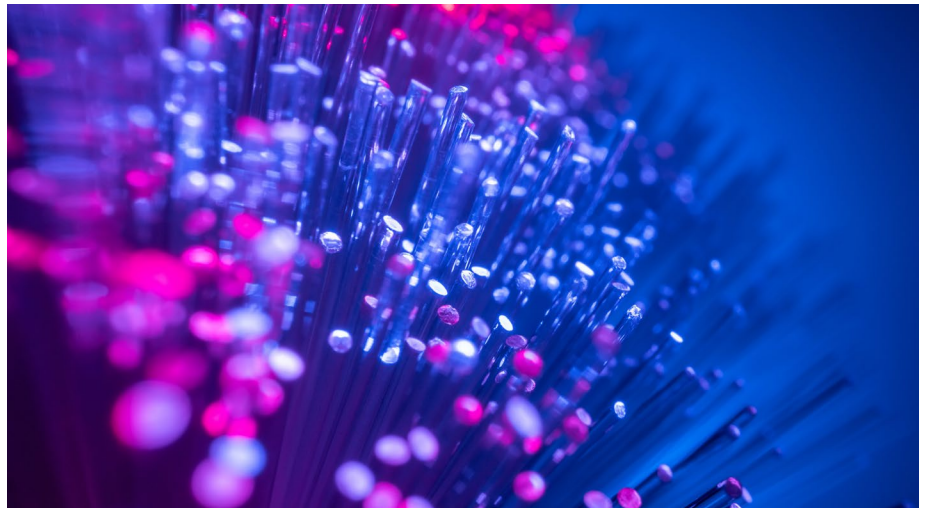
Introduction

Arelion operates the world's best-connected IP fiber backbone, providing high-capacity transit services to a variety of the globe's leading ISPs as well as many large enterprises. They provide an award-winning customer experience to clients in 129 countries worldwide, and their global Internet services connect more than 700 cloud, security, and content providers with low-latency transit. Furthermore, Arelion's private Cloud Connect service connects directly to Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud, and Oracle Cloud across North America, Europe, and Asia.

The Challenge

To get a clearer picture of their current DDoS protection infrastructure, Arelion reached out to NETSCOUT®, which had been providing DDoS protection with NETSCOUT Arbor Sightline and the Threat Mitigation System (TMS) for over 16 years. Arelion wanted a better understanding of the efficiency of the system and how it was bringing value to their internal security strategy as well as the protection services for their customers.

Once NETSCOUT provided the required information regarding the infrastructure and configuration of their current product portfolio, the project manager initiated a research activity to gain clarity on what new developments and solutions in the DDoS space could be implemented to enhance the DDoS protection of internal systems as well as the offering they provide to their customers. The goal for this action was to increase the efficiency of the DDoS protection both internally and for their customer base.

✳ Arelion

"As a Tier-1 Internet carrier supporting the majority of global Internet traffic, this continued collaboration reflects our ongoing investment in best-of-breed network security solutions to protect the technology ecosystem.

Our partnership combines Arelion's global network performance and NETSCOUT's leading Arbor DDoS attack protection solutions to provide world-class experiences for our customers."

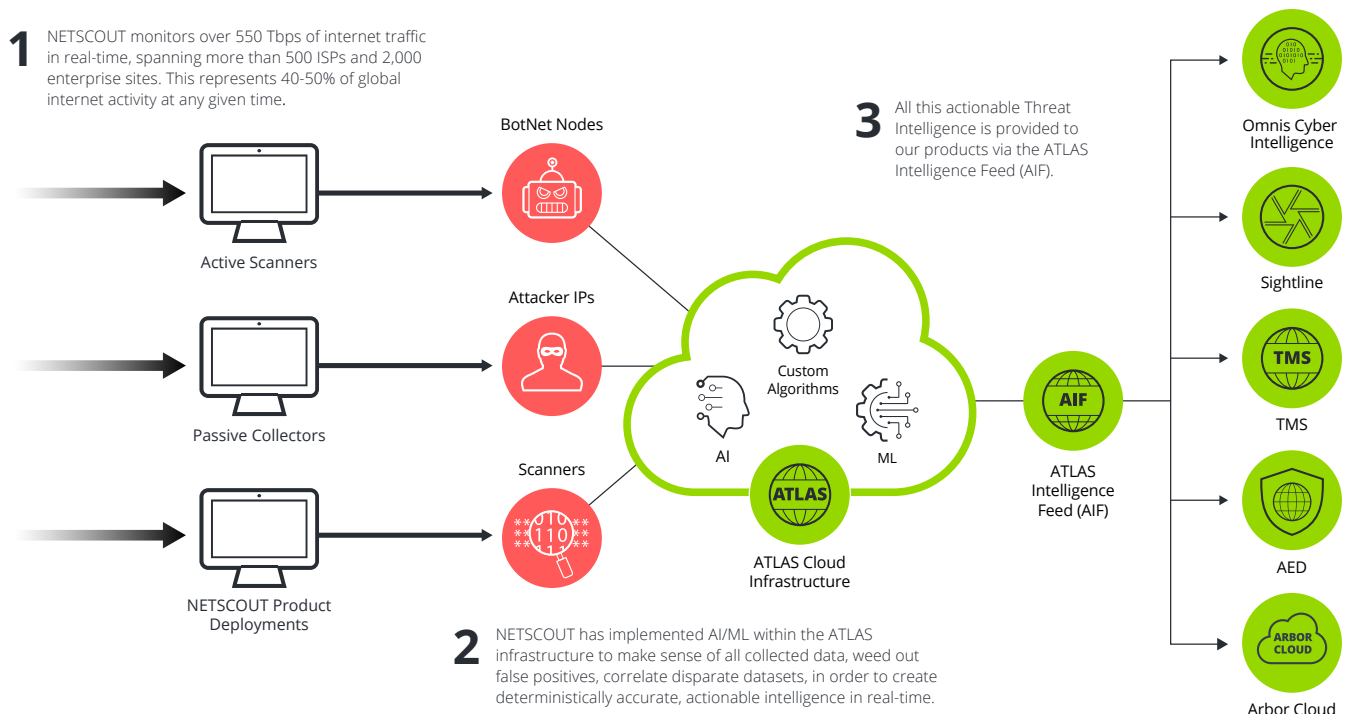Scott Nichols, Chief Commercial Officer at Arelion.

The Solution

Once Arelion completed its due diligence in the effort to gain more clarity around the current DDoS protection landscape, the NETSCOUT team initiated conversations regarding improvements in the NETSCOUT DDoS defense capabilities, including threat intelligence, mitigation orchestration, automation and reporting. The team also helped Arelion see the value that these capabilities could provide to their internal security teams, but more importantly, to their protection services customers. The NETSCOUT team introduced Arelion to three new offerings that provided the emphasized capabilities that they had identified during the discovery process to improve the DDoS protection for them and their customers.
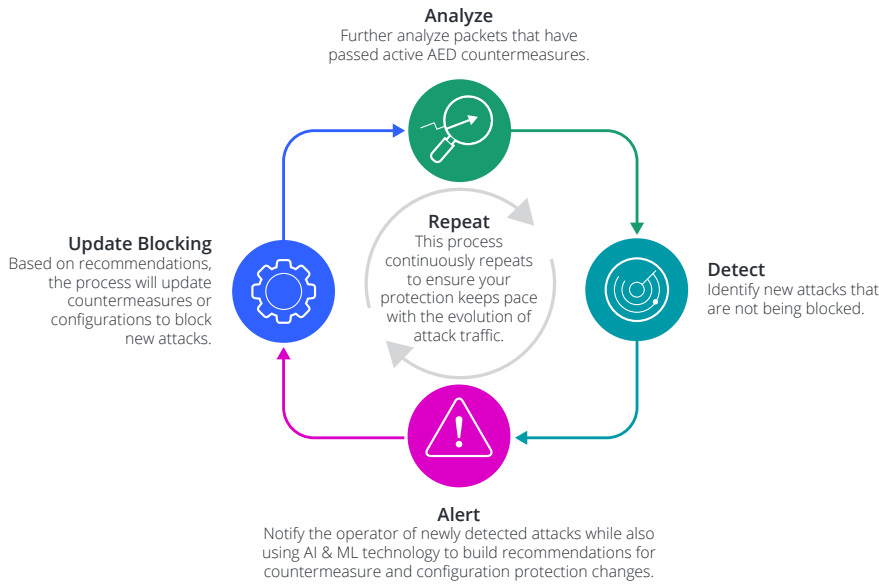
The first product introduced was an add-on to Sightline called Sentinel. Sightline with Sentinel understands the capabilities of the routers and other security devices in the security stack within Arelion's multi-vendor infrastructure and uses the capabilities of those devices (i.e., flowspec and other technologies) in combination with TMS to orchestrate defenses to automatically mitigate any DDoS attack, regardless of size and complexity, stopping them nearer to their source. This feature spreads

the mitigation load of large volumetric attacks over all potential system mitigation capabilities, lightening the load across the entire system.

The second offering NETSCOUT suggested was the ATLAS Intelligence Feed (AIF) for TMS. AIF taps into the best threat intelligence offered in the DDoS space, which provides deterministically accurate and actionable Threat Intelligence to enhance DDoS detection at every level of Arelion's network. As cyber threats continue to increase in frequency and sophistication, mature security teams will not only rely on the latest cybersecurity technology but also on the highly curated threat intelligence that arms these products. NETSCOUT's unmatched monitoring of over 50% of all internet traffic, our AI-powered analysis processes, and the expertise of NETSCOUT's ASERT Team have enabled NETSCOUT to automatically arm all NETSCOUT Arbor DDoS attack protection products with the latest DDoS attack tactics and methodologies, known sources of DDoS attacks, and Indicators of Compromise so organizations, such as Arelion, can protect themselves and their customers from DDoS attacks and other cyber threats and automatically adapt protections as those attacks change vectors.

1 NETSCOUT monitors over 550 Tbps of internet traffic in real-time, spanning more than 500 ISPs and 2,000 enterprise sites. This represents 40-50% of global internet activity at any given time.

Active Scanners

Passive Collectors

NETSCOUT Product Deployments

BotNet Nodes

Attacker IPs

Scanners

Custom Algorithms

AI

ML

ATLAS Cloud Infrastructure

3 All this actionable Threat Intelligence is provided to our products via the ATLAS Intelligence Feed (AIF).

AIF

ATLAS Intelligence Feed (AIF)

Omnis Cyber Intelligence

Sightline

TMS

AED

Arbor Cloud

2 NETSCOUT has implemented AI/ML within the ATLAS infrastructure to make sense of all collected data, weed out false positives, correlate disparate datasets, in order to create deterministically accurate, actionable intelligence in real-time.

AI & ML Powered Adaptive DDoS Protection Process

Analyze
Further analyze packets that have passed active AED countermeasures.

Repeat
This process continuously repeats to ensure your protection keeps pace with the evolution of attack traffic.

Update Blocking
Based on recommendations, the process will update countermeasures or configurations to block new attacks.

Detect
Identify new attacks that are not being blocked.

Alert
Notify the operator of newly detected attacks while also using AI & ML technology to build recommendations for countermeasure and configuration protection changes.

The Results

Arelion has experienced an increase in visibility into their network, meaning they can protect their internal systems and their customers' critical business applications and services against all types of attacks. This also gives them confidence in adopting all types of customers, no matter if it is the largest service providers or a multi-homed enterprise.

Overarching Benefit

Arelion believes that to provide proven and trusted DDoS protection to their customers, they needed to do two things. First was to partner with a world-class DDoS defense organization, and second was to project confidence in the chosen solution and strategy by employing it internally to protect their systems. The partnership with NETSCOUT and its proven DDoS protection products and threat intelligence provides Arelion and its customers with the confidence that their systems are protected by a best-of-breed DDoS-specific solution. Arelion customers value their services more because of the trust they have in the collaboration between Arelion and NETSCOUT.

The third offering NETSCOUT suggested, Adaptive DDoS protection (ADP), adds significant automation and targets newly detected attacks that require changes to configurations to mitigate. Once an attack is detected and classified, AI-driven intelligence determines the optimal mitigation strategy—whether via RTBH, BGP, Flowspec, ACLs, or TMS. The attack is continually monitored, and mitigations are adapted in real-time as the attack evolves, ensuring that mitigation strategies remain effective even as attackers shift tactics. This combination of intelligence, detection, and automation provides significantly improved protection against carpet bombing attacks. The faster aggregate detection, as well as automation of mitigations on selected subnets and hosts within the targeted network, keeps external services and internal protections active while not over-mitigating. This intelligent, automated, and adaptive approach ensures that Arelion's team stays ahead of increasingly sophisticated DDoS threats with minimal manual effort and maximum efficiency.

This expanded partnership enables Arelion to support the network security requirements of its customers amid rising attacks on critical infrastructure. By enhancing its capabilities with NETSCOUT, Arelion improves network security across its #1-ranked global Internet backbone, empowering enterprise customers with resilient, high-performance connectivity services.

"Financial services, government, utilities, and other vital sectors are experiencing increased risk from more sophisticated and frequent DDoS attacks, reinforcing the need for comprehensive DDoS protection," stated Darren Anstee, chief security technologist, NETSCOUT. *"Our latest DDoS Threat Intelligence Report echoes Arelion's experience of increasing numbers of application-layer and volumetric attacks, as well as greater attack sophistication. This partnership will help Arelion enhance the protection it can provide to enterprises facing more frequent cyberattacks on their businesses."*

LEARN MORE

For more information about NETSCOUT 's Arbor DDoS Protection Solutions visit:

www.netscout.com/arbor

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