

Visibility Extended to Remote Medical Buildings for Protecting Health Care Services

Healthcare Expands Use of nGeniusONE To Assure Performance & Security of Patient-Impacting Applications

OVERVIEW

The Challenge

- Gap in visibility at new medical office buildings
- Product knowledge and best-practices to implement new NETSCOUT® data sources and workflows for remote building service assurance

The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG® software appliances
- Software-based nGenius® 5000 series Packet Flow Switches
- nGenius Visibility-as-a-Service

The Results

- Gained smart edge visibility that reduced MTTR for voice services issues and for identification of SSL/TLS certificate issues
- Gained quick value from this investment with nVaaS team engagement and expertise



Customer Profile

Founded more than a century ago, this healthcare is a national leader in delivering patient care, as well as advancing research and treatment protocols in several critical specialty areas. A pioneer in patient care, research, and education in life threatening illnesses, including diabetes and cancer, they are experiencing tremendous growth.

A strategic building initiative will result in an expansion of their main hospital campus, as well as the addition of patient and research facilities staffed by more than 5,000 doctors, nurses, research associates, scientists, and essential staff.

The organization heavily relies on their network and application resources for swift access to patient, diagnostic, and research information, as well as voice and video communications throughout their sprawling state-wide environment. A steady, well-planned IT strategy to gain benefits from digital transformation has helped them achieve research milestones and patient treatment successes.

The Challenge

Maintaining the health, availability, and performance of these services is essential to the healthcare which was a primary driver behind the broad implementation of NETSCOUT's nGeniusONE® Service Assurance solution for monitoring and troubleshooting issues enterprise-wide. Not long after deploying nGeniusONE, the healthcare made the decision to outsource much of their network operations requirements to a third-party organization. They would be required to use the healthcare's existing nGeniusONE solution for monitoring and troubleshooting issues with their critical applications, not the least of which was their electronic medical records application, Epic.

The security team within the healthcare's IT organization also consumed nGeniusONE metrics and analysis to assist in potential threats and to assist in identifying potential threats and ensure compliance with regulatory requirements for protecting the network, applications, and patient data.

It became a priority of the overall IT team to develop a comprehensive plan that would allow an expansion of NETSCOUT visibility into the new and soon-to-be-completed patient treatment, research, and administrative buildings for both performance and security requirements. The team identified the following requirements for the additional smart edge visibility:

- Additional traffic broker technology for aggregating and distributing copies of traffic packets from the 1GB and 10GB network segments to downstream monitoring and security tools, including NETSCOUT InfiniStreamNG (ISNG) appliances. These packet flow switches would need to be both cost-effective and offer advanced capabilities, like packet filtering and deduplication.
- Monitor and analyze long-standing, as well as recently introduced applications, including Epic, Microsoft Office 365, and Microsoft Teams.
- Gain quick time-to-value from the additional service edge visibility, with ability to leverage outsource alternatives.

Solution in Action

This quickly became a collaborative effort supported by senior leadership at the healthcare organization, the in-house security team, and the outsource organization for NetOps. All parties involved were intimately familiar with the challenges they faced with the expansion of their facilities and patient reach. Speed, agility, and cost-controls were essential to make this visibility project a success.

The following highlights how the IT team added to their nGeniusONE deployment to meet the health care's needs:

- InfiniStreamNG 2700 series certified software appliances with support for either 1GB or 10GB for packet-based, real-time, smart edge monitoring of application activity in the new medical, research, and administrative buildings, including the newly added Microsoft Office 365 and Microsoft Teams services.
- nGenius Packet Flow Switches 5000 series certified software appliances to collect, distribute, and aggregate network traffic from various links in the new buildings to the ISNG appliances, as well as other cybersecurity tools.
- NETSCOUT's innovative nGenius Visibility as a Service (nVaaS) consultative approach to operationalizing nGeniusONE in the hospital's building expansion for the benefit of the entire IT department, particularly the security team and outsourced NetOps team. The combination of deployment, ongoing configuration, and troubleshooting workflow support was instrumental in establishing best-practices and dashboards for NetOps to quickly investigate issues impacting the staff at the new buildings, be they performance- or security-related in nature.

Both SecOps and NetOps teams at the healthcare are already benefitting from the additional ISNG visibility and analysis with nGeniusONE by the nVaaS team.

- A group of doctors, nurses, and staff was reporting significant latency and poor call quality issues trying to use Microsoft Teams from one of the new medical office buildings. nVaaS, using nGeniusONE with smart data from the ISNG at that building, was able to isolate a quality of service (QoS) misconfiguration that placed Microsoft Teams traffic in a lower-priority delivery class. Once correctly configured, the quality of calls and conference improved.
- The SecOps team, working with the nVaaS experts, used the Certificate Monitor feature in nGeniusONE to evaluate their Secure Socket Layer / Transport Layer Security (SSL/TLS) certificates. They uncovered several potential issues with some certificates that had expired and others that were lower-level versions that put the hospital at potential risk. They addressed both of these issues with replacement of expired certificates and upgrades to stronger certificates.

The Results

The reputation of this leading-edge healthcare organization for delivering superior patient care based on exceptional research depends on their seamless access and use of the organization's clinical application services. With this latest implementation of the ISNG appliances and nGenius Packet Flow Switches at their recently opened remote medical facilities, they have filled a gap in critical service edge visibility for supporting the needs of both NetOps and SecOps.

The broader and more complete visibility and analysis at the new medical buildings provide the insight necessary to ensure performance and assist in security-related incidents from the data center core of this healthcare to the access edge, to the remote medical facilities. They can now proactively assist in troubleshooting critical, patient-impacting services that traverse the full path of the infrastructure, including ever-growing multi-building environments, and ensure that they are performing optimally.

Already benefiting from lower mean-time-to-repair (MTTR) when performance issues have occurred in the campus data center, they are now able to rapidly address issues impacting their staff and patient care in their state-of-the-art medical facilities. From both a patient care and patient impression standpoint, this was a critical step in the opening of these buildings.

Meeting the need for quick-time-to-value leveraging the NETSCOUT nVaaS team provided immediate returns, with expertise during deployment and configuration and best-practices guidance used to quickly pinpoint the voice and certificate issues. When an entire employee population depends on their network and clinical applications twenty-four hours a day, seven days a week, 365 days a year to deliver swift, secure patient care, NETSCOUT service assurance solutions are providing the visibility necessary to help meet these challenges.

LEARN MORE

For more information about NETSCOUT solutions for Health care organizations, please visit:

<https://www.netscout.com/solutions/service-assurance-healthcare>



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