

NETSCOUT Omnis Cyber Security Solution for AWS

Illuminate Threats Everywhere, Anywhere, Anytime with Smarter Security

Challenges

Migrating workloads to the cloud is the new normal for enterprises. But this new hybrid cloud era amplifies infrastructure complexity, increases the attack surface, and limits end-to-end visibility. Limited visibility in these complex hybrid cloud environments makes it much harder to detect, analyze, and mitigate threats. Operational overhead and cost to business are compounded as the power, sophistication, and frequency of threats increase daily. Whatever the motivation, cyber threats can cause severe financial harm, reputational damage, and disrupt business continuity. SOC teams across every industry need help to secure dynamic infrastructures that span the cloud, on-premises, and network edge. Strengthening the security posture and reducing business risk, therefore, requires a smart solution to illuminate threats everywhere, anywhere, anytime.

Solution

NETSCOUT® and AWS have come together to provide smarter security with end-to-end visibility and actionable intelligence. Leveraging the power of the NETSCOUT advanced network detection and response (NDR) platform with AWS Security Hub, this solution for enterprises streamlines contextual investigations for security risks and strengthens the corporate security posture. Organizations can deliver innovative and secure user experiences by using NETSCOUT® Omnis™ Cyber Intelligence (OCI) and Omnis™ vCyberStream for AWS. SecOps teams can perform cybersecurity investigations throughout the entire network, whether on-premises or in the cloud—during and after workload migration projects to AWS. The Omnis Cyber Security solution reduces Mean Time to Resolution (MTTR). In addition, SOC teams use AWS Security Hub as a single place that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services and NETSCOUT OCI. Events and insights detected by NETSCOUT OCI are displayed in AWS Security Hub and users can do contextual drill-downs from AWS Security Hub to investigate these events further in NETSCOUT OCI. AWS Security Hub continuously aggregates and prioritizes events from multiple sources, including NETSCOUT OCI, making it easy to visualize findings and enabling insights so that SecOps teams can intervene and investigate high-severity findings.

Users can detect and conduct highly contextual investigations of security risks and cyber threats based on NETSCOUT Smart Data derived from packet data (cloud, on-premises, network edge) and IoCs (Indicators of Compromise) identified based on NETSCOUT ATLAS® Intelligent Feed (AIF) and 3rd party threat intelligence feeds using STIX/TAXII. The solution identifies threats at the packet capture source using signature matching (IDS) and behavior analytics. It also identifies malicious files by matching them with known hash datasets. What's more, the solution allows customers to create simple host group-based policies and generates events if there is a policy violation.

FEATURES AND BENEFITS

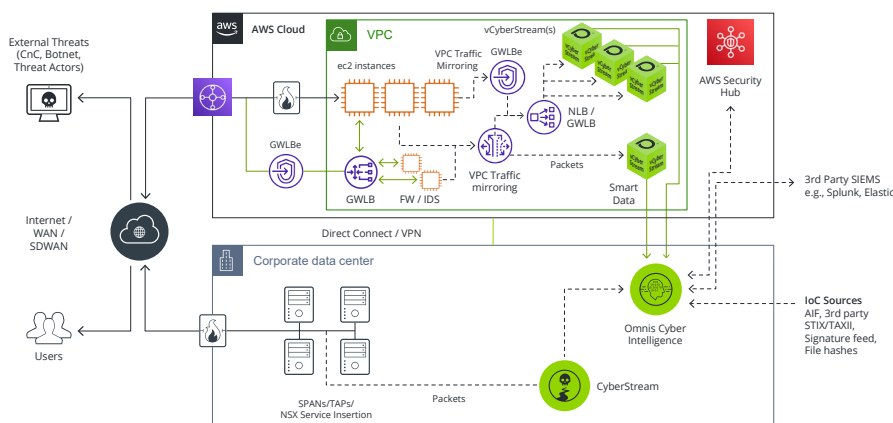
Key Benefits

- Strengthen security posture and reduce business risk by integrating NETSCOUT OCI with AWS Security Hub. This integration enables SOC teams to effectively use AWS Security Hub to aggregate, organize and prioritize findings, and conduct contextual drill-downs into OCI for investigation and forensics analysis to quickly resolve the highest priority security issues.
 - Gain visibility into threats and derive actionable insights for security issues that span AWS, multi-cloud, and on-premises environments.
 - Use vCyberStream highly scalable DPI technology to cost-effectively convert packet data, from key vantage points, into Smart Data for comprehensive network visibility and actionable security intelligence.
 - Industry leading NETSCOUT Smart Data and global threat intelligence feeds are used to proactively examine security risks end-to-end in complex geographically distributed infrastructures.
 - Identify malicious files transacted over the network through real-time detection at vCyberStream.
 - Reduces Mean Time to Resolution of cybersecurity incidents.
 - NETSCOUT solutions are AWS tested and certified.
-

NETSCOUT collaboration with AWS enables practical, affordable, and scalable access to packet data for end-to-end security visibility in the hybrid cloud. For example, using seamless integration with AWS Gateway Load Balancer, vCyberStream can effectively access large volumes of AWS packet data at scale and convert it into Smart Data, thus enabling effective and cost-efficient vulnerability and threat detection and investigation. Integrating NETSCOUT OCI integration with AWS Security Hub and 3rd-party SIEM/SOAR platforms increases security team productivity and enables them to intelligently combat cyber threats and attacks across complex hybrid cloud environments by increasing the efficiency of collecting, prioritizing, and investigating cyberthreat findings.

AWS and NETSCOUT Collaboration

Enterprise IT organizations want to rely on vendors who can demonstrate strong collaboration with AWS. NETSCOUT has achieved several qualifications to provide Visibility without Borders through interoperability with a variety of AWS services and technologies. These qualifications have been validated by AWS in the specialization areas listed below.



Sample Omnis Cyber Security Solution Deployment in AWS

The diagram above shows a sample deployment of the Omnis Cyber Security solution in AWS, illustrating the following:

- NETSCOUT Omnis vCyberStream uses ASI technology to turn packet data into Smart Data which is security metadata used by NETSCOUT OCI.
- Native AWS packet acquisition features such as VPC traffic mirroring, VPC ingress routing, and Gateway Load Balancer (GWLB) endpoint as target, enable vCyberStream to monitor network traffic from key vantage points without leaving the cloud.
- NETSCOUT OCI can export its findings to AWS Security Hub using AWS Security Finding Format (ASFF). These alerts are displayed and prioritized in AWS Security Hub with the ability to conduct contextual drill-down to investigate these and other alerts in NETSCOUT OCI.
- NETSCOUT OCI incorporates IoCs based on Atlas Intelligence Feed (AIF), curated by NETSCOUT cybersecurity experts based on analysis of over 50% of the global Internet Traffic. Other, 3rd party intelligence signature feeds and file hashes are supported in OCI via STIX/ TAXII interfaces.

AWS Validated Qualifications

NETSCOUT has demonstrated the highest level of specialization, deep AWS technical expertise, and proven customer success for all qualifications listed below.

AWS Competencies

- Networking ISV Competency
- Migration and Modernization ISV Competency
- Security ISV Competency

Partner Programs

- AWS Public Sector Partner
- AWS Marketplace Seller

AWS Certifications

- AWS Certified Security – Specialty
- AWS Certified DevOps Engineer – Professional
- AWS Certified Solutions Architect – Associate
- AWS Certified SysOps Administrator – Associate
- AWS Certified Cloud Practitioner
- AWS Certified Solutions Architect – Professional
- AWS Certified Developer – Associate

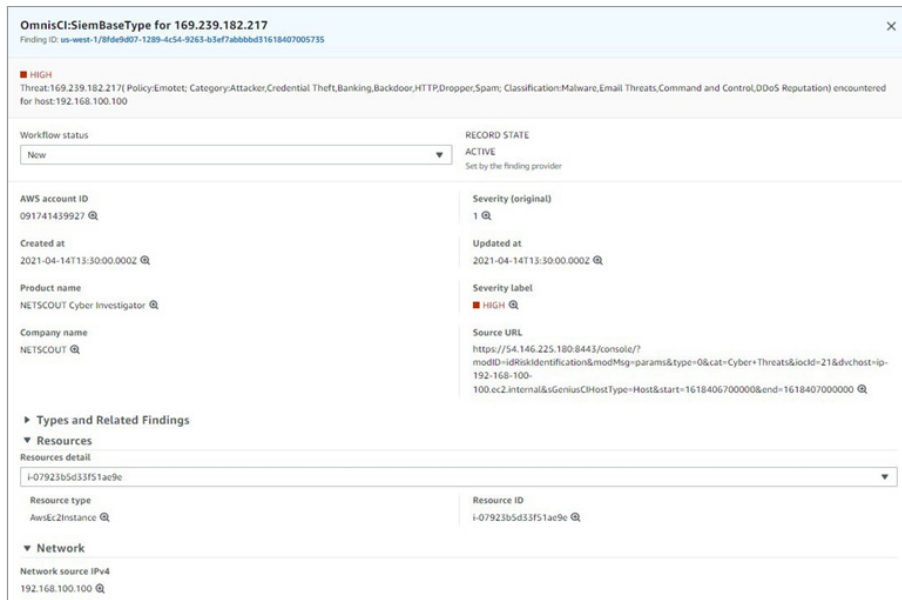


Figure 1: AWS Security Hub with NETSCOUT Omnis Cyber Intelligence Insight.

Omnis Cyber Intelligence Use Case Example

NETSCOUT OCI through the Security Events Center (see figure 1) serves as the central console for managing vCyberStream, offering comprehensive capabilities for security events management, investigation, and historical analytics.

The Security Events Center host-centric display enhances visibility into host-level activities and their corresponding security events (see figure 2). Use investigation modules like Host Investigation, Packet Analysis, and Session Analysis for further drill down. For example, the Host Investigation module provides:

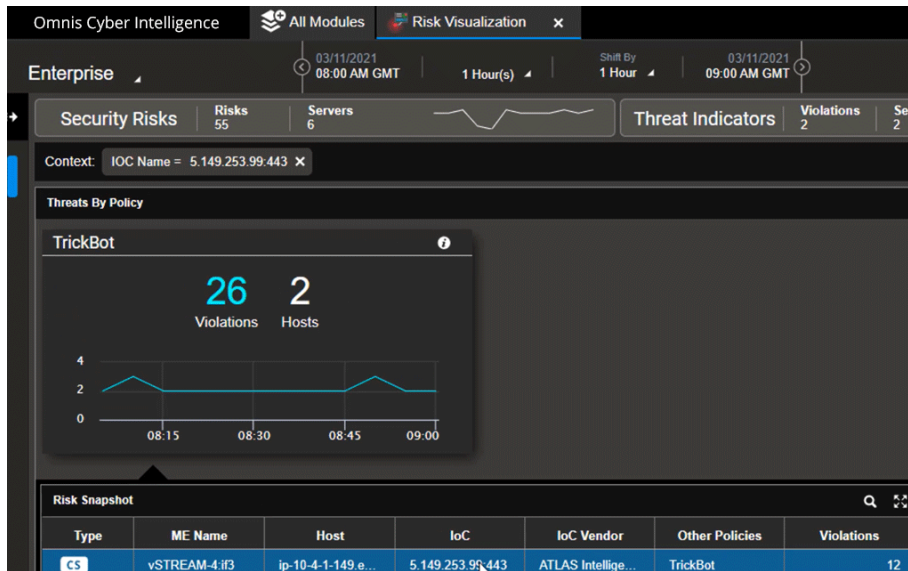
- Visibility across all Hosts in the network
- View all connections for a selected host
- Identification of compromised connections and hosts
- List of IoCs detected for each host

Other NETSCOUT OCI features include:

- Showcase security events for a host, complete with mappings to the MITRE ATT&CK framework.
- IDS events detected with match to signature-based feed and behavior analytics.
- Visibility into the current state of the internet-facing attack surface and compliance status.
- Workflows for historical and forensic investigations, including host investigation, session analysis and packet decodes.

Omnis Cyber Intelligence with AWS Security Hub Use Case Example

Gain visibility in critical and questionable host interactions—both internal and external. AWS Security Hub shows Insight graphs including findings over time by severity and a table with high-severity findings from NETSCOUT OCI. Findings can include EC2 hosts infected by malicious IP such as DNS exfiltration from internal EC2 hosts to external servers. The finding details (see figure 1) have an embedded URL that takes the user to NETSCOUT OCI for contextual drill-down. Risk visualization (see figure 2) in NETSCOUT OCI allows comprehensive and contextual visibility of security risks, threat indicators, and cyber threats in the hybrid cloud (see table below). Risk visualization allows host investigation drilldowns (see figure 3) to examine the specific hosts conversations as well as related traffic and throughput information involved in the threats. Users can analyze sessions and do packet decodes for specific events.



LEARN MORE

For more information visit:

- [AWS and NETSCOUT Collaboration](#)
- [NETSCOUT Omnis Cyber Intelligence AWS Security Hub](#)
- [AWS Marketplace](#)

Figure 2: Omnis Cyber Intelligence risk visualization directly from alert in AWS Security Hub.

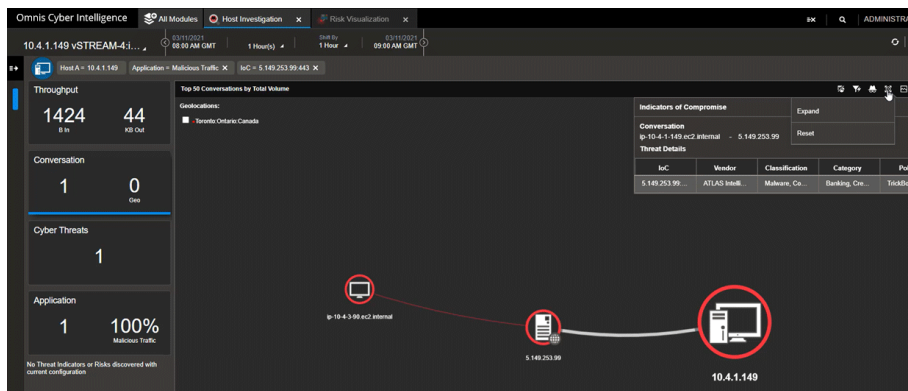


Figure 3: Omnis Cyber Intelligence Host Investigation.



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