Manufacturer Improves Network Perimeter Defense and DDoS Prevention With Arbor Edge Defense

Fosters NetOps and SecOps Collaboration Through Enhanced NETSCOUT Operationalization

OVERVIEW

The Challenge

- Network perimeter security reliant on manual IP "blacklist" process
- Increased company threat landscape necessitated enhanced DDoS Prevention solution

The Solution

- Arbor Edge Defense

The Results

- Automated network perimeter defense, enhanced DDoS protection, integration with security stack
- Inline solution on network links already tapped by NETSCOUT® for packet processing and smart data generation

Customer Profile

This U.S manufacturer produces heavy-duty equipment under multiple brands. With production plants in more than a dozen countries, the organization has strived to comply with high-quality industrial standards, which has helped the company maintain their status as a world-class manufacturer.

The company's information technology (IT) team has long used their NETSCOUT nGeniusONE® Service Assurance solution with InfiniStreamNG® (ISNG) and Packet Flow Switch (PFS) technology for real-time packet monitoring at their data center and headquarters locations. In coordination with Network Operations (NetOps), the Security Operations (SecOps) team derived additional value from the company's investment in NETSCOUT by accessing nGeniusONE analytics and smart data visibility sources for packet-based forensics for incident-related troubleshooting.

The Challenge

Historically, SecOps' efforts to secure the network perimeter were largely manually intensive, involving maintaining a rolling list of IP addresses (i.e., blacklist) at the firewall level. Any new IP address potentially viewed as a rogue actor was manually added to the "bottom of the list" by a SecOps resource. While that approach had proven effective in blacklisting suspect network traffic, SecOps was challenged by the vast size of this IP address list, manual efforts associated with its maintenance, and questions regarding both accuracy and currency. For example, for some entries dating back several years, SecOps was unsure whether or not the IP address should continue to be blocked by the firewall.

With the company's network and data center operations growth and the resultant expansion of their threat landscape, SecOps turned to their long-time NETSCOUT business partner for a next-generation perimeter security solution that would better safeguard business and complement what the nGeniusONE and smart visibility solution was already providing to cross-IT resources.

Solution in Action

The company has transformed its network perimeter defense strategy and automated its DDoS protection from attacks by deploying the NETSCOUT Arbor Edge Defense (AED) solution. With AED, SecOps has automated processes associated with defining both "deny" and "allow" lists at its firewall, leading to enhanced network perimeter security and better protection of the company's manufacturing business.

AED was deployed inline (i.e., between the internet router and firewall) on the same links already being tapped by NETSCOUT to feed network packet traffic to the long-deployed ISNG and PFS smart visibility sources responsible for real-time generation of smart data used by nGeniusONE analytics.

In addition to improving network perimeter security and firewall efficiencies, AED equipped SecOps to stop DDoS attacks as large as 40 Gbps. Using NETSCOUT's stateless packet processing technology, SecOps can also use AED to stop TCP-state exhaustion attacks that target and impact stateful devices, such as next-generation firewalls.

The Results

The SecOps team's enhanced ability to better protect the business from external cyberthreats with AED was delivered just as attacks on global manufacturers were on the rise. For a company with a manufacturing environment as vast and complex as this one, it was difficult to assign a value on the importance of SecOps' move to the AED perimeter defense and DDoS solution.

The earlier organizational collaboration between NetOps and SecOps to maximize relevance of production-level nGeniusONE analysis and NETSCOUT smart visibility across this manufacturer's business helped set the stage for deploying the hybrid DDoS protection and perimeter defense solution delivered by AED.

The company also optimized expense controls and increased IT efficiencies by moving to a single-vendor solution that met current-day NetOps and SecOps requirements. In that context, the AED solution also offered opportunities to increase returns on investment from SecOps' existing security stack and processes by using a RESTful application programming interface providing support for both Syslog (e.g., Common Event Format, Log Event Extended Format) and Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) cybersecurity standards.

LEARN MORE

For more information about NETSCOUT's Intelligently Automated, Hybrid DDoS Protection and Perimeter Defense solutions visit:

https://www.netscout.com/product/netscout-aed

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)

bako tech

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. BAKOTECH is the official distributor of Netscout in Ukraine, Georgia & CIS, Central Asia countries.

netscout@bakotech.com

+380 44 273 3333

www.netscout.bakotech.com

SECSB_001_EN-2201 02/2022