

Enhancing Cybersecurity for a Global Financial Services BPO with Omnis Cyber Intelligence (OCI) Solution on AWS

OVERVIEW

The Challenge

The global financial services BPO faced challenges in ensuring comprehensive network visibility, rapid threat detection and response, compliance enforcement, and efficient security operations across a distributed infrastructure.

The Solution

The company deployed NETSCOUT's Omnis™ Cyber Intelligence (OCI) on AWS, leveraging deep packet inspection (DPI) for real-time network visibility, advanced threat detection, and proactive compliance monitoring. The solution integrated with AWS services to enhance security operations.

The Results

The implementation enhanced the company's security posture with improved threat detection and compliance, reduced Mean Time to Knowledge and Mean Time to Resolve, and achieved cost-effective security management, optimizing resources and consolidating security tools.

95% of surveyed organizations say NETSCOUT scalable Deep Packet Inspection (DPI) and smarter analytics required for pre-migration, during migration and post-migration to the cloud.

– TechValidate by SurveyMonkey



Customer Profile

This global BPO company is a trusted leader in strategic management and financial consulting, providing services to numerous financial institutions worldwide. With tens of thousands of employees across hundreds of offices, the company offers comprehensive business process outsourcing solutions, including risk management and compliance.

The Challenge

With a strong global presence, the company's network infrastructure is distributed across the Americas, EMEA, and Asia. The company faced many challenges, the following are some of the key security challenges:

- Global Network Visibility:** Ensuring comprehensive visibility across a distributed network that includes on-premises data centers, public clouds such as AWS, and colocation facilities.
- Threat Detection and Response:** Identifying and responding to known and zero-day threats quickly and accurately.
- Compliance and Policy Enforcement:** Maintaining stringent security policies and compliance across diverse network environments.
- Efficient Security Operations:** Reducing Mean Time to Knowledge (MTTK) and Mean Time to Resolve (MTTR) while managing security events across a complex infrastructure.

OCI Solution in Action

To address these challenges, the company implemented Omnis™ Cyber Intelligence (OCI) solution on AWS. This advanced network threat detection and response platform leverages deep packet inspection (DPI) to provide comprehensive security visibility, identify vulnerabilities, and detect threats with high accuracy.

1. Global Network Visibility and Monitoring:

- Omnis™ CyberStream is deployed across various environments, including AWS, to capture network packets in real-time, achieving speeds up to 100 Gbps. Deploying Omnis CyberStream across different environments can help ensure continuous packet capture and real-time threat detection, offering a complete view of network activities in the hybrid cloud.
- Uses Adaptive Service Intelligence® (ASI) DPI technology to extract and store layer 2-7 metadata and packet decodes, ensuring comprehensive security visibility in complex network infrastructures.
- OCI centralizes security event management, providing a unified interface for monitoring and managing security events across the global network. Consolidating this data into a single pane of glass makes it easier to monitor, investigate, and respond to threats irrespective of their location.

2. Advanced Threat Detection and Response:

- Omnis CyberStream utilizes multiple threat detection techniques, at the source of capture, including IoCs, policy violations, signature matching, unexpected traffic detection, and behavior analytics. Multidimensional threat detection methods can help ensure comprehensive coverage, leveraging machine learning algorithms for behavioral analytics to detect anomalies and threats with high accuracy.
- Integrates with AWS services such as Amazon VPC Traffic Mirroring to capture and analyze network traffic, enhancing threat detection capabilities.

3. Compliance and Policy Enforcement:

- Supports the creation and enforcement of custom security policies, continuously monitoring for compliance violations. By continuously monitoring the network for policy violations and compliance issues, Omnis CyberStream helps ensure adherence to internal and external security standards.
- MITRE ATT&CK Mapping provides prebuilt threat detection programs aligned with industry standards, enhancing compliance reporting capabilities. The integration with MITRE ATT&CK framework within OCI can provide better contextualization of threats and supports regulatory compliance efforts.

4. Proactive Threat Hunting and Investigation:

- OCI helps conduct proactive threat hunting using long-term stored metadata, identifying signs of compromise and breaches.
- Omnis CyberStream's historical data storage and packet decodes enable detailed retrospective analysis, helping to quickly eliminate false positives and providing forensic evidence for incident resolution.

- Enhanced collaboration between IT and security teams, improving overall operational efficiency.
- Evaluating OCI 3rd party integration with Splunk and AWS Security Hub to help solve security issues faster and reduce business risk.

3. Cost-Effective Security Management:

- Leveraged AWS's scalable infrastructure to manage costs effectively, optimizing resource utilization and reducing overhead associated with on-premises solutions.
- Realized significant cost savings by minimizing the need for multiple disparate security tools and consolidating security operations through the OCI solution.

By implementing the Omnis Cyber Intelligence solution on AWS, this BPO company successfully enhanced its cybersecurity capabilities, ensuring robust risk management, compliance monitoring, and proactive threat detection and response. This deployment not only fortified the company's security posture but also streamlined its operations and optimized costs, aligning with the goals of financial institutions to innovate securely in a cloud-based environment.

The Results

1. Enhanced Security Posture:

- Achieved comprehensive visibility and real-time threat detection across global network infrastructure, significantly reducing the risk of cyberattacks and fraudulent activities.
- Improved compliance with strict financial industry regulations through continuous monitoring and policy enforcement.

2. Operational Efficiency:

- Reduced Mean Time to Knowledge (MTTK) and Mean Time to Resolve (MTTR) by streamlining security event management and automating response processes.

LEARN MORE

For more information about NETSCOUT security solutions visit:

www.netscout.com/product/cyber-intelligence

www.netscout.com/technology-partners/amazon-web-services

Read and subscribe to our blog to [stay up to date on the latest news and innovations from 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