NETSCOUT

European Military Agencies Improve Network Performance, Data Security with NETSCOUT

Next-Generation Service Assurance Solution Reduces MTTR in Defense Environments

OVERVIEW

The Challenge

- Expanding network topology / speed requirements for government military purposes
- Increasing data storage for forensic activities and data encryption for enhanced government security mandates

The Solution

- nGeniusONE® Service Assurance platform, with UC smart analytics
- InfiniStreamNG™ appliances, with ASI-generated smart data and self-encryption support
- nGenius® 5000 series packet flow switch technology, supporting upgraded 100G network speeds

The Results

- Increased network agility and data security for country's military operations

Customer Profile

The defense agencies tasked with safeguarding this European country have entrusted operations of non-military network and application elements to a government-owned information technology (IT) provider. Whether deployed in ground, air, or naval defense pursuits, today's military applications must rely on many commercial network, application, and Unified Communications (UC) technologies to operate sufficiently. The IT provider offers the subject matter expertise necessary to support these general-purpose technology platforms on behalf of the country's defense agencies.

The country's military agencies and IT provider each benefit from this business partnership:

- Defense agencies can better-focus on core military missions by offloading labor-intensive monitoring of non-military technology platforms to the IT provider.
- The military benefits from the IT provider's ability to recruit and retain industry-proven network, application, UC, and cybersecurity technologists, leading to workload efficiencies and related opportunities to reduced government spending.
- The IT provider can apply lessons learned with this military customer to benefit other company delivery teams operating in government jurisdictions across the globe.

The IT provider uses several of their own in-country data centers to help deliver business technology services to these agencies. The IT provider has historically relied on NETSCOUT's nGeniusONE Service Assurance platform with data collected by InfiniStreamNG (ISNG) appliances. Packet traffic is forwarded to the InfiniStreamNG appliances and other tools by the nGenius packet flow switch (PFS) technologies to support network performance for the non-military applications and services supporting the respective defense agency environments.

The Challenge

Given their customer's high need for security, the IT provider must comply with policies regarding the monitoring approaches used to support sensitive military business. Such guidelines applied to post-incident troubleshooting, which relegated the IT provider's troubleshooting to a reactive approach reliant on network packet captures for off-line forensic analysis. The military also prioritized the use of additional safeguards, including mandatory data encryption in the communications environment. These challenges made gaining the visibility necessary to manage the performance of these networks even more complex.

The ongoing need for secure technology operations helped prompt government decision-makers to implement several new policy changes to support the military's digital transformations and additional safeguards for technology operations, including:

- Upgrading networks to support 100G speeds
- Increasing network data storage capabilities to provide enhanced access to network packets for troubleshooting and forensic analysis
- Expanding use of data encryption across all military communications

The IT provider knew these updates and technology enhancements would mean necessary changes in their NETSCOUT® production environment.

Solution in Action

The IT provider is meeting the customer's new network and security-related requirements by adding next-generation InfiniStreamNG (ISNG) and nGenius packet flow switch appliance technology to their data center environments. The ISNG appliances offer both expanded storage and encryption support to meet the military's requirements. The nGenius PFS appliances support the customer's demand for both 40 GbE and 100 GbE network speeds, while also enabling the IT provider to:

- Aggregate, replicate, distribute and manage the flows of traffic from the network to monitoring tools to improve performance of the downstream devices
- Optimize the flow of network packets to ISNG appliances, which then use Adaptive Service Intelligence (ASI) technology to convert those packets into NETSCOUT smart data for consumption by nGeniusONE performance analytics

Performance of applications and services across the military network is now better assured, with the IT provider's specialized Service Performance Analysis technologists operating as "firefighters" who troubleshoot problems as they occur, using nGeniusONE in the following manner:

- When a performance issue is observed in the service delivery environment, the Service Performance Analysis team can use nGeniusONE as-needed in key locations to conduct forensic activities to troubleshoot and identify root cause.
- By generating nGeniusONE Service Dashboard views, the team quickly, contextually drills down into precise, packet-level details and analysis, without the need for time-consuming packet captures and off-line analysis.

In this regard, the military further benefits from NETSCOUT's ability to capture more network traffic for forensic troubleshooting, with ASI technology performing granular data mining as traffic crosses physical network links, which reduces management traffic workloads.

The Results

The military is realizing improved system security and network agility as a result of the IT provider enhancing the NETSCOUT solution with next-generation data sources to meet the government's updated requirements.

While still working within the government's guidelines limiting real-time monitoring to non-military applications, the IT provider continues to extend returns on investment offered by nGeniusONE, which offers a single solution to perform:

- **Service Enabler monitoring** across the multi-tier network, factoring analysis of Simple Network Management Protocol (SNMP), HTTP errors, database queries, and DNS
- **Application monitoring,** including SAP, Oracle, and custom applications
- **UC Monitoring,** including quality of service (Qos) and Session Initiation Protocol (SIP) monitoring for Voice over IP technology, as well as Microsoft® Exchange messaging platform monitoring

Additionally, the IT provider benefits from using NETSCOUT as their single vendor for service assurance and packet broker technologies, which reduces complexity and costs that would otherwise be associated with managing multiple maintenance contracts and vendor technology training activities.

LEARN MORE

For more information about NETSCOUT solutions for international military agencies, please visit:

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

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