APAC Financial Leader Complying with Central Bank Cybersecurity Challenges with NETSCOUT

Extending nGeniusONE Platform and NETSCOUT Smart Visibility to Manage Cyber Risk, Assure E-Banking Services

OVERVIEW

The Challenge

- New Central Bank guidelines require institutional compliance with cybersecurity measures
- Financial growth tied to always-available digital banking platforms

The Solution

- nGeniusONE® Service Assurance platform, with smart performance analytics
- InfiniStreamNG™ appliances and extended storage units, with ASI-generated NETSCOUT® smart data
- nGenius® 5010 packet flow switch appliances

The Results

- Bank's regulatory compliance protects customers from cyberthreats and risk
- Extending NETSCOUT use reduces CapEx and associated tool and vendor churn, enhances ROI

Customer Profile

This leading Asian-Pacific (APAC) bank has enjoyed sustained financial growth in the last decade by capitalizing on market expansion in emerging Indo-China countries, as well as increasing returns in the corporate lending and investment businesses.

The bank has also recognized the financial benefits associated with helping lead the growth of the country's electronic payment (e-payment) ecosystem, with the institution's mobile and internet banking platforms experiencing double-digit growth in client use on a year-over-year basis. Today, 18,000+ employees support the banking transactions of more than 10 million customers in the region.

Recognizing the importance of high-quality customer experience in the highly competitive APAC marketplace, the bank's Network Operations (NetOps) team has used NETSCOUT performance assurance and smart data solutions for 10 years to lead their troubleshooting and forensic security activities.

The Challenge

Like other national business leaders, this institution's management team was working to assess the impact of a new Risk Management in Technology policy developed by the country's Central Bank to better regulate the information technology (IT) environments deployed by regional financial and insurance companies.

Developed to factor earlier Central Bank governance ranging back more than 15 years, the policy was to become effective on January 1, 2020, addressing the following requirements areas:

- Technological risk safeguards
- Cyber resilience
- Cyber risk solutions

With the Central Bank's history of levying multimillion-dollar fines for non-compliance with other government financial policies, there was some urgency across the bank's NetOps and Security Operations (SecOps) teams to assess the technological and cybersecurity compliance readiness offered by their existing IT environment.

To meet government standards and avoid the potential of future Central Bank financial penalties, the collective IT team coordinated an internal gap analysis to identify potential compliance and network visibility shortfalls, then began identifying possible vendor solutions that would assist in those areas.

Solution in Action

The bank is compliant with the Risk Management in Technology guidelines for cybersecurity using their production-level nGeniusONE platform and NETSCOUT smart data sources to meet relevant requirements, while also deploying additional InfiniStreamNG™ (ISNG) appliances with Adaptive Service Intelligence™ (ASI) technology and nGenius packet flow switch (PFS) appliances at their remote data center and disaster recovery (DR) locations to close visibility and monitoring gaps. As a result:

- The bank's data center and DR locations operate mirrored ISNG and PFS appliances at each facility.
- nGeniusONE is hosted at their primary data center, with ISNG appliances forwarding ASI-generated smart data from the other data centers to nGeniusONE.
- PFS appliances optimize the flow of network packets, including e-banking network traffic, to ISNG appliances, in real-time, and the smart data is consumed by nGeniusONE for performance analytics. The PFS appliances also aggregate, replicate, distribute, and manage the flow of network packets to the bank's third-party cybersecurity tools.

The bank uses the nGeniusONE platform to maintain service availability and quality performance, as well as compliance with the following Risk Management in Technology policy areas:

- **Deployment of effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities** in its technology infrastructure: More than 30 IT users employ nGeniusONE on a 24x7, shift-by-shift basis to manage real-time monitoring of the bank's network, applications, and business services across all data center and DR locations.
- **Network security controls requiring capture of full network packets** to rebuild relevant network sessions to aid forensics in the event of incidents: ISNG appliances with Extended Storage Units (ESUs) provide the longer packet retention periods required for comprehensive security forensic activities. As a result, the bank sees as a significant differentiator in their ongoing NETSCOUT solution investment.
- **Technology Operations Management requirements for DR operational readiness** following the implementation of new or enhanced systems: With NETSCOUT operating at their DR facility, the bank benefits from hot switchover from Production-to-DR, with nGeniusONE providing real-time monitoring and troubleshooting to assist NetOps' efforts to return the production system to online status.

For a NetOps team that is "particular" about the service assurance of their online and mobile bank applications, as well transactions involving financial service providers (e.g., MasterCard and Visa), IT users can take advantage of single-pane nGeniusONE Service Dashboard and Monitor views to collectively access:

- Real-time alerting
- Timely event monitoring
- Forensic investigation of any security events

The Results

The bank was able to avoid financial penalties that could adversely impact business growth, national brand value, and continued adoption of e-banking platforms, thanks to the NetOps team's use of NETSCOUT technology to validate compliance with the Risk Management in Technology policy's cybersecurity guidelines.

While the NetOps team considered other competitive approaches to managing organizational compliance, based on the ongoing reliance on the nGeniusONE performance assurance solution, they knew they would be "flying bind" without extending use of NETSCOUT smart visibility instrumentation at their remote data center and DR locations.

The bank has been able to reduce risk and control related compliance costs by teaming with their local NETSCOUT subject matter experts to develop a multi-year strategic approach that factored phased deployment of additional NETSCOUT smart data sources at remote data center and DR locations that had not been previously instrumented with ISNG and PFS appliances.

The bank continues to enhance its return on investment from NETSCOUT technology, with the IT team extending use of nGeniusONE to:

- Assure optimal end-user experience by monitoring third-party vendor technology performance against in-place Service Level Agreements
- Ensure service up-time via real-time monitoring
- Quickly address service downtime through effective troubleshooting needed to reduce mean time to repair cycles

LEARN MORE

For more information about NETSCOUT Retail Banking solutions, please visit:

https://www.netscout.com/solutions/retail-banking

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_241_EN-2001 02/2020