Health Care Gains Visibility for Service Assurance & Security of Patient-Impacting Services

NETSCOUT nGeniusONE & AED Combined to Protect Performance & Availability of Health Care Applications

OVERVIEW

The Challenge

- Needed visibility at data center DMZs to assure performance and availability of healthcare applications
- Reduce time to troubleshoot issues and pinpoint cause of disruptions and security threats

The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG® software appliances
- Arbor Edge Defense
- ATLAS® Intelligence Feed
- Software-based nGenius® 5000 series Packet Flow Switches

The Results

- Protected availability & performance of patient-impacting services
- Reduced MTTR for disruptions with evidence and improved team collaboration

Customer Profile

A leading U.S. health care provider, this 100-year old non-profit delivers both health insurance and health care services across member hospitals, medical centers, and group practices serving the needs of their community. Beyond operating a Level 1 Trauma Center and several hospitals, more than 1,600 physicians and 30,000 employees deliver exceptional care to millions of admitted and walk-in patients annually. These front-line workers provide exceptional care and treatment in the health care's 40+ specialty areas, including cardiology, neurology, orthopedics, oncology, and more. As the organization makes teaching and research a cornerstone of their services, they are regarded as a premier academic medical center.

The Challenge

For this health care provider, digital transformations have been a part of their success. The staff depends heavily on the availability and performance of their electronic medical record (EMR) applications, telemedicine and patient portals, enterprise resource planning services, as well as patient monitoring software. The IT staff at the health care had strategically deployed these services across redundant data centers and behind secure DMZs.

The year 2020 was unlike any health care had seen, with unimaginable patient volumes associated with the COVID-19 pandemic that pushed physician and staff support to its highest levels ever, with many doctors checking in remotely on patients' treatment even when off duty. It was further complicated by a workplace shift for many of the hospital's employees. Finance and accounting personnel were just some of the staff now working from home and requiring remote access via virtual private network (VPN) or virtual desktop interface (VDI). Dramatic increases in security threats from distributed denial of service (DDoS) and ransomware attacks presented an unprecedented need for comprehensive visibility at these data centers to protect against either performance or security-related issues.

Disruptions at the access point are challenging for any organization - even just determining if it is performance or capacity-related or if it's a potential security event can be time-consuming and impact staff access to vital resources. And for a health care organization, time lost determining which of these two areas is involved, and how to then pinpoint the exact nature of that issue would mean the difference between a quick, successful resolution or a protracted, patient-care disrupting event. This IT organization's goal was to implement solutions to enable rapid identification of the issue type and timely ways to restore or mitigate it with minimal disruption to clinical services.

As a long-time user of NETSCOUT's nGeniusONE Service Assurance solution with InfiniStreamNG (ISNG) appliances and vSTREAM™ virtual appliances, the IT team had leveraged the real-time packet flow monitoring and Adaptive Service Intelligence™ (ASI) technology analysis in the core of their data center and in the virtualized environments. They were well-versed using the solution to monitor and triage their Epic, MyChart, PeopleSoft, and Carescape clinical applications, among many others. Time and again, the IT team had successfully used the nGeniusONE solution to quickly pinpoint and resolve issues to ensure reliability and usability of clinical services. The network team at the health care turned to their NETSCOUT team to understand the best way to gain visibility for activity coming into their data centers at the DMZ. Showing great forethought and planning, they included members of their security team at the same time to cover all the visibility requirements simultaneously.

Solution in Action

Following a thorough review of available approaches, the health care network and security teams decided on expanding their existing nGeniusONE solution for network and application service assurance coming into the data centers at the DMZ, as well as the addition of NETSCOUT's Arbor Edge Defense (AED) and ATLAS Intelligence Feed solutions for DDoS on the outside of the DMZ. The following highlights how the solutions operate for the health care's needs:

For Service Assurance at the redundant data centers - The IT team added to their nGeniusONE deployment with:

- **InfiniStreamNG** 9000 series certified software appliances with support for up to 40GB for packet-based, real-time monitoring of critical patient care applications.
- **nGenius Packet Flow Switches** 5000 series certified software appliances to collect, distribute and aggregate network traffic from various links to the ISNG appliances, as well as other cybersecurity tools.

By adding to their existing nGeniusONE deployment, the health care gained visibility at the DMZ that expanded analysis capabilities to the edge of their environment, which enabled the IT team to identify and analyze activity for issues impacting their networked applications and service, including:

- Proactive service assurance with early warning alarms to identify when performance of their Epic EMR, Citrix, Oracle database, HTTP, and other services are experiencing responsiveness issues, providing valuable evidence to more rapidly pinpoint the cause.
- Troubleshoot issues involving complex, multi-tier application services, such as Epic, that may include web and supporting services like HTTP, DNS, and LDAP, as well as virtualized services, such as their Citrix VDI, and other services in their VMware environment, that otherwise make troubleshooting the true source of degradations among the individual application components quite difficult.
- Analyze internet access issues to stay ahead of problems such as bandwidth constraint - either caused by performance issues such as high remote access use, QoS misconfiguration settings on voice and data traffic, and bandwidth-intensive imaging file transfers, or that may be coming from potential security threats (e.g., denial of service events).
- Anomaly detection by traffic type for performance and security violations with ability to recognize unidentified applications and potential malware threats.

As a result, the IT had access to broader and more complete analysis, with visibility from the core to the edge of their data center. It will proactively assist in troubleshooting critical patient care services that traverse the full path of the infrastructure, including virtualized environment, and ensure that they are performing optimally.

For **Security Visibility** at the redundant data centers - The IT team selected and deployed:

- **Arbor Edge Defense** appliances with 10GB support for DDoS visibility on the network edge that leverages its stateless packet processing engine to automatically detect and stop both inbound threats and outbound (command and control) communication from internal compromised hosts.
- **ATLAS Intelligence Feed (AIF)** that provides advanced insights, based on potentially millions of Indicators of Compromise (IoCs) from NETSCOUT data collection and analysis and other 3rd parties. As new attack information is discovered, AIF is updated, and changes are delivered automatically via a subscription to AED over a secured SSL connection, arming the health care security team with the latest threat intelligence necessary to thwart modern-day DDoS attacks or advanced threats.

For this health care, the addition of AED and AIF to their NETSCOUT deployment provided their IT team with visibility at the DMZ that will protect their environment from outside cyber-attacks targeted to disrupt their patient-impacting services by:

- Stopping DDoS attacks as large as 10 Gbps leveraging the AED's stateless packet processing technology, which can stop TCP-state exhaustion attacks that target and impact stateful devices such as Next Generation Firewalls (NGFW).
- Improving ways to deal with DDoS attacks with capability to have AED's Cloud Signaling functionality automatically route large DDoS attacks upon their inception to one of NETSCOUT's Arbor Cloud global scrubbing centers for mitigation to "scrub" away bad traffic and resend clean traffic back to the health care's links to process as normal.
- Enforcing threat intelligence at the network perimeter to stop inbound DDoS attacks and outbound communication to known bad sites based on the millions of IoCs from NETSCOUT AIF and 3rd parties.

The Results

The IT team in this award-wining health care organization has a reputation for ensuring their clinical application services have high availability and quality performance – after all, it is critical to their patients' health care and treatment. With this latest deployment of ISNG appliances, nGenius Packet Flow Switches, and Arbor Edge Defense with ATLAS Intelligence Feed, they have taken yet another step toward gaining critical visibility to now enable both Service Assurance and Security Protection at the data centers' DMZ!

Suffice it to say, early detection and actual traffic and application analysis reduces the time to understand if the disruption relates to performance degradations or DDoS threats, expediting time to troubleshoot, rectify and/or remediate as appropriate. The lower mean time to restore (MTTR) availability and/or performance improvement for critical services helps to avoid delays in potentially life-saving patient care and treatment.

The health care is also benefiting from the vendor and tool consolidation that comes with sourcing NETSCOUT for both the service assurance solution as well as the DDoS protection solution. It is more cost-effective, with ability to leverage the existing investment in nGeniusONE to gain the visibility at the DMZ from the new ISNG COTS appliances. It is also less costly from an expense and training perspective to manage one vendor and solution set. Team collaboration between the network and security teams is enhanced, with ability to share data and strategy when evaluating disruptions at the DMZ.

Today, more so than ever, doctors, nurses, and staff depend on their network and clinical applications twenty-four hours a day, seven days a week, 365 days a year - there simply is NO down time in a hospital. NETSCOUT is helping ensure performance and availability with service assurance and DDoS protection.

LEARN MORE

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

https://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