Enhancing Global Financial Services Cybersecurity With Smart Edge Protection

Reduced Time to Value With Incremental NETSCOUT Service Edge Visibility

OVERVIEW

The Challenge

Expanded threat landscape in remote business operations geography

The Solution

- NETSCOUT® Omnis™ Cyber Intelligence with Cyber Adaptor for use with InfiniStreamNG®
- NETSCOUT Certified Packet Flow Operating Software, Packet Flow Switch (PFS), PFS Fabric Manager, and PFS Monitor
- nGenius® Decryption Appliance
- NETSCOUT Remote Services Engineer

The Results

- Enhanced threat management solution secured remote financial business operations
- Increased NetOps and SecOps integration, with single-vendor service assurance and cybersecurity approach

Customer Profile

With a history spanning 75+ years, this global company offers diverse insurance policy products for commercial and personal customers.

During the early phase of COVID-19, the Executive Team authorized tens of thousands of employees to move from regional headquarters and remote offices to work-from-home (WFH) environments. While this transitioned insurance service delivery from face-to-face exchanges to online, voice, and video communications, the company still reported double-digit growth across their business and personal lines during their most-recent quarterly financial filing.

For years, the company has relied on NETSCOUT technology to assist with transformative Network Operations (NetOps) and Security Operations (SecOps) projects involving infrastructure monitoring and remote office visibility, Unified Communications (UC) and business application monitoring, and virtual platform transitions. The SecOps team extrapolated further NETSCOUT value by using InfiniStreamNG (ISNG) smart visibility technology for real-time network traffic monitoring, with the nGeniusONE® Service Assurance platform employing smart data derived from those network packets for accurate analysis and forensic data for multiple cybersecurity initiatives.

The Challenge

In response to rising cybersecurity threats accompanying the company's global hybrid workforce transition, the SecOps team oversaw ongoing architectural and environmental reviews to assess their enterprise-wide security profile. One such review identified the presence of significant security risks in one region's business operations environment, which resulted in SecOps articulating an immediate need to enhance their network visibility, threat intelligence, mitigation controls, and forensic capabilities.

These findings prompted the Executive Team to establish a project to enhance the company's network security posture and evaluate several leading Network Detection and Response (NDR) vendors capable of providing a solution to their immediate cybersecurity requirements.

Solution in Action

After evaluating multiple vendors, the company's Executive Team determined that NETSCOUT's Omnis Cyber Intelligence (OCI) was the NDR platform best-suited for their remote operations cybersecurity requirements. Beyond addressing their immediate regional cybersecurity requirements, OCI has provided the company with an enterprise-wide network threat and risk investigation solution that helps reduce the impact of cyber threats across the business. OCI offered several additional features of paramount value to SecOps, including:

- Detecting emerging, targeted, and unknown threats as they traversed the network.
- Monitoring the timing and movement of attackers across north/south network traffic traversing in and out of their data center environments.
- Providing capabilities to export data to internal data lakes for future, long-term historical analysis.

While there were other standalone approaches from which to choose, OCI offered the company several distinct advantages in the context of security operations and extracting extended value from their NETSCOUT environment, including:

- Enhanced, rather than disrupted SecOps workflows by integrating with Splunk Security Information and Event Management (SIEM) and Palo Alto Cortex Security Orchestration, Automation and Response (SOAR) investments for controls and mitigation.
- Accessed the highly reliable metadata employed in other NetOps/SecOps project successes, with OCI NDR analytics also using NETSCOUT smart data generated by patented Adaptive Service Intelligence® (ASI) technology in already-deployed ISNG appliances.
- Cost-effectively elevated the value of service edge visibility sources operating in their global data centers and remote locations by configuring the Cyber Adaptor on their ISNG appliances to serve as a single data source for both OCI and nGeniusONE, thereby offering NetOps and SecOps access to pervasive NETSCOUT smart data generated from their network traffic, as well as packet-based forensics.
- Provided extended network packet retention for security audit support.

Based on SecOps' analysis and recommendations, the Executive Team also recognized that in addition to investing in the technology, they needed to mature their operational model around controls and mitigation and integrate this as part of their security ecosystem. In collaborating with SecOps to address these cybersecurity challenges, NETSCOUT designed a robust global packet flow network and decryption solution that complemented their installed packet flow switch (PFS) investments by adding:

- NETSCOUT Certified Packet Flow Operating Software, PFS appliance, PFS Fabric Manager, and PFS Monitor technology.
- nGenius Decryption Appliance, which addressed previously lacking visibility into encrypted packets necessary for analysis throughout cybersecurity operations.
- NETSCOUT Remote Services Engineer for expertise in operating, configuring, and interpreting the overall service assurance and cybersecurity solutions from NETSCOUT.

The Results

By extending their business technology partnership with NETSCOUT, the company is achieving IT goals — specifically providing the means to respond faster to the most-severe threats, reduce the potential of associated financial loss, extend the value provided by earlier capital investments, and set the stage for globally scaling their NDR solution across other business geographies in a controlled manner.

The company's use of a singular NETSCOUT approach for service assurance and cybersecurity solutions helps manage capital expenditures, reduce vendor management activities, and support extended NetOps and SecOps integration efforts.

LEARN MORE

For more information regarding NETSCOUT solutions for Assuring Availability and Performance for the Insurance Industry, visit:

www.netscout.com/solutions/insurance

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

© 2021 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.