NETSCOUT Omnis Cyber Investigator With AWS Security Hub

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 is 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 cyber threat and risk investigation platform with AWS Security Hub, this solution for enterprises streamlines contextual investigations for security risks and strengthens the corporate security posture. SOC teams use AWS Security Hub as a single place that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services and now, NETSCOUT Omnis™ Cyber Investigator (OCI). Events and insights detected by NETSCOUT OCI are displayed in AWS Security Hub and users can do contextual drilldowns 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. Within the NETSCOUT OCI platform, 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. 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, NETSCOUT OCI 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. The AWS Security Hub and NETSCOUT Omnis Cyber Investigator solution increases security team productivity and enables them to intelligently combat cyber threats and attacks across complex hybrid cloud environments by reducing the effort of collecting and prioritizing security findings and enabling integrated context rich investigations.

FEATURES AND BENEFITS

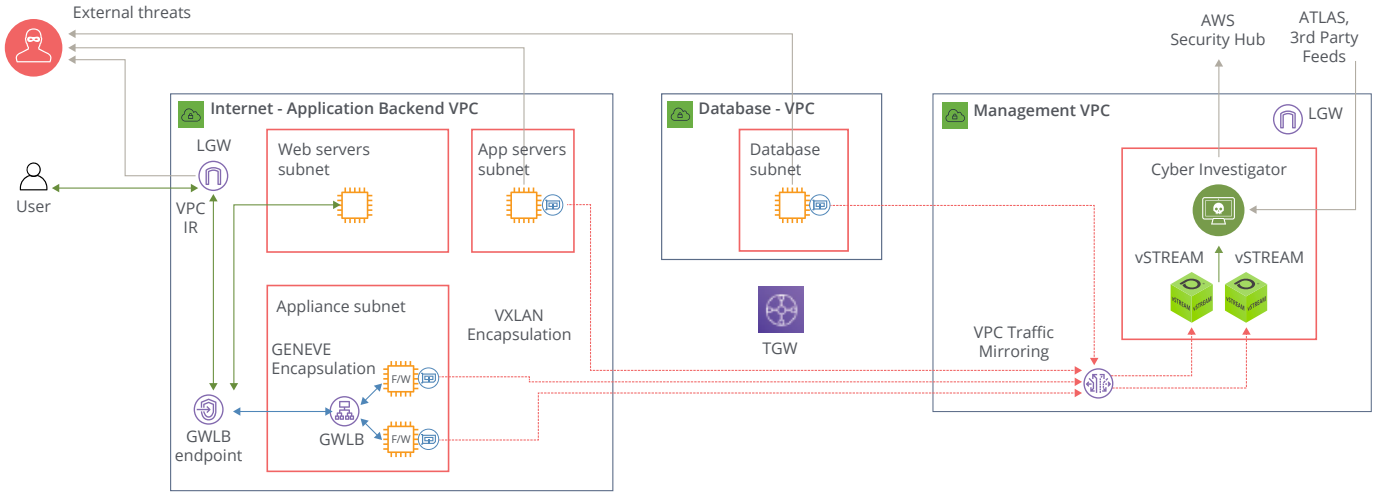
Key Benefits

- Strengthen security posture and reduce business risk by integrating NETSCOUT OCI with AWS Security Hub to aggregate, organize and prioritize findings, and for contextual drill-down and forensics analysis to resolve the highest priority security issues
- Gain visibility into threats and derive actionable insights for security issues that span AWS, on-premises, and hybrid environments
- Proactively examine security risks and Indicators of Compromise in complex, interconnected infrastructures by turning network traffic and global threat intelligence feeds into smart data and use results of highly contextual investigation to remediate with confidence
- AWS tested and certified NETSCOUT solutions

AWS and NETSCOUT Collaboration

Enterprise IT organizations want to rely on vendors who can demonstrate strong collaboration with AWS. NETSCOUT has collaborated with AWS to provide Visibility without Borders through interoperability with a variety of AWS services and technologies. NETSCOUT has achieved an Advanced Tier AWS Partner Network (APN) ISV membership with Networking, Cloud Migration, and Public Sector competencies. The benefits to customers from this powerful alliance include faster technological innovation, reduced capital and operational expenses, and the ability to accelerate their application modernization and cloud migration journey, while retaining happy customers and assuring a delightful end-user experience.

Visibility Without Borders to Quickly Identify and Contain Cyber Threats on AWS



NETSCOUT requires deploying the Omnis Cyber Investigator application as the data integration point for AWS Security Hub.

NETSCOUT vSTREAM® virtual appliances with Cyber Adaptor add-on translates packet data in real time using NETSCOUT's patented Adaptive Service Intelligence® (ASI) technology turning it into security metadata for the NETSCOUT OCI application. AWS native packet acquisition features such as Amazon VPC Traffic Mirroring combined with Amazon VPC Ingress Routing and Gateway Load Balancer, enable vSTREAM to monitor effectively both East-West and North-South network traffic on AWS, convert it into actionable intelligence with NETSCOUT OCI and give SecOps teams an unprecedented level of visibility and ability to conduct highly contextual guided investigations or unguided hunting.

As part of the OCI integration with the AWS Security Hub, NETSCOUT OCI automatically formats violations in the Amazon Security Findings Format (ASFF) and built-in intelligence suppresses duplicate alerts and groups them as needed. After NETSCOUT OCI and vSTREAM with Cyber Adaptor are deployed, to get started with AWS Security Hub:

1. The user configures NETSCOUT OCI to send alerts to the AWS Security Hub. NETSCOUT OCI configuration requires the user to identify AWS regions and the Amazon Account ID or authentication using the IAM role associated with the EC2 instance.
2. AWS Security Hub collects the NETSCOUT OCI threat and risk alerts and populates its findings and insights database which also includes data collected from AWS services and other third-party tools like Splunk and Palo Alto Networks Cortex XSOAR.
3. AWS Security Hub displays findings in charts through its dashboard. Custom insights allow the user to see NETSCOUT OCI findings and perform advanced queries and reports.
4. Finding details have a built-in NETSCOUT OCI URL for contextual threat and risk investigation drill downs.

Risk Visualization and Host Investigation Use Case

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) has an embedded URL that takes the user to NETSCOUT OCI for contextual drilldown. 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 the specific events.

Risk Visualizations	Types
Cyber threat events	Malware, C2, Campaign & Targeted Attacks
Threat indicators	Volumetric, State Exhaustion, Application Layer DDoS Attacks
Security risk events	Certificate Expiration, Self-signed Certificate Usage, Weak Cyphers

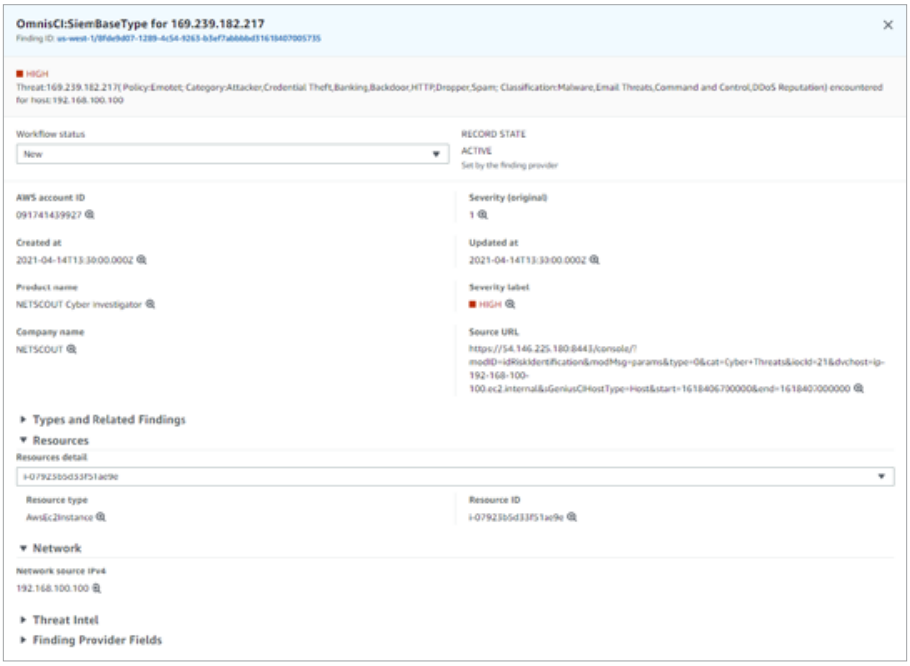


Figure 1: AWS Security Hub with NETSCOUT Omnis Cyber Investigator Insight.

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

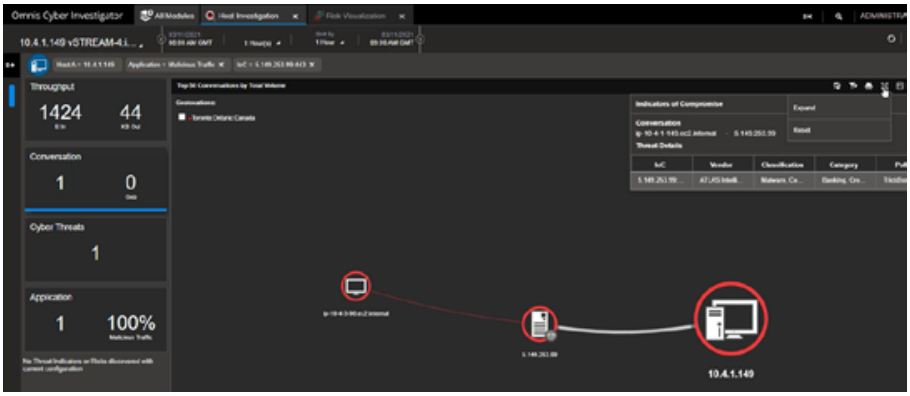


Figure 3: Omnis Cyber Investigator Host Investigation.

LEARN MORE

For more information visit:

AWS and NETSCOUT Collaboration

NETSCOUT Omnis Cyber Investigator

AWS Security Hub

AWS Marketplace

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

SECSB_030_EN-2101 04/2021