Healthcare Assures Services with NETSCOUT Performance and Security Visibility

Packets Provide Single Source of Truth to Protect Reliability and Availability of Patient-Impacting Applications

OVERVIEW

The Challenge

- Lacked visibility throughout the distributed healthcare campus
- Needed longer retention of packet data to support security use cases

The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG® software appliances
- nGenius® 5000 Packet Flow Switches
- Omnis® Cyber Intelligence
- Omnis® Cyber Adaptor
- NETSCOUT® Visibility as a Service

The Results

- Comprehensive visibility for service assurance and security of Epic, VoIP, and other healthcare applications
- Achieving cost, time management, and vendor administration efficiencies with a single vendor approach for both performance management and security protection

Customer Profile

This top-ranked academic medical center delivers patient care from several regional hospitals and scores of medical offices, including a Level 1 trauma center, a world-renowned pediatric hospital with neonatal intensive care unit, and advanced research facilities. They are nationally recognized for delivering the highest-quality care to the surrounding community, supporting hundreds of thousands of unique patients in millions of outpatient clinical visits per year. They are known for their expertise in a variety of general and specialized services, including cardiology, emergency services, orthopedics, geriatrics, and pediatrics.

Tens of thousands of physicians, nurses, and residents are employed by the medical center, along with researchers and faculty from an associated school of medicine. They are dedicated to providing safe, swift diagnoses and personalized treatment plans for patients, as well as training and educating the medical professionals of tomorrow. It is critically important for both medical staff and their patients to have efficient, high-quality network and application performance throughout their multi-vendor healthcare environment to achieve exceptional patient-care treatment and services.

The Challenge

This healthcare had selected the NETSCOUT nGeniusONE Service Assurance solution with InfiniStreamNG (ISNG) appliances the year earlier to replace a NetFlow-based tool and improve visibility into and between their geographically distributed primary and backup data centers. The healthcare IT team had standardized on network packets to provide wider and much deeper details for assuring performance and availability of all their clinical and business application services, including their essential Epic health records application and Citrix virtual desktop interface (VDI) services. With nGenius 5000 series Packet Flow Switches

(PFS) passing network packet traffic from strategic points throughout the data centers to the downstream ISNGs, the network operations (NetOps) staff was able to support performance management initiatives and share data with their security operations (SecOps) counterparts as threats continued to increase during the pandemic.

As the benefits of the solution increased, additional use cases emerged, revealing areas where there were blind spots in necessary visibility to assure the digital experience for doctors, nurses, and medical staff throughout the distributed healthcare campus. With IT leadership at the medical center fully endorsing packets as the source of truth for both performance and security, the IT and SecOps teams took the opportunity to leverage the packet data collected in the ISNGs for other security challenges they were facing. However, the unique demands of security use cases would require longer retention of packets than the network operations group was currently supporting. This would need to be addressed, as well.

Solution in Action

In incrementally enhancing their existing NETSCOUT nGeniusONE, ISNG, and nGenius PFS deployment, the medical center NetOps team deployed ISNG 9800 Series software appliances to other key data center locations for both performance management and security visibility and protection. They also used the opportunity to extend storage for some of their existing ISNG appliances to ensure packet retention was available to meet the needs of their security incident response requirements going forward. The Security team also added Omnis Cyber Intelligence and Omnis Cyber Adaptors to use the packet data from all the ISNG appliances for securing the healthcare network and resources.

To pull the project all together, the medical center IT staff leveraged their existing relationship with the NETSCOUT's Visibility as a Service (VaaS) team, providing 24 x 7 x 365 managed support of the NETSCOUT solution. The organization had already realized a rapid return on their initial investments in the NETSCOUT solution when the VaaS team was able to quickly configure and operate the solution to resolve performance issues with both their Epic patient records application and their Voice over IP (VoIP) services. The goal going forward, with help from the VaaS team's expertise in both nGeniusONE and Omnis Cyber Intelligence, is to achieve swift deployment, configuration, and ongoing operation with best practices to add security visibility for this critical healthcare network and its patient-impacting applications and services.

As it pertains to the medical center's service assurance initiatives, the storage expansion of existing ISNG appliances and the deployment of the new ISNG visibility in the data center was quickly implemented and configured in the existing dashboards and workflows to extend analysis to newly monitored areas of their network. The additional visibility is providing NetOps and the VaaS teams with valuable information that is helping identify, troubleshoot, and resolve user-impacting issues throughout the healthcare network.

The Results

The vision imagined by the healthcare's CTO office executives was now being realized with the expansion of nGeniusONE performance analysis and the addition of Omnis Cyber Intelligence for security. The same packet-flow visibility from ISNG appliances provided consistent, reliable truth for ensuring performance, availability, and security of patient and medical staff-facing applications and services.

Healthcare is a 24 hours a day, seven days a week operation, and even scheduled downtime is a problem. Disruptions of any kind, either from a networking degradation or security threat, must be resolved quickly or, if possible, avoided altogether. ISNG smart data from packet analysis, feeding both nGeniusONE and Omnis Cyber Intelligence, is cost-efficient and eliminates the need for another monitoring tool for security. It is also a more efficient approach from a time commitment perspective, as the IT team only needs to implement, learn, and maintain a single solution to support two critical initiatives. This efficiency extends to the healthcare's finance department, with reduced vendor management obligations and costs.

Finally, the IT team is continuing to benefit from both quick time to value and optimizing the overall investment of their NETSCOUT solutions, with the VaaS team providing implementation, configuration, and ongoing operations for both performance and security issues. From a patient care perspective, the reliability, responsiveness, and security of this critical healthcare network is the ultimate value.

LEARN MORE

For more information about NETSCOUT solutions for the Healthcare industry, please visit:

www.netscout.com/solutions/service-assurance-healthcare

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

© 2022 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

ECS_379_EN-2201 01/2022