# AI-Powered Adaptive DDoS Protection with Sightline and TMS

## The Growing Need for Adaptive DDoS Capabilities

In today's digital landscape, where attackers utilize AI, Distributed Denial of Service (DDoS) attacks remain a persistent and evolving threat. These attacks can severely disrupt online services, damage brand reputation, and result in significant financial losses. Traditional DDoS defenses, often reliant on static thresholds or localized data, are no longer sufficient to counter the increasingly sophisticated and distributed nature of modern attacks.

To effectively combat these threats, organizations require an intelligent, AI and ML-driven adaptive approach to DDoS detection and mitigation – a solution that can dynamically detect, analyze, and adaptively mitigate attacks in real time. NETSCOUT's Adaptive DDoS Protection, powered by the ATLAS® Threat Intelligence platform, delivers precisely this capability by combining global visibility, machine learning, and intelligent automation.

*The unmatched breadth and depth of our DDoS attack data allows us to identify the exact point in time when new DDoS attack vectors are discovered, tested, optimized, first utilized by adaptive attackers, and eventually weaponized in DDoS-for-hire services.*

## Global Visibility is the Foundation

NETSCOUT's ATLAS platform provides unmatched global visibility, continuously analyzing over 550 Tbps of internet traffic from more than 500 ISPs and 2,000 enterprise sites across 100+ countries. This expansive visibility into approximately 50% of Internet traffic,enables early detection of DDoS attacks, even those distributed across multiple geographies, providing real-time threat intelligence about attacks across the globe to inform adaptive detection and mitigation.

## Adaptive Intelligence Informs Adaptive Response and Automation

NETSCOUT's ATLAS threat intelligence system leverages artificial intelligence (AI) and machine learning (ML) to analyze vast amounts of data and identify potential threats. The ATLAS Intelligence Feed® (AIF) continuously collects and processes data, providing real-time insights into DDoS attack patterns and trends. This feed continuously fuels NETSCOUT's DDoS protection products, enabling them to automatically detect and mitigate evolving DDoS attacks.

The ATLAS platform's global visibility and advanced analytics are crucial for several reasons:

- **Early Detection:** By monitoring internet traffic globally, ATLAS can detect DDoS attacks in their early stages, allowing for prompt mitigation before they escalate.
- **Comprehensive Analysis:** The platform's ability to analyze traffic from diverse sources helps identify complex attack vectors that might be missed by localized systems.
- **Adaptive DDoS Detection and Mitigation:** The continuous flow of threat intelligence enables NETSCOUT's products to adapt to new attack methods, block currently active DDoS attackers, and ensuring robust protection against emerging threats.

## Dynamic Mitigation That's Also Smarter

Today's DDoS attacks are dynamic, continually changing tactics and targets. For example, modern-day DDoS attacks commonly utilize multiple attack vectors (e.g. up to twenty) that the attacker dynamically changes as defenders mitigate. Or Carpet Bombing attacks which dynamically target multiple IP addresses (e.g. 100) within an organization's IP address range, making it difficult for defenders to detect and mitigate. Dynamic detection and mitigation are crucial for defending against these attacks because of their evolving nature.

In relation to carpet-bombing attacks specifically, Adaptive DDoS Protection features such as the following are used to stop them:

- **Managed object misuse detection** identifies abnormal traffic patterns across entire IP ranges rather than individual hosts—crucial for detecting stealthy carpet-bombing attacks. This method ensures that low-volume, distributed attacks are not missed and that alerts are consolidated for operational efficiency.
- **Precise Protection Prefixes (PPP)** further refines carpet-bombing attack mitigations by dynamically identifying and isolating affected IP ranges during an attack. This ensures that only malicious traffic is redirected, preventing over-mitigation and maximizing efficiency.

## Protecting the Internet by Protecting Yourself and Your Customers

Stopping misuse from within a service provider's own network helps everyone and allows them to be vigilant and responsive to emerging threats while ensuring that their networks remain secure and reliable. Moreover, by actively participating in the detection and mitigation of attack traffic originating within their networks, service providers contribute to the overall health of the internet ecosystem. This proactive stance not only protects their own interests but also demonstrates their commitment to being responsible Internet citizens. For these outbound/cross-bound attacks, Adaptive DDoS Protection features such as the following can be used:

- **Source misuse detection** enables service providers to identify and mitigate malicious traffic originating within their own networks. This includes tracking compromised IoT devices and misbehaving subscribers, helping to prevent outbound attacks and reduce the risk of reflection-amplification vectors.
- **Source-based mitigation** adds another layer of defense by blocking malicious traffic closer to its origin. This approach not only protects external targets but also reduces collateral damage and enhances the overall security posture of the service provider's network.

## Conclusion

With NETSCOUT's AI-powered Adaptive DDoS Protection, customers gain enhanced security through real-time, globally informed threat detection and mitigation. The solution supports informed decision-making by providing deep insights into attack patterns and trends. Its scalability ensures that protection evolves alongside the growing complexity and volume of threats, while its precision reduces operational overhead, improves response times, and increases efficiency.

As DDoS attacks become more distributed, deceptive, and damaging, adaptive protection is no longer optional—it is essential. NETSCOUT's Adaptive DDoS Protection, powered by the ATLAS platform, offers a comprehensive, intelligent, and scalable defense. By combining global visibility, advanced AI-powered analytics, and targeted mitigation techniques, Adaptive DDoS Protection helps organizations safeguard their networks, maintain business continuity, and stay ahead of emerging threats.

*Threat actors are now relying more on DDoS-capable botnets, Tor nodes, and open proxy servers to generate and obfuscate the actual sources of direct-path DDoS attacks. Initially revealed in our 2H 2022 DDoS Threat Intelligence Report and continuing to today, we have seen a renewed emphasis on direct-path attacks and a transition from a nearly decade-long stint of reflection/amplification preeminence.*

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



SECSB_041_EN-2502 07/2025