NetSecOps Collaboration

Traditionally Network Operations and Security Operations teams have operated in their own silos mainly due to different goals. Network teams focus on facilitating access to information and devices, while security teams focus on limiting access to information and devices. They also have different responsibilities; network teams implement and manage the network while the security teams monitor and determines if a network is secure. Even how they measure success is different for these two teams; network is based on performance, quality, and speed while the security team's success is based on compliance, risk reduction and protection.

This results in disparate tools and leads to blind spots within the network which bad actors can exploit. Furthermore, if/when a threat is detected, it can take days/weeks/months to investigate, contain and remediate the issue due to lack of communication and collaboration between the two teams.

How NetScout Helps

Comprehensive Visibility Without Boarders – Provides a single source of smart network derived data (Smart Data) for more efficient service assurance and cybersecurity

Shared Data – Gives both NetOps and SecOps the ability to view the same network-derived data, with a different lens of network and application performance via nGenius and the lens of cybersecurity via Cyber Investigator, to collaborate and quickly act on that data to prevent further damage to the organization.

Investigation – Omnis® Cyber Intelligence to mine NETSCOUT® Smart Data for real-time, high-quality insights that power highly contextual investigation and threat hunting.

The components and functionality of the Omnis® Network Security Platform and InfiniStreamNG® are:

InfiniStreamNG and vSTREAM® – Network instrumentation for pervasive network visibility, no matter where that network resides, and is available as an appliance, COTS and virtual. Packet collection converts packets to Smart Data through Adaptive Service Intelligence® (ASI), and provides local storage of packets and metadata for investigation with Cyber Investigator.

Omnis Cyber Intelligence – Central console for network-based threat/risk detection and contextual threat investigation using network-derived Smart Data and packets collected via InfiniStreamNG instrumentation. Has bi-directional integration with SIEM/SOAR providing the ability to send alerts to the SIEM and enable contextual investigation from the SIEM. Omnis Cyber Intelligence also integrates with Omnis Arbor Edge Defense® (Omnis AED) and can receive alerts from AED and/or configure it to mitigate threats as well as support for 3rd part mitigation (e.g., firewalls).

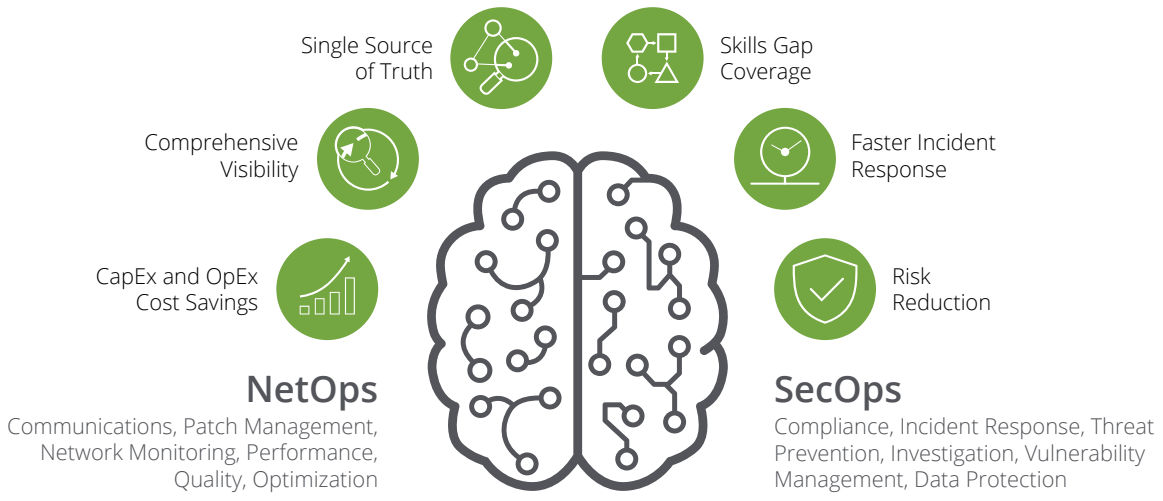

Figure 1: Benefits of collaboration while maintaining team responsibilities.

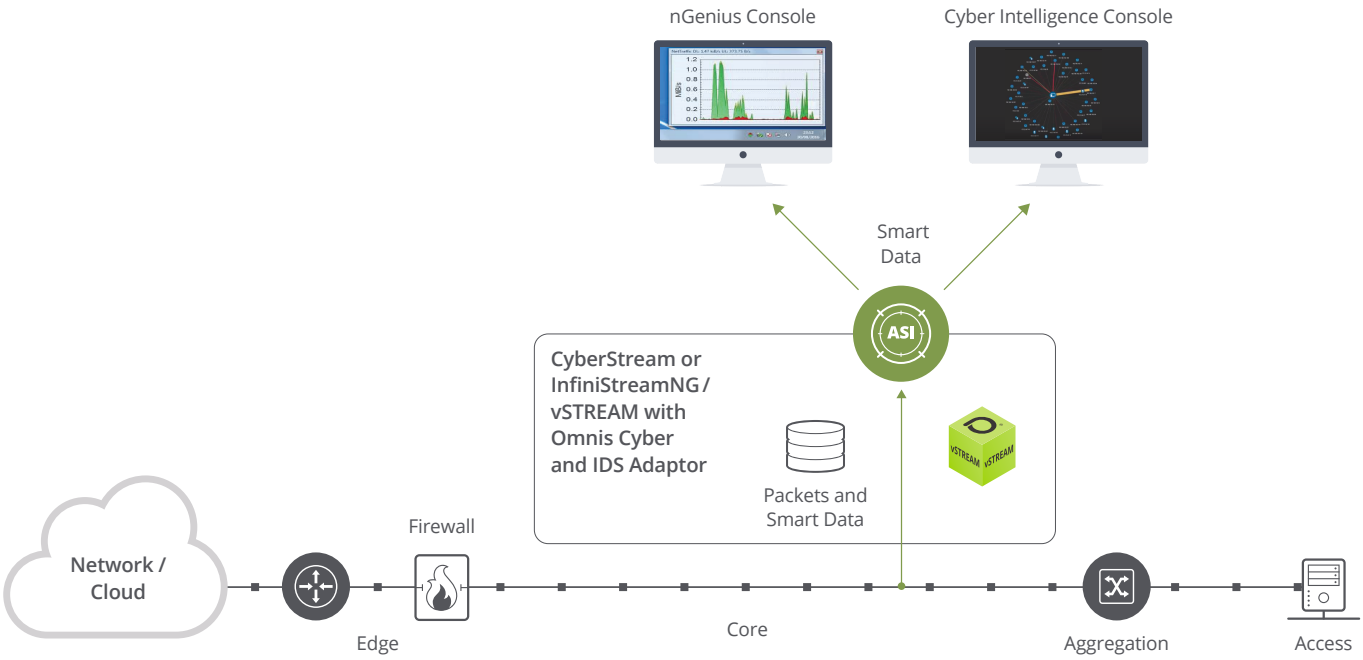

Figure 2: Wire data moving throughout the network.

NETSCOUT ATLAS Intelligence Feed® – Highly curated, threat intelligence for detection of DDoS and other cyber threats. Feeds Omnis Arbor Edge Defense, and Cyber Intelligence enabling network-based detection and mitigation. Backed by ATLAS® global visibility.

nGeniusONE® Service Assurance Platform – is a real-time information platform that provides a single pane of glass to view the data, voice, and video service delivery performance to manage both the availability and quality of the user's experience.

ASI Technology – 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.

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