NEWS RELEASE

NETSCOUT Partners with UMass Lowell to Protect the University's Network from Cyber Attacks

2019-06-05

NETSCOUT Donating Arbor Edge Defense Software and Hardware to IT Department

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC**., (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, announced today that it is partnering with the University of Massachusetts Lowell (**UMass Lowell**) to protect the university's network from cyber attacks. NETSCOUT is donating **NETSCOUT Arbor Edge Defense (AED)** software and hardware to the university's IT department. Using highly-scalable stateless packet processing technology, NETSCOUT AED acts as a network perimeter enforcement point, where it detects and blocks inbound cyber threats and outbound malicious communication in bulk, acting as the first and last line of perimeter defense for an organization.

"At UMass Lowell, our network is constantly being scanned for attacks, threatening everything from research to human resources and payroll," said Jim Packard, UMass Lowell's chief information security officer. "We realized we needed better DDoS protection and determined that NETSCOUT's Arbor Edge Defense solution was best-in-breed. Right out of the box, this solution provides far more than just DDoS protection, making it a perfect fit for our purposes and a critical element in our suite of security measures. Higher education is not immune from attacks, which is why AED's first and last line of defense capabilities are exactly what we needed."

NETSCOUT Arbor Edge Defense (AED)

NETSCOUT AED is an always-on, in-line solution which can be deployed as a physical appliance or virtual network function. It sits outside the firewall, between the enterprise or data center and the internet. A unique stateless packet processing engine provides efficient blocking of DDoS attacks and other malicious traffic matching Indicators of Compromise (IoCs) without tracking any session state. As a result, NETSCOUT AED can make other perimeter

defenses more effective by shielding them from DDoS attacks, and offloading the overhead associated with applying millions of IoCs to traffic streams.

NETSCOUT AED leverages the company's proven market-leading DDoS technology that is already trusted by thousands of enterprises worldwide. As a result, it provides advanced packet-based protection against complex application-specific DDoS attacks and state-exhaustion techniques; as well as defenses against internet scale threats, neutralizing the malware families that make up the global botnet threat. Armed with millions of reputation-based IoCs, NETSCOUT's stateless packet processing engine can also detect and block outbound communication from internal compromised hosts that have been missed by other devices in the security stack; helping to stop further proliferation of malware and other tactics used within crimeware and advanced threat campaigns.

"As student interaction and testing are increasingly done online, universities across the country, and around the world, are facing many of the same cyber-security challenges encountered by businesses and government agencies," said Carlos Morales, NETSCOUT's vice president and general manager of DDoS Mitigation Services. "UMass Lowell has a great program in place to ensure network security, and it recognized that NETSCOUT's innovative, market-leading Smart DDoS technology can help further harden the network against DDoS and other internet bound threats. Partnering with the university's IT team not only helps protect the university's vitally important network, it also provides NETSCOUT with invaluable feedback and sharing of threat intelligence. This will, in turn, help us evolve our solutions to better help other universities and higher education programs."

As part of the partnership, UMass Lowell has committed to share indicator data based on what NETSCOUT AED blocks providing NETSCOUT with insights into what kinds of threats are targeting the university. This data will not contain IP addresses or any other personal information. NETSCOUT will also gain feedback from periodic user experience studies on installed devices.

Operationalizing Threat Intelligence

NETSCOUT has the ability to enable security and network teams to connect and correlate unique intelligence on emerging internet threats and trends, with visibility into what is happening across their internal organization from a threat perspective. This is a core component of NETSCOUT's Smart DDoS strategy. NETSCOUT's Active Threat Level Analysis System (ATLAS®), collects, prioritizes, and disseminates data on emerging threats based on our unique visibility into over one-third of all internet traffic. **The ATLAS Security Engineering & Response Team** (ASERT) is continuously and automatically delivering high fidelity threat intelligence via the **ATLAS Intelligence Feed**, enabling customers to not only block threats in real-time but enhance their defenses over time.

NETSCOUT's robust threat intelligence not only identifies an attack, but also provides high-value context, such as the attack infrastructure, methods, and related indicators that enable organizations to make faster security

decisions with greater confidence. NETSCOUT AED supports standards such as STIX/TAXII for ingestion of third-party threat intelligence and provides a robust REST API to integrate threat detection and blocking telemetry, and contextual threat intelligence into existing SOC workflows and management tools.

About UMass Lowell

UMass Lowell is a national research university located on a high-energy campus in the heart of a global community. The university offers its more than 18,000 students bachelor's, master's and doctoral degrees in business, education, engineering, fine arts, health, humanities, sciences and social sciences. UMass Lowell delivers high-quality educational programs, vigorous hands-on learning and personal attention from leading faculty and staff, all of which prepare graduates to be leaders in their communities and around the globe. **www.uml.edu**

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions help protect against DDoS attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit **http://www.netscout.com** or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20190605005625/en/**

Suraj Mashru
Senior Campaign Manager
E: **Suraj@BabelPR.com**
DD: +44 (0) 207 1993 977
W: **www.babelpr.com**
TW: **@Suraj_Mashru**

Source: NETSCOUT SYSTEMS, INC.