

High-Flying Agency Assures Critical Aviation R&D with NETSCOUT

All-Inclusive Service Assurance and Cybersecurity Platform Improves Visibility, Meets Government Budget

OVERVIEW

The Challenge

- Service assurance and cybersecurity needs, improved IT collaboration
- Virtual network blind spots
- Government budget limitations

The Solution

- nGeniusONE® Service Assurance platform
- COTS InfiniStreamNG® and vSTREAM™ virtual appliances
- Arbor Threat Analytics
- Arbor Edge Defense

The Results

- All-inclusive service assurance and cybersecurity solution reduces vendor management, enhances existing IT toolsets
 - Closes gaps in virtual network visibility and application monitoring
 - Increases IT collaboration, reduces total of ownership
-



Customer Profile

This government agency specializes in advanced global flight solutions. The agency's innovation activities are distributed across a dozen facilities, with their main research & development (R&D) center providing an operations base for more than 3,000 aviation experts.

The Challenge

In light of the success of this high-flying agency, their Information Technology (IT) team understandably places paramount importance on maintaining the integrity and availability of the R&D environment supporting the activities of their researchers. To that end, the legacy technology located in the primary data center provides log management and packet forensics analysis, with IT also deploying a mix of packet brokers to pass traffic to their network and security tools.

Wanting to transform this approach to encompass a proactive network, application, and cybersecurity monitoring framework that also leveraged their existing technology investments, the agency's Cybersecurity team contacted a range of industry-leading service assurance and cyber threat/DDoS protection providers to identify a next-generation solution.

In assessing breadth of service assurance/cybersecurity solutions available from their identified vendors, the Cybersecurity team issued a Request for Information document that baselined their requirements for packet forensics, proactive security analysis, traffic blocking, anomaly detection, and threat analytics.

With this agency's funding otherwise largely focused on R&D activities, IT also had tight budget limitations for this project and encouraged vendors to sharpen their pencils when submitting price proposals.

Solution in Action

The agency is improving their R&D program integrity by implementing a converged NETSCOUT® service assurance and cybersecurity solution at their primary data center that singularly leverages NETSCOUT's Adaptive Service Intelligence™ (ASI) technology for smart data. NETSCOUT Smart Data instantly provides the intelligence the agency needs to drive network and application performance, deliver unmatched user experience, and find and address advanced cyber threats

The NETSCOUT nGeniusONE Service Assurance platform leverages COTS InfiniStreamNG (COTS ISNG) Adaptive Service Intelligence (ASI) software to provide the global visibility the agency needed to better support the effectiveness of network and application performance management.

The agency is addressing their virtual network visibility issues by deploying the vSTREAM virtual appliance, which complements the COTS ISNG. As a result, the agency now benefits from complete visibility into East-West traffic with vSTREAM and North-South traffic with COTS ISNG, enabling IT to monitor packets flowing into and out of the application servers, as well as across the data center and remote offices.

In addition, the agency is meeting their cyberthreat analytics needs by newly deploying the Arbor Threat Analytics high-performance internal network traffic security solution, which enables the Cybersecurity team to detect and confirm hidden threats quickly and accurately. The agency is also automatically detecting and blocking inbound threats (e.g., DDoS attacks, malware) and outbound malicious communications (e.g., bad URLs) by using the Arbor Edge Defense (AED) solution at their network perimeter (i.e., between router and firewall).

The Results

The agency quickly realized the value of the NETSCOUT solution as a Business Operations Analysis tool that assures mission-critical R&D technology environment performance and frees the agency from cyberthreats.

NETSCOUT's solution approach meets the agency's preference for an all-inclusive platform service assurance and cybersecurity platform that also meets their budgetary restrictions. The agency also sees NETSCOUT as offering best-of-both-worlds technology, when compared to other vendors whose technology met only a portion of their service assurance & cybersecurity requirements at a higher price.

The agency is improving protection of their R&D assets by transitioning from a service assurance solution based on packet forensics and log management analyses to a next-generation NETSCOUT approach leveraging end-to-end visibility and real-time network, application, and cybersecurity smart analytics. The agency also benefits by removing virtual network & application visibility gaps through the vSTREAM Virtual Appliance's ability to monitor ingress-egress traffic in the data center's virtualized environment.

The agency uses the Arbor cybersecurity solutions for threat hunting, allowing them to maintain system integrity by seeing "who has been on their network, where they've been, and what they've touched."

Beyond total service assurance and cybersecurity coverage, the agency's budget requirements were met with an all-in-one solution approach using common NETSCOUT Smart Data and a software-based COTS ISNG platform for cost-effectively monitoring critical business services.

The company is further reducing operating expenses by using NETSCOUT as their single vendor for service assurance and cybersecurity technologies. The agency also realizes maximized IT efficiencies by reducing the number of silo-specific tools, with NETSCOUT technology benefitting IT network and applications teams, as well as core cybersecurity subject matter experts.

Finally, the agency is achieving a project goal of improved third-party packet broker performance, with the vendor-agnostic COTS ISNG solution feeding network packets into those packet brokers, as well as enhanced packet forensics with NETSCOUT.

LEARN MORE

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

<https://www.netscout.com/solutions/federal-civilian-state-local-governments>



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