NETSCOUT

NEWS RELEASE

NETSCOUT Combines Leading Global Threat Intelligence With Machine Learning to Protect Enterprises From Rapidly Spreading Dynamic DDoS Attacks

2023-07-11

Adaptive DDoS Protection for AED Defeats Dynamic DDoS Attacks, Securing Enterprises and Reducing Risks and Costly Network Downtime

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.** (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS attack protection solutions, today released its latest version of Arbor Edge Defense (AED) which includes new ML-based Adaptive DDoS Protection.

According to NETSCOUT's latest DDoS Threat Intelligence Report, there has been a significant increase in a new breed of dynamic DDoS attacks that use multiple vectors and techniques to launch botnet-based, direct-path, state exhaustion, and application-layer attacks designed to evade conventional static network and cloud-only-based DDoS defense.

Every enterprise is at grave risk today if they don’t deploy an effective DDoS solution on-premises to protect their network edge, internet-facing services, and critical stateful infrastructure such as firewalls and load balancers from these constantly evolving attacks. Attackers can send dynamic direct-path DDoS traffic at any time, and they can quickly change attack vectors during the attack making them nearly impossible to defend without the right technology. With AED’s Adaptive DDoS Protection, IT teams now have a scalable, always-on stateless packet processing solution that uses unmatched visibility into more than 50% of all internet traffic, global, real-time DDoS attack threat intelligence, decades of DDoS mitigation experience, and machine learning (ML) software intelligence to automatically detect, adapt to, and mitigate dynamic DDoS attacks.

“As cyber threats become more sophisticated and dynamic, IT teams need to out-smart bad actors with the ability to adapt and surgically block unwanted traffic at the network edge,” said Scott Iekel-Johnson, AVP, DDoS and Threat Intelligence at NETSCOUT. “With unmatched real-time visibility into global DDoS attack activity and decades of mitigation experience, no one knows more about DDoS attacks than NETSCOUT. With AED’s Adaptive DDoS Protection, enterprises can take advantage of our DDoS attack expertise and minimize unnecessary workloads that force expensive upgrades with an always-on product that can scale to protect every edge from a single pane of glass.”

Automated AED Protects Enterprises from Threats

Deployed at the Internet edge in front of any firewall, AED screens incoming and outgoing traffic using stateless packet processing, global DDoS threat intelligence, and ML to block inbound cyber threats, including DDoS attacks and other bulk malicious traffic. It protects and reduces the load on firewalls, load balancers, or VPN concentrators and stops the proliferation of malware within an organization. AED can also block outbound communications sent from compromised internal devices to sites run by bad actors to prevent data breaches and other malware activity. It contains the threat while giving the IT team time to investigate and remove it before it can cause further damage. In the event of a large volumetric DDoS attack, AED’s cloud signaling feature integrates with cloud DDoS protection providers, including NETSCOUT’s **Arbor Cloud**, to intelligently and automatically coordinate attack response between cloud-based volumetric protection and on-premise adaptive DDoS attack protection.

Visibility into 50% of All Internet Traffic

NETSCOUT ASERT, the company’s expert security research and DDoS attack mitigation team, works with over 500 Internet Service Providers (ISPs) to maintain a unique sensor network called ATLAS. With over 400 Tbps of international transit traffic received every second of every day from 93 countries, 600 industry verticals, and more than 31,000 autonomous systems, ATLAS provides ASERT with unmatched visibility into more than 50% of all internet traffic and real-time DDoS attack activity. ASERT analyzes the ATLAS data and distributes its findings to the Arbor Edge Defense (AED) solution via the ATLAS Intelligence Feed (AIF). AIF continually arms AED with highly curated intelligence that constantly updates the IP addresses of bots and reflectors/amplifiers actively participating in DDoS attacks around the globe. Created from real-world ASERT mitigation experience, AED’s Adaptive DDoS defense capabilities use ML-based algorithms to automatically recommend changes to attack countermeasures designed to stop dynamic DDoS attacks.

To learn more about how Adaptive DDoS Protection for AED automatically protects networks from dynamic DDoS attacks, visit our **website**.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through the company's unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. NETSCOUT serves the world's largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on LinkedIn, Twitter, or Facebook.

Maribel Lopez
Manager, Marketing & Corporate Communications
+1 781 362 4330
maribel.lopez@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 404 502 6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC