State Agency Manages Expanding IT Environment With NETSCOUT

Addresses Federal Cybersecurity Requirements and Extended Hybrid Workforce Demands With Smart Visibility

OVERVIEW

The Challenge

- Federal and state-level cybersecurity projects resulted in new NetOps & SecOps visibility monitoring needs
- Required hybrid workforce reliability safeguards

The Solution

- nGenius® 5000 and 7000 series packet flow switches
- PFS 7000 series appliance add-on for PFS 5000
- Already-deployed nGeniusONE® Service Assurance and InfiniStreamNG® solutions

The Results

- Addressed cybersecurity requirements with NETSCOUT® smart visibility
- Assured state agency business operations across evolving hybrid workforce landscape

Customer Profile

This centralized State government information technology (IT) organization has vast responsibilities associated with delivering business services to more than 30,000 agency employees.

The agency has taken advantage of NETSCOUT's "single-vendor/multi-solution" approach, with nGeniusONE Service Assurance and Arbor Sightline & Threat Mitigation System technologies helping IT operations address Smart Visibility/Smarter Analytics and Cybersecurity requirements across their environment.

The Challenge

The everyday challenges of managing their large-scale, complex government service delivery environment were already substantial. Now, IT leadership faced additional cybersecurity and network demands, including those described in the subsections that follow.

Supporting Federal Cybersecurity Program Requirements

Like many other State IT organizations across the U.S., this team relied on and participated in one Federal Government Cybersecurity program to protect their environment from global threats.

As part of this program, the Network Operations (NetOps) team worked with the Federal Cybersecurity Infrastructure Security Agency and Center for Internet Security organization, as well as State-level IT leaders to analyze cyberattack traffic and share threat details for collaborative review.

With this effort, NetOps:

- Deployed specialized sensors (supplied by Federal Government agencies) across the network
- Analyzed attack traffic instances
- Shared malware threat details with participating Federal and State agencies to help collectively identified trends that needed to be monitored and addressed

While these sensors (essentially regarded by the IT team as an intrusion detection system) represented a new addition to their already-complex network environment, NetOps recognized their ability to satisfactorily visualize and monitor them was going to be highly scrutinized by the Federal and State agencies participating in this collaborative effort.

While this Federal program itself was largely "under the radar" in terms of public awareness, any threats that imperiled government agency operations surely wouldn't be, so NetOps' support and execution would be directly linked to success of this cybersecurity initiative.

Sustaining Hybrid Workforce Operations and User Experience

If meeting Federal cybersecurity program requirements was a national initiative, ensuring high-quality user experience for State agencies operating in an extended hybrid workforce model was a critical, ongoing local project.

While they had successfully managed an earlier pandemic-related workforce transition that involved extensive virtual private network (VPN) and Citrix virtual desktop infrastructure (VDI) additions, IT leadership wanted to assure steady-state operations for all agencies or employees, regardless of government business function or work location. As a result, NetOps team wanted to design a solution that offered security and redundancy necessary to further safeguard service delivery to State employees.

Enhancing Security Operations Intelligence Into New Data Center Operations

The Security Operations (SecOps) team identifies and manages the mitigation of threats to their network by using Arbor Sightline, while also relying on the Arbor Threat Mitigation System to remove identified Distributed Denial of Service (DDoS) attack traffic from their network without disrupting key network services.

With a regional data center recently added to the State IT network, the SecOps team wanted to deploy a next-generation packet flow switch (PFS) solution that would:

- Supplement their packet broker redundancy
- Further distribute network traffic processing loads
- Feed network traffic to other third-party cybersecurity tools to support triage efforts for any future infrastructure attacks potentially impacting the new facility

Solution in Action

The agency's collaborative cross-IT efforts focused on using NETSCOUT smart data sources and analytics to address their high-profile challenges in the following manner:

- **Meeting Federal Cybersecurity Program Requirements** – An nGenius 5000 Series PFS appliance supporting 40GB network speeds was instrumented at the agency's network connection edge in front of their Palo Alto firewall environment to aggregate network traffic and forward packets to their already-deployed InfiniStreamNG (ISNG) appliances for nGeniusONE's service assurance analysis. NetOps subsequently used nGeniusONE analytics to survey this network traffic and share that data with government agencies supporting the Federal Government cybersecurity program. In supporting this initiative, NetOps also realized the benefits of accessing Federal Government alerts regarding "situations to watch" across their environment.
- **Sustaining Hybrid Workforce Security and User Experience** – The IT team added redundancy to further safeguard business operations by deploying PFS 7000 appliance technology, as well as a PFS software add-on for their already-installed PFS 5000 appliance that resulted in an upgrade to advanced PFS 7000 functionality without hardware replacement. Deploying these PFS 7000 technology solutions enabled the IT team to support in-line bypass taps that both enhanced operational security and simplified their data center security management.
- **Enhancing Security Operations Intelligence into Data Center Performance** – The SecOps team deployed PFS 5000 technology to provide network traffic aggregation for cybersecurity and service assurance monitoring at its new data center. The PFS 5000 integrates with the agency's NETSCOUT PFS network, providing core packet broker functionality, including filtering, load balancing, aggregation, and replication.

The Results

The cross-IT operations team's abilities to meet these diverse cybersecurity and network project specifications were directly connected to their familiarity with the far-reaching smart visibility and comprehensive analytics offered by NETSCOUT Service Assurance and Cybersecurity solutions.

By relying on nGeniusONE analytics, ISNG smart data sources, and PFS technology already trusted by NetOps and SecOps, IT leadership was able to focus on economically adding necessary PFS technology that addressed their new cybersecurity and hybrid workforce demands, while elevating the value of their NETSCOUT investment.

LEARN MORE

For more information about NETSCOUT State and Local Governments solutions, visit:

https://www.netscout.com/solutions/government

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