Bridging Network and Security Operations Requirements With NETSCOUT

Optimized Vulnerability Scanning Scheduling Assures Server Environment Performance

OVERVIEW

The Challenge

- Increased vulnerability scanning requirements prompted SecOps request for more frequent scheduling.
- NetOps concerned how weekday scanning could impact network performance.

The Solution

- nGeniusONE® Service Assurance platform
- NETSCOUT® InfiniStreamNG® appliances
- nGenius® 5000 Series Packet Flow Switches
- NETSCOUT Premium Support Services

The Results

- Increased vulnerability scanning assured security and performance of server environment supporting business operations.
- IT silos reduced and collaboration improved.

Customer Profile

This financial services leader successfully processes millions of business transactions every day, which has helped make the company a household name.

This company is a long-time NETSCOUT customer, years ago standardizing on nGeniusONE as their service assurance platform of choice. The company had widely deployed InfiniStreamNG (ISNG) smart data sources and nGenius Packet Flow Switches (PFS) to provide service edge visibility across their network, with additional service assurance operations guidance provided by their contracted NETSCOUT Premium Support Services (PSS) engineering resources.

The Challenge

Given the nature of this company's business, regular Security Operations (SecOps) scanning of its server farm to assure the environment was free of vulnerabilities was understandably an area of intense focus.

The work-from-home (WFH) business era has seen exponential increases in cyberthreat attacks for all global companies, and the SecOps team wanted to take additional measures to safeguard the company's server environment. In this case, SecOps wanted to increase the vulnerability scanning cadence to include weekday scheduling, during non-peak hours, in addition to its standard weekend processes. Traditionally, SecOps scanning had been coordinated to run on weekends using their industry-leading vulnerability reporting tool. This practice allowed vulnerability scanning to be conducted when network traffic volumes were lower and bandwidth was readily available to accommodate the workloads that Network Operations (NetOps) believed were required for this SecOps testing.

Adding vulnerability scans during off-hours Monday through Friday would simply offer more opportunities for SecOps to assure the security of their server environment. With more than 1,000 host servers operating across their environment, receiving executive endorsement of this modified testing plan was a major SecOps priority.

For their NetOps colleagues, however, there was concern any weekday testing would impair performance of regular, daily business workloads by introducing additional network traffic that would be traveling across the network and through firewalls. Since this is truly a global business, "off-hours" in one geography are still "business hours" in another.

As a result, when SecOps appealed to IT leadership to reconcile this issue, there was an identified need for network traffic modeling, analysis, and reporting that would provide the evidence necessary to assure NetOps that this modified testing schedule would not unnecessarily consume bandwidth or impact application responsiveness.

In response, IT leadership agreed to a one-month trial of this modified vulnerability scanning approach to determine whether additional SecOps server testing cycles would hinder network performance.

Solution in Action

The company has reliably used nGeniusONE analytics and ISNG appliances for smart visibility to assure business performance across its enterprise environment, so approaching their long-time NETSCOUT PSS Engineer to assist them during this month-long trial was a logical extension of a strong track record in troubleshooting other service delivery issues.

By using the NETSCOUT production environment, the PSS Engineer collaborated with IT Operations to visualize vulnerability scanning traffic, with real-time nGeniusONE service dashboard and monitor views into client/server performance that showed associated bandwidth consumption. In doing so, IT Operations and PSS took advantage of NETSCOUT smart visibility views across several service edges, including data center (which included firewalls, load balancers, and service enablers, as well as the host server environment) and network edges.

Using NETSCOUT smart data (generated in real-time by ISNG smart visibility sources monitoring application packets from the company's network traffic), nGeniusONE contextual views factored the multi-tier infrastructure, including MIB2 interfaces and firewall environments.

This nGeniusONE performance snapshot enabled IT Operations to visualize how applications and servers at two key data centers handled the vulnerability scanning workload during a 10 p.m.-to-5 a.m. schedule being used as a trial for modeling the vulnerability scanning's performance impact. Through analysis and trend reporting conducted over the course of the month, as well as real-time monitoring occurring on a daily basis, IT Operations could view traffic impacts as scanning tests started and when network consumption peaked.

This vendor-neutral analysis with nGeniusONE throughout their enterprise showed what SecOps had hoped – there was no major associated network load with vulnerability scanning during weekday "off hours."

The Results

The company's earlier investments in NETSCOUT technology and consultative PSS Engineering resources enabled the collective IT Operations teams to benefit from informed decision-making about how increased vulnerability scanning practices would impact network operations – thus, the additional weeknight scans for its server network provided enhanced assurance that the business service and data center operations environment was running with integrity and better protected from cyberthreats.

LEARN MORE

For more information about NETSCOUT network performance management solutions, visit:

https://www.netscout.com/solutions/network-performance-management

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)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

ECS_333_EN-2101 06/2021