Omnis Cyber Intelligence Brings Value of Packet Data for Faster Incident Response

OVERVIEW

The Challenge

- Cybersecurity team needed help with Incident Response and Remediation
- Cybersecurity team had to replace a NetFlow-based cybersecurity solution that had a pending End of Life

The Solution

- Added Cyber Adaptor to existing NETSCOUT® InfiniStreamNG® (ISNG) deployment for use with Omnis® Cyber Intelligence
- Expanded ISNG deployment with Cyber Adaptor for use with Omnis Cyber Intelligence
- Leveraged NETSCOUT Smart Data consisting of packets and metadata infused with ATLAS® Threat Intelligence

The Results

- Network team expanded ISNG deployment using cybersecurity team's budget
- Security team transitioned from their NetFlow-based EOL solution to a packet-based solution that provided much wider and deeper visibility
- Better actionability from Threat Intelligence for faster detection, investigation, and remediation
- Bridging both network and security perspectives for improved Network Operations and Security Operations collaboration

Customer Profile

For 60+ years, this company has provided the best in healthcare and the latest in medical technology, leveraging a network of more than 100 clinics and multiple major hospitals.

This company was happy with their previous year's purchase of NETSCOUT ISNG and nGeniusONE Service Assurance solution to ensure the performance and availability of their critical patient care and medical records applications. Seeing the value of a packet-based monitoring approach, the team wanted to expand on this investment and explore what more they could get out of the data, specifically for forensics purposes to help the Security Incident Response Team identify and remediate threats quickly and effectively. Both network operations and security operations teams reported to the assistant CTO, which helped bridge communication, foster collaboration, and show value to both organizations.

The Challenge

The Network Operations team (NetOps) wanted to expand their existing ISNG deployment but didn't have the budget, so they approached the Security Operations team (SecOps) to show them the enhanced value of their packet-based solution vs. the NetFlow-based solution the security team was currently using. The SecOps team's existing NetFlow-based platform was approaching end of life and required a significant investment to upgrade. With this issue, the SecOps team was interested but hesitant in a new platform, because they didn't fully understand the capability of packet-derived data and preferred their existing NetFlow-based platform. The team used this platform on a daily basis, and that familiarity provided a lot of comfort to them.

They believed this NetFlow-based solution was providing adequate information for them to be successful at identifying, investigating, and remediating threats. However, the team was open-minded throughout these conversations, coming to see the gaps in detail using NetFlow, such as identifying individual IP addresses using a particular protocol. They began to understand and value the different types of information that packet-based data would be able to provide.

Solution

After evaluating the value of packet-based monitoring, NETSCOUT's Omnis Cyber Intelligence technology, and the added benefit of tool consolidation, the executive team determined packet-based monitoring was the best approach going forward, with NETSCOUT providing the best solution for both service assurance and security purposes. Using a single source of packets and metadata that provided value to the NetOps team, via NETSCOUT nGeniusONE, and value to the SecOps team via Omnis Cyber Intelligence helped bridge the gap between security and network operations.

More specifically, with Omnis Cyber Intelligence, the security team can leverage their existing NETSCOUT ISNG investments for Smart Data, which is derived from:

- NETSCOUT's patented Adaptive Service Intelligence® (ASI) technology, which transforms wire traffic into smart data, providing real-time visibility into user experience for the most advanced and adaptable information platform to ensure security, manage risk, and drive service performance.
- Along with NETSCOUT ATLAS Intelligence Feed®, a highly curated, threat intelligence feed for detection of DDoS and other cyber threats. This combination helps turn massive amounts of wire data into actionable insights for efficient cyber threat detection and investigation.

By bringing more contextually rich, packet-derived data, the SecOps team can go beyond viewing mainly lateral movement, which was what they were relying on previously with their NetFlow-based solution. They are now able to see the origin of the attack, associated people and assets that may be impacted, and the ability to reconstruct and visualize the entire attack chain. Additionally, by being able to bring in ATLAS threat intelligence and use it to find threats within this data, forensics became more effective and efficient with the ability to perform guided contextual or ad hoc, unguided investigations to determine extent of breach and necessary remediation.

The Result

By moving to a packet-based monitoring approach and leveraging it for both network and security purposes, the security team was able to efficiently investigate threats to better understand them and determine risk and/or actions to take based on that risk.

Both NetOps and SecOps teams can collaborate to identify and manage issues more effectively to determine if the issue is related to network or security concerns. This allows both teams to view the same data, but from different perspectives, to gain better insights and remediate issues faster. This also resulted in significant capital expense savings by consolidating their tools and avoiding a very costly upgrade with their previous solution.

In addition, the Incident Response Team now can quickly and effectively identify and remediate threats, thereby reducing the impact from cyber-attacks that could put patient lives at risk and expose sensitive personal health records to exfiltration and ransomware.

LEARN MORE

For more information about NETSCOUT solutions visit:

www.netscout.com

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

SECCS_024_EN-2201 01/2022