

High-Capacity DDoS Attacks Surge 1,286% in 1H 2026 According to NETSCOUT Threat Intelligence Research

2026-10-14

Massive 1Tbps Events and Weaponized Residential Proxies Expose Critical Mitigation Gaps, Forcing Organizations to Rethink Enterprise and Carrier Defenses

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® SYSTEMS, INC. (NASDAQ: NTCT) released its first half **2026 Distributed Denial-of-Service (DDoS) Threat Intelligence Report**, revealing a significant shift in how attacks are launched and sourced. With more than 9.1 million DDoS attacks recorded globally by NETSCOUT between January and June 2026, the report highlights that DDoS risk is growing along three axes: the volume of traffic that must be inspected, the number of places where mitigation must be deployed, and the share of attacks that disrupt service without ever saturating a link.

"The 1,286% rise in attacks clearing 1Tbps or 1Gpps means high-capacity events are no longer anomalies; they are routine," stated Hardik Modi, VP Engineering, DDoS Solutions, and ASERT Threat Intelligence Team, NETSCOUT. "With the proliferation of residential proxies and short, rate-based attacks from DDoS-for-hire platforms, traditional coarse network controls are insufficient. Providers and enterprises alike need finer-grained, selective mitigation and increased scrubbing capacity at network edges to combat these qualitative shifts in attack sophistication."

Key findings include:

- Massive Attacks on a Global Scale – NETSCOUT ATLAS recorded more than 9.1 million DDoS attacks across 209 countries and territories, underscoring the expanding operational risk to enterprises and providers.
- Surge in High-Impact Capacity – Attacks exceeding 1Tbps or 1Gpps increased 1,286% year over year, suggesting defenders must continue to prepare for greater attack intensity.
- IPv6 crossed the terabit threshold – NETSCOUT observed its first IPv6 attack exceeding 1Tbps, while active

mitigation of IPv6 attacks rose by more than 300% year over year even as IPv6's share of attacks remained roughly flat, illustrating the need for robust IPv6 protection.

- Pressure on Carrier Mitigation – Direct-path methods accounted for 64% of observed attacks and gained share for a third consecutive half-year, while carpet-bombing grew from 3.97% to 4.54% of attacks, and outbound attacks clearing 1Tbps/1Gpps caused operational impacts. Dedicated mitigation capacity remains the selective layer that providers need to intelligently filter malicious traffic.
- DDoS for Hire and Attack Economics – Attacks lasting one minute or less have roughly doubled as a share since 2H 2023, stressing connection tables, application backends, and resolvers, suggesting DDoS-for-hire platforms are shortening the path to attack.
- Residential Proxy Supply Chain – by pairing residential proxy network tracking with DDoS telemetry, NETSCOUT ASERT identified residential proxy sources participating in DDoS attacks, highlighting that attack traffic can originate from harder-to-distinguish consumer IP addresses.

NETSCOUT maps the DDoS landscape through passive, active, and reactive vantage points, providing unparalleled visibility into global attack trends. For more than 15 years, NETSCOUT has delivered trusted, consistent DDoS Intelligence based exclusively on directly observed, verifiable attack traffic. NETSCOUT does not aggregate multiple alerts or geographically distributed events into composite peak values, which ensures accuracy, repeatability, and true comparability across reporting periods. Peak metrics reflect single-second maximum bits-per-second (bps) and packets-per-second (pps) rates measured at defined mitigation and monitoring points.

From Verified DDoS Intelligence to Layered Protection

NETSCOUT protects two-thirds of the routed IPv4 space, securing network edges that carried global peak traffic of over 800 Tbps. It monitors tens of thousands of daily DDoS attacks by tracking multiple botnets and DDoS-for-hire services that leverage millions of abused or compromised devices. NETSCOUT ARBOR Cloud, backed by ATLAS visibility and dedicated DDoS mitigation capacity, complements on-premises defenses and helps organizations absorb large, distributed attacks before they overwhelm critical services.

These findings show why DDoS resilience now depends on more than stopping the largest attack. Organizations need to recognize changing attack sources and methods, mitigate both inbound and outbound attacks, apply precise protection where services are exposed, and draw on cloud capacity when attacks exceed local defenses. NETSCOUT combines directly observed ATLAS intelligence with on-premises and cloud-delivered mitigation to help customers protect service availability and sustain the digital operations their businesses depend on.

Resources:

- Download the **NETSCOUT 1H 2026 DDoS Threat Intelligence Report**

- See real-time DDoS attack stats and insights at **NETSCOUT Cyber Threat Horizon**
- Learn more about **NETSCOUT Arbor DDoS Protection Services**

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through its unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. As a leading provider of network observability, AIOps, carrier service assurance, cybersecurity, and Distributed Denial-of-Service (DDoS) attack protection solutions, NETSCOUT serves the world's largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on **LinkedIn, X, or Facebook**.

©2026 NETSCOUT SYSTEMS, INC. All rights reserved. Third-party trademarks mentioned are the property of their respective owners.

Editorial Contacts:

Chris Lucas

NETSCOUT SYSTEMS, INC.

+1 978 614 4124

Chris.Lucas@netscout.com

Chris Shattuck

Finn Partners for NETSCOUT

+1 404 502 6755

NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC