Enhancing Security and Compliance for a Global Government Communications Provider with Omnis Cyber Intelligence

OVERVIEW

The Challenge

- Customer base is high-level top-secret government projects, security is of utmost importance.
- Needed multiple functionalities on a single sensor (multiple divisions with distinct network subnets).
- Needed a visibility solution that can provide packet level data with ability to scale.

The Solution

- Omnis™ Cyber Intelligence (OCI) – For seamless management, visualization, and workflows for real-time and historical threat detection and investigation.
- Omnis™ CyberStream – Network sensors providing scalable Deep Packet Inspection (DPI) and multiple methods of threat detection.
- Omnis™ Data Streamer – Exporting patented ASI data to a data lake and combine it with other data sources for custom analysis.

The Results

- Omnis CyberStream provided comprehensive network observability, allowing proactive management and securing infrastructure while enhancing operational efficiency.
- OCI facilitated easy compliance monitoring of certificates, issuing immediate alerts for non-compliance to enable swift resolution.
- OCI's host group feature enabled customer-based segmentation for monitoring and rapid identification of violations, aiding in prompt remedial actions.
- The organization plans to employ Omnis Data Streamer for future data export functionality, enhancing security measures by utilizing actionable network data for proactive threat mitigation and compliance support.

Company Profile

This high-level information systems services provider caters to a global clientele of government agencies, specializing in top-secret projects where security and encryption are of utmost significance. Their services are a linchpin for multiple government agencies, supporting critical operations for a user base ranging from 3 to 5 million. As current NETSCOUT® nGeniusONE® and InfiniStreamNG® customers, they understand and trust in the value of NETSCOUT technologies and Smart Data, recognizing its crucial role in providing actionable insights for their mission-critical endeavors.

Business Challenges

The company embarked on two crucial initiatives, both focused on compliance. The first was geared towards identifying policy violations, uncovering unauthorized connections within their network. The second initiative was laser-focused on rooting out weak encryption methods like shaky SSH ciphers and vulnerable TLS ciphers. Within these initiatives came many challenges and requirements that needed to be solved such as:

1. **Monitoring Multiple Divisions:** Their first challenge revolved around the need to efficiently monitor multiple divisions, who had distinct network subnets, using a single sensor. This necessitated a streamlined network security infrastructure to handle their complex operations effectively.
2. **Scalability Requirement:** Given the company's large and highly distributed network infrastructure, they recognized the importance of a network monitoring solution that could scale to meet not only their current but also their future needs. This requirement became a cornerstone of their strategy for the right solution to their multifaceted challenges.

3. **Functionality Beyond Traditional IDS:** Recognizing the limitations of a traditional Intrusion Detection System (IDS), they sought advanced functionality that could provide a more comprehensive approach to security.
4. **Instrumentation Overload:** The company found itself inundated with a multitude of devices and instrumentation, which not only added complexity but also hampered management and monitoring efforts. They needed a path to consolidation to improve efficiency and effectiveness.
5. **Deep Packet-Based Security:** With the critical nature of their security requirements, they required Deep Packet Inspection (DPI) to effectively identify sophisticated threats hidden within network traffic and ensure compliance with strict security standards. All critical to fortify their defenses against potential threats in their top-secret government agency operations.
6. **Network Packet Data for Security Analytics:** Faced with visibility gaps that traditional approaches couldn't bridge, they recognized that only network packet data could augment their security analytics and provide a clearer picture of their environment.

Solution in Action

The implementation of Omnis CyberStream and Omnis Cyber Intelligence (OCI) addressed their challenges and provided several key benefits such as:

- **Enhanced Sensor Functionality:** With OCI, the company significantly enhanced sensor functionality, leveraging a single sensor for multiple threat detection capabilities. This not only streamlined their network security infrastructure but also reduced costs, providing a more cost-effective solution.
- **Policy Violation Detection:** OCI's policy violations feature proved invaluable by delivering real-time alerts for non-compliance events. During the proof-of-concept stage, it unveiled a shocking reality: more than half of their environment was unencrypted, contradicting their initial assumption of their entire environment being encrypted. This discovery not only bolstered security but also ensured regulatory compliance, mitigating potential risks and fines.
- **Multidimensional Threat Detection:** OCI empowered the company to deploy an array of advanced detection methods, including threat intelligence, behavioral analytics, attack surface events, compliance events, intrusion detection system (IDS) events, policy violations, and file extraction detection. This comprehensive suite of detections not only fortified their security posture but also improved their ability to proactively respond to emerging threats and vulnerabilities, reducing the potential for data breaches and ensuring data integrity.

Benefits and Results

The implementation of OCI delivered several notable benefits including:

- **Comprehensive Network Observability:** Omnis CyberStream provided this organization with a holistic view of their entre network landscape. This real-time monitoring, analysis, and reporting capability empower them to proactively manage, optimize, and secure their network infrastructure, leading to improved operational efficiency and heightened security.
- **Compliance Monitoring:** OCI allowed the company to easily monitor certificates to ensure compliance. Immediate notifications are received if any non-compliance issues arise, enabling prompt remediation.
- **Customer Segmentation:** OCI's host group feature provides the ability to gain visibility based on customer segments. This segmentation allows the company to monitor the activities of each customer group, quickly identify any violations, and take remedial actions.
- **Leveraging Actionable Data and Future Data Export Functionality:** The company plans to utilize Omnis Data Streamer for future data export functionality, ensuring they can efficiently manage and analyze data. Incorporating actionable network data export as part of an organization's security strategy can significantly enhance the effectiveness of security measures, providing more comprehensive insights, enabling proactive threat mitigation, and supporting compliance efforts.

In conclusion, this high-level information systems provider trusts Omnis Cyber Intelligence to tackle their complex security and compliance challenges. As current NETSCOUT customers, they trust and rely on NETSCOUT's Smart Data for actionable insights for their mission-critical operations. OCI streamlines their security, aids policy compliance, and offers an array of advanced threat detection methods. Data export functionality improves data management and decision-making. Compliance monitoring and customer segmentation enhance regulatory adherence and operational efficiency, fortifying their digital security and compliance efforts. They now face evolving threats with confidence and resilience.

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

SECCS_033_EN-2301 12/2023