# NETSCOUT

# Healthcare Protects IoT devices With Network Packet Visibility

## Using NETSCOUT Cost-effective, COTS-based nGenius Packet Flow Switches



## OVERVIEW

### The Challenge

- Increased security threats against the Healthcare provider during the pandemic
- A security tool to protect IoT devices required packet visibility

### The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG® software appliances
- nGenius® Packet Flow Operating System (PFOS) for Certified 5010 Series Packet Brokers
- nGenius® Visibility as a Service

### The Results

- Ensured visibility from valuable network packets for use by both service assurance and IoT security solutions
- Optimized value of investments and overall cost of ownership with one vendor for performance management and packet broker technology
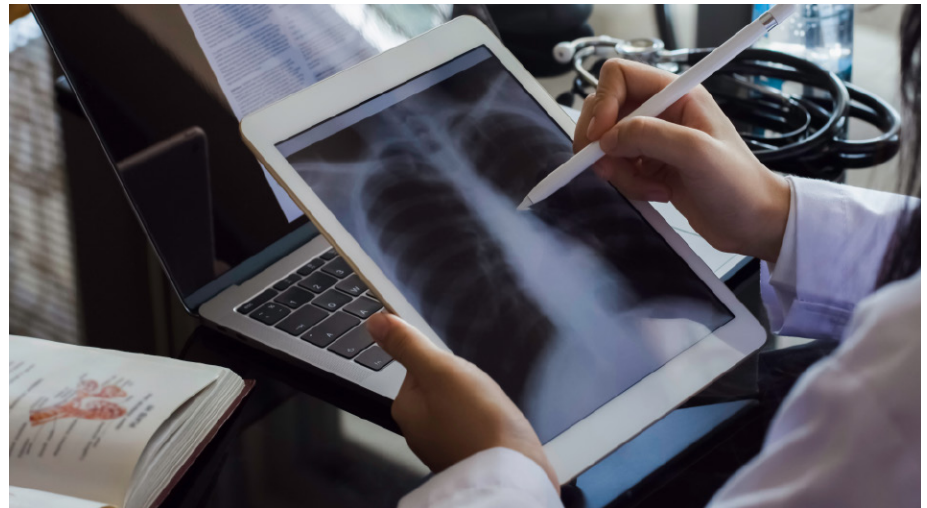
## Customer Profile

This Western U.S. healthcare system supports both a health plan program as well as a community of more than 20 hospitals and 150 clinics. Thousands of patients a week depend on the care and treatment of more than 40,000 skilled and dedicated physicians, nurses, clinicians, and staff.

Networking services and clinical applications are the priorities of the healthcare's IT staff. Like most hospitals, they rely heavily on several applications and services, including electronic medical records, as well as technology, like imaging equipment and tablets to diagnose and treat patients quickly and effectively both in and out of the hospitals. Anything that prevents availability or access to these services, or the equipment used to interact with them, need to be prevented or remediated by their IT organization.

## The Challenge

This healthcare organization was a long-time user of NETSCOUT® nGeniusONE Service Assurance solution to help maintain the quality, availability, and reliability of their clinical applications and services, including Cerner electronic medical records and their cloud-based telemedicine application. The onset of the COVID-19 pandemic presented them with several additional service assurance and security challenges.

Specifically, the healthcare provider faced challenges related to security risks and their response to them, in particular, with threats against their many and varied Internet of Things (IoT) devices. During the pandemic, healthcare organizations nationwide experienced significant increases in targeted threats and attacks. It was a priority for NetOps and SecOps teams to work together in reducing the threats and investigating potential incidents of compromise, particularly with their extensive cache of distributed IoT devices.

Healthcare organizations depend on a substantial number of distributed intelligent devices, including smart phones, tablets, carts on wheels (COWs), and smart beds, just to name a few. As networked packet traffic is the preferred source for data intelligence for the solution used by this healthcare center to secure their IoT devices, the IT team needed ways to share that data between both the IoT security tool and their NETSCOUT Service Assurance solution.

## Solution in Action

Securing the healthcare's IoT devices, during an unprecedented pandemic, from the onslaught of nefarious threats was a main concern for their security team. The tool that had been selected for IoT security leveraged packet data, just like the NETSCOUT nGeniusONE Service Assurance solution. The NetOps and SecOps teams highlighted cost-effectiveness, advanced features, and Custom-off-the-Shelf (COTS) capabilities as their reasons for selecting the nGenius® Packet Flow Operating System (PFOS) for Certified 5010 Series Packet Brokers.

Jointly, NetOps and SecOps at the healthcare organization designed a targeted implementation strategy for their nGenius 5010 Packet Flow Switches. They deployed several distributed nGenius 5010's to tap the network in strategic segments throughout the data centers, hospitals, and medical buildings to simultaneously feed the appropriate packet data downstream to the respective InfiniStreamNG appliances for performance management and to the IoT devices for cybersecurity analysis.

The flexible configuration and filtering capabilities of the nGenius 5010 proved invaluable in ensuring the right data from each location was forwarded to the service assurance ISNGs, as well as to the IoT security devices. Profiles for the type of traffic necessary for the particular use case streamlined the process and ensured the data is there when needed.

## The Results

This healthcare IT team is continuing to work strategically and collaboratively with its visibility partner, NETSCOUT, to meet the unique, critical demands that emerged during the pandemic and the ongoing security requirements. They are reducing the risk of cyber threats by leveraging the addition of the nGenius® 5010 Series Packet Flow Switches to feed network traffic to their IoT cybersecurity tool. This helps keep devices safe and available for use by their medical community providing life-saving treatment to their patients.

The healthcare organization is also benefiting from the vendor and tool consolidation that comes with sourcing NETSCOUT for the network and application service assurance solution, the packet broker technology, as well as the outsourced manage support services. Today, as doctors, nurses, and staff depend on their network and clinical applications 24 hours a day, 7 days a week, 365 days a year, there simply is NO down time in a hospital. NETSCOUT is helping ensure secure performance and availability of applications, services, and devices for this healthcare organization.

## LEARN MORE

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

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

---

**NETSCOUT®**