Global Insurer Meets State Regulations for Secure Networks with NETSCOUT Cybersecurity Analytics

Assures Availability and Performance through Workload Migrations to Cloud and Co-Lo's with nGeniusONE Real-time Visibility

OVERVIEW

The Challenge

- **Phase 1:** Forensic security and packet-based visibility needed for compliance with new State requirements for financial institutions
- **Phase 2:** Cloud outage impacts services from co-lo facility, prompts CISO to seek enhanced visibility and performance analytics

The Solution

- nGeniusONE® Service Assurance platform
- InfiniStreamNG™ appliances with ASI-generated NETSCOUT® smart data

The Results

- Timely compliance with State requirements protects customer business operations and brand reputation
- Better-assuring workload migration to Azure/AWS cloud services and Equinix Co-lo environments

Customer Profile

This international insurance and financial services company is a market leader, administering more than $500 billion in assets for 9 million customers.

The company offers a broad portfolio of financial and benefit plan solutions for individuals, families, and businesses. They provide a wide range of retirement savings and income plans, as well as life, disability, and critical illness insurance.

The Challenge

The company's Security Operations (SecOps) team faced new business and compliance management challenges that were surpassing current IT toolset capabilities. The New York State government had enacted requirements upon any financial institutions that required those businesses operating in NY to:

- Implement cybersecurity measures, including endpoint protection, firewalls, and data loss prevention solutions
- Report data breaches, including the origin, affected company location(s), and any adverse impact to organizational assets
- Identify whether the threat traveled past the point of initial infiltration, as well as any impact to customer data
- Provide associated network packet captures as further evidence of effective forensic security analysis used to successfully troubleshoot the breach, thereby proving the IT environment had not been compromised

While the SecOps team had in the past implemented security tools and established reporting mechanisms, those solutions were not providing network traffic visibility or the packet-based forensic support required for the State-mandated post-incident analysis. Complicating matters: the company had to deploy a complete solution in an accelerated timeframe in order to meet a State-specified deadline for organizational compliance; otherwise, the business would be subject to government fines and adverse impacts to brand reputation.

While the SecOps team focused on finding a solution to address their network visibility and security compliance issues at their New York data center, the company's data center transformation challenges were also grabbing the attention of their Chief Information Security Officer (CISO). As part of strategic business initiatives, the company decided to move certain data center workloads to cloud-based Amazon Web Services (AWS) and Microsoft Azure (Azure) platforms, as well as newly added Equinix co-location facilities. In sequentially transitioning workloads in this manner, the company looked to reduce data center costs and provide operational efficiencies. However, when an Equinix co-lo facility reported an outage with Azure services, the CISO learned the company's existing IT toolsets lacked visibility into this new hybrid cloud environment necessary for troubleshooting and remediating performance anomalies, so that business services could be quickly restored for customers and users.

Facing these collective challenges, the company needed a vendor solution that could be deployed quickly to meet the near-term security compliance requirements, while offering sustained visibility and performance monitoring to assure that ongoing workload migrations to the AWS, Azure, and Equinix environments did not impact business service performance and availability for customers or employees.

Solution in Action

The company is addressing their emerging security, compliance, service assurance, and cloud monitoring challenges by leveraging the NETSCOUT nGeniusONE Service Assurance platform across US business operations.

In initially tackling the State's security compliance challenges, the SecOps team installed InfiniStreamNG (ISNG) appliance technology to gain the visibility they had lacked into networked application traffic coming in and out their data center environment. The ISNG uses integrated NETSCOUT Adaptive Service Intelligence (ASI) technology to convert the company's packet-based traffic into smart data, with nGeniusONE's performance analytics using this metadata to provide real-time visibility required to ensure security and manage business service performance. The SecOps team has eased the evidentiary compliance process with the State by using nGeniusONE contextual drill-downs from Service Dashboard and Service Monitor views into:

- Corresponding, specific session-level analysis, ladder diagrams, with hop-by-hop transaction analysis to help identify specific issues
- Packet-level analysis and forensic evidence collection relevant to the issue at hand, based on the initial nGeniusONE workflow

Additionally, the SecOps team is now gaining critical visibility into company workloads throughout the Azure and AWS platforms, with nGeniusONE using ISNG technology installed at the Equinix co-lo and ASI-generated smart data for proactive monitoring of the business services operating in this hybrid cloud environment.

nGeniusONE-generated Service Alerts are providing the SecOps team with early-warning analysis of issues in their data center and cloud environments. As a standard practice, findings from nGeniusONE are included in the team's Incident Reports.

The Results

As a result of their successes with reconciling both State-level security compliance issues and cloud performance challenges, the SecOps team acquired the internal cachet necessary to lead a more-coordinated data center transformation effort. Based on the SecOps team's positive experiences with nGeniusONE analytics and ISNG data sources, the CISO has included NETSCOUT's technology in the company's data center transformation "template." Moving forward, the company will factor nGeniusONE in their expanding move to hybrid cloud environments, as well as architecting a next-generation disaster recovery architecture.

Ultimately, it is the company's customers and users who benefit from these improvements, with proactive business service and security monitoring enhancements leading to reliable execution of insurance and financial transactions across the business. The secondary benefit is the avoidance of potentially high fines and reputational damage if compliance with regulatory requirements had not being achieved.

LEARN MORE

For more information about NETSCOUT Insurance Industry Cybersecurity Solutions, please visit:

https://www.netscout.com/solutions/digital-transformation-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

ECS_232_EN-1901 12/2019