Financial Institution Increases Security Posture With Omnis Cyber Intelligence

Lowering Risk with Deep Packet Inspection at Scale

OVERVIEW

The Challenge

- Migrating Datacenter for potential natural disaster purposes
- Large Financial institution with high attack volume daily
- Current solution was over 4 years old with limitations

The Solution

- NETSCOUT® Omnis® Cyber Intelligence
- Omnis® CyberStream for packet-based data sources
- MasterCare Support

The Results

- Reliable and trustworthy data to detect, investigate and respond to threats
- Deep Packet Inspection with functionality to gain the most insight on threats
- Early Warning Threat Detection to reduce mean time to knowledge and decrease mean time to resolution

Customer Profile

This is a top 5 largest financial and banking services company within their country. These services include corporate, institutional, and retail banking, insurance, trading, etc. With around $10 billion in yearly revenue and thousands of locations, over 20 million people rely on this company.

This institution is a long-standing NETSCOUT® customer, with their Network Operations (NetOps) team relying on the nGeniusONE® Service Assurance platform to visualize and monitor data center and network communication services, and their Security Operations (SecOps) team relying on Omnis Arbor Edge Defense® (AED) to block bulk (e.g. DDoS attacks, IoCs) inbound cyberthreats and outbound malicious communication. This organization knew the NETSCOUT product line, trusted the capabilities and data they were receiving.

The Challenge

As a very well-known financial institution, and like many other financial institutions, these businesses face many, highly sophisticated, security threats on a daily basis.

The company was expanding and needed to migrate their datacenter to a less risky region in the country due to potential earthquakes as a disaster recovery strategy and increment service level agreements with their customers. Their previous network detection and response solution, which they had been using for over 4 years, was not meeting the business needs in functionality, ability to scale with their growth, and customer service, which led the team to begin a replacement process. Over the years the security team would occasionally reach out to the network team for data and troubleshooting purposes, so they were familiar with the value NETSCOUT provides. When the organization put out a bid for a replacement of their current solution, NETSCOUT was invited via their channel partner. This organization really valued quality data and was looking for a deep packet inspection solution with the best functionality. They also needed a solution that can scale to match their growth and will also integrate with their current security stack, specifically Palo Alto Networks.

Solution in Action

In previous purchases of nGeniusONE/InfiniStreamNG's for service assurance and Omnis AED for DDoS protection, this account had knowledge and trust in the NETSCOUT products and wanted to leverage those purchases for cybersecurity purposes via Omnis Cyber Intelligence. NETSCOUT was capable of providing that solution to the security team but shifted to a stand-alone solution for compliance requirements.

- Omnis Cyber Intelligence is an advanced threat detection and response solution that brings deep packet inspection at scale. With its comprehensive security visibility and NETSCOUT's global threat intelligence feed, it provides the ability to detect, validate, investigate, and respond to cyber threats, whether on-prem or in the cloud promptly and efficiently.
- Omnis CyberStream deployed at key aggregation points in the network environment, to generate smart data for OCI, thus enabling SecOps to gain enterprise security views from those locations.
- Back-in-Time analysis feature for host investigations to expand the communication from compromised hosts and the existence of lateral movements via packet retention.

Using this solution, both network packets and NETSCOUT Smart Data are stored locally on CyberStream appliances, enabling Omnis Cyber Intelligence to employ unique indexing and compression techniques to store this data for long durations of time (e.g., months), allowing the SecOps team to conduct back-in-time analysis, contact tracing, and IP alerting to resolve threats.

The Results

The SecOps team enabled Omnis Cyber Intelligence to function as an Advanced Early Warning system, as it was already analyzing the network data gathered by ISNG technology and creating an inventory of all assets and looking for signs of exploitation.

Proven reliability based on previous purchases combined with Deep Packet Inspection for raw data provides confidence and trust to know exactly what happened and how to address any potential issues.

NETSCOUT is providing a common source of data that can be shared with NetOps and SecOps teams for network service assurance and security use cases—saving costs, improving efficiency, and reducing the time to investigate and remediate threats and prevent losses.

This institution now has a stronger security stack and more comprehensive view of their entire infrastructure due to integration with their Palo Alto Networks solutions and workflows for faster threat detection, investigation, and response.

LEARN MORE

For more information about NETSCOUT solutions visit:

www.netscout.com/product/cyber-intelligence

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