NETSCOUT

NEWS RELEASE

NETSCOUT Closes Critical CDN Security Gap to Safeguard Essential Digital Services

2026-08-20

Enhanced Arbor Edge Defense Identifies Attack Sources Hidden Behind CDN Proxies

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced enhancements to its Arbor Edge Defense (AED) solution that helps enterprises maintain the availability of revenue-generating and mission-critical applications against sophisticated DDoS attacks that evade or bypass content delivery network (CDN) DDoS defenses. The enhancements identify malicious sources concealed behind shared CDN infrastructure and apply precise, service-specific countermeasures to block attacks without denying access to legitimate customers using the same CDN.

“Cybercriminals launch DDoS attacks for many reasons, but the ultimate outcome is to drain the targeted organization's resources,” said Christopher Rodriguez, research director, security and trust, IDC. “These attacks pose significant operational and financial risk because adversaries can target multiple layers of an organization’s infrastructure and rapidly shift attack methods. Effective DDoS defense must be dynamic, highly performant, and broad enough to protect critical services across the attack surface.”

Organizations rely on CDNs to accelerate digital experiences and absorb large-scale traffic surges, but CDN deployment alone does not eliminate DDoS risk. Dynamic applications, APIs, authentication services, uncached requests, and exposed origin infrastructure can remain vulnerable. Attackers exploit these gaps by sending DDoS attacks disguised as application-layer traffic that resembles legitimate user activity. CDN DDoS defenses can miss this traffic because they focus on detecting volumetric DDoS attacks and rely on generic protections that are not customized to the individual customer applications being protected. These advanced application-layer DDoS attacks bypass CDN DDoS protections to the customer datacenter, causing outages and impacting revenue. Defenders

must either allow the attack through or block it, including the legitimate traffic along with it. NETSCOUT restores source-level visibility and enables precise mitigation of all CDN traffic closer to the protected service.

The enhanced AED solution enables enterprises to:

- Reveal Attack sources hidden by CDN proxies: AED integrates a high-performance TLS transparent proxy to decrypt and inspect application traffic, identify its true source from application headers, and apply precise application-layer DDoS countermeasures to block DDoS traffic that CDNs do not.
- Stop application layer attacks: Detect traffic designed to exhaust application, API, authentication or infrastructure resources.
- Protect applications with service-specific policies: Apply countermeasures tailored to the behavior and requirements of each protected service.
- Preserve legitimate customer access: Block malicious traffic precisely without denying service to broad ranges of users behind shared CDN infrastructure and without impacting other traffic arriving from the CDN proxy.
- Defend direct and CDN-mediated traffic paths: Mitigate attacks that pass through the CDN as well as attacks that bypass it and target origin infrastructure directly.
- Extend existing CDN investments: Add an independent layer of protection and visibility without requiring the enterprise to replace their CDN provider.

“Enterprises cannot assume that putting a CDN in front of an application protects every path attackers can use to reach it,” said Scott Iekel-Johnson, AVP, product management, NETSCOUT. “Attackers increasingly look for ways around defenses, including targeting origin infrastructure directly or slipping through the CDN by mimicking legitimate traffic. AED closes those gaps by extending DDoS protection beyond the CDN, closer to the application itself, securing the paths attackers still exploit, enabling enterprises to protect critical applications precisely while keeping legitimate customers connected.”

The AED enhancements extend NETSCOUT’s established DDoS protection portfolio into an increasingly important point of enterprise exposure: the connection between shared cloud delivery infrastructure and business-critical applications. By complementing existing CDN investments rather than requiring organizations to replace them, AED helps customers address a significant area of exposure while extracting greater security value from current infrastructure investments. For enterprises whose revenue, operations and public services depend on application availability, this provides an additional layer of resilience at the point where an attack can have the greatest business impact.

Resources:

- Explore NETSCOUT **Arbor Edge Defense** and its CDN-aware DDoS protection capabilities.

- Learn why **CDNs alone are not sufficient** for modern DDoS Protection.
- Review current global DDoS attack trends in the NETSCOUT **DDoS Threat Intelligence Report**.

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**.

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