NETSCOUT®

Enhancing Government NetOps and SecOps Collaboration With NETSCOUT Smart Data

Providing a Single Source of Truth for Cybersecurity and Service Edge Monitoring Efficiencies

HIGHLIGHTS

The Challenge

- Agency needed to meet national cybersecurity mandates
- Requirements for improved network, virtual, remote, and data center visibility and agency operations

The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG® (ISNG) and vSTREAM® smart visibility appliances, with nGenius Flow Collectors
- nGenius® 5000 Series Packet Flow Switches
- NETSCOUT® Omnis® Cyber Intelligence, with Cyber Adaptor for use with ISNG packet-based data sources

The Results

- Agency advanced cybersecurity in compliance with governmental proclamation
- Single-vendor data source for Cybersecurity and Service Assurance, with IT tool consolidation and CapEx/OpEx reduction

Customer Profile

This government agency oversees national security strategy and preparedness to safeguard this country's residents, resources, and business assets.

The agency is a NETSCOUT® customer, some years earlier selecting nGenius 5000 Series Packet Flow Switch (PFS) technology to improve network packet visibility and accessibility across information technology (IT) operations by using core network packet broker features, including filtering, load balancing, replication, and aggregation.

The Challenge

The country's leadership had previously announced a strategic commitment to enhance the government's cybersecurity measures in response to persistent threats in today's global landscape. This announcement prompted the agency's Security Operations (SecOps) team to reconsider their long-time Network Performance Management (NPM) strategy, which relied on vendor tools that used NetFlow, MIB-II, and SNMP as data sources for analysis, post-incident troubleshooting, and forensic security efforts.

The operation of nGenius 5000 Series PFS appliances in the agency environment helped increased SecOps' awareness of potentially expanding the use of packet-based data sources to improve their monitoring and troubleshooting activities. When combined with the benefits of packet-based metadata, the SecOps team was confident that expanded visibility across the agency environment would assist in meeting their aspirations for improving real-time network, application, and cybersecurity monitoring and enhancing the performance of government services.

Government leaders around the world have committed to heightening cybersecurity awareness. As a result, this SecOps project had increased levels of scrutiny within the agency and even this country's residents.

Solution in Action

Having already established a trusted partnership related to the nGenius PFS appliance deployment and its ongoing performance, the agency deployed an integrated, single-vendor NETSCOUT service assurance and cybersecurity solution that delivered:

- **Improved data center and network edge visibility**, with InfiniStreamNG (ISNG) smart data sources and additional nGenius PFS appliances deployed in the agency's data center core, including their server farm service edge environment. The ISNG's Adaptive Service Intelligence® (ASI) technology generates smart data from packet traffic flowing across their wide area network and data center environment for use by nGeniusONE's real-time analysis, enabling Network Operations (NetOps) to assure network and application performance, as well as reporting and troubleshooting activities.
- **Enhanced remote edge visibility**, by instrumenting nGenius NetFlow Collectors at regional agency locations to provide NetOps with access to MIB-II, Cisco NetFlow data, and SFlow data from routers and switches that could, in turn, provide smart data for nGeniusONE analysis.
- **Gained visibility into east-west traffic within a Kubernetes cluster,** by deploying vSTREAM virtual smart data sources in their on-premises VMware environment.
- **Established monitored edge visibility** that fortified the agency's cybersecurity posture, by deploying NETSCOUT's Omnis Cyber Intelligence enterprise-wide network threat and risk investigation platform. By enabling an Omnis® Cyber Adaptor software license, the agency used the same smart data generated by their already-deployed NETSCOUT ISNG and vSTREAM appliances to source Omnis Cyber Intelligence real-time analytics into actionable cyberthreat detection and investigation.

The SecOps and NetOps teams used the integrated NETSCOUT solution to address the following use cases:

- Visualize and successfully troubleshoot lagging application sessions and impaired performance of multi-tiered applications in operation at the agency.
- Analyze and resolve issues related to LDAP directory, authentication, and HTTP.
- Monitor real-time performance delivered to agency users by their Webex Unified Communications as a Service, Microsoft Office 365 Software as a Service, and Citrix virtual desktop infrastructure.
- Identify and address front-end issues that had impacted Website performance.
- Reconcile a performance issue in a Kubernetes platform used to manage containerized applications by specifically leveraging the NETSCOUT vSTREAM virtual appliance's ability to visualize east-west network traffic within the agency's VMware environment.
- Improve end-through-end monitoring of the agency's network across remote, network, and data center service edges, adding to NetOps' ability for real-time monitoring of a leased-line network supporting remote agency users.

From a cybersecurity perspective, the SecOps team employed Omnis Cyber Intelligence as a prevention and detection tool. Omnis Cyber Intelligence provided SecOps with their own platform for use in their Security Incident and Event Management environment, which also equipped them with access to environments the NetOps team was using. The SecOps team uses the Omnis Cyber Intelligence Threat Indicator interface to discover unauthorized servers, as well as firewall rules and access.

The Results

For an agency focused on enhancing national security, the NETSCOUT solution satisfied a number of project criteria, including:

- Providing single-pane real-time views of Service Assurance and Cybersecurity analysis and reporting, which were well-suited for presenting to Governmental Leaders as evidence of compliance with agency goals.
- Relying on a single data source for Service Assurance and Cybersecurity analysis, which enabled them to meet overarching goals for safeguarding their operations environments with fewer vendors and reduced tools to manage.
- Managing government cost-containment targets, with use of a singular NETSCOUT data source to feed both performance and security applications to help manage capital expenditures, reduce vendor management activities, and extend NetOps/SecOps collaboration.

LEARN MORE

For more information, visit:

NETSCOUT Department of Defense & Intelligence Agencies solutions:
www.netscout.com/solutions/government/department-defense-intelligence

Omnis Cyber Intelligence:
www.netscout.com/product/cyber-intelligence

NetOps and SecOps Collaboration:
www.netscout.com/solutions/netops-secops

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