

Strengthen Cybersecurity of Space and SATCOM Network with NETSCOUT Omnis Cyber Intelligence

KEY BENEFITS

Comprehensive Protection: NETSCOUT® Omnis™ Cyber Intelligence (OCI) detects various threats, including IoC's, behavioral anomalies, attack surface changes, compliance issues, signature-based alerts, and policy violations, ensuring robust security for the network.

Streamlined Operations: Providing a single view for centralized management, OCI offers unparalleled visibility across all security events, simplifying threat detection and response efforts.

Targeted Threat Mitigation: OCI identifies victim hosts, enabling focused remediation actions to mitigate threats effectively and minimize potential damages.

Enhanced Situational Awareness: Users can tailor dashboards and reports to highlight critical threat indicators, enhancing situational awareness and enabling proactive decision-making.

Business challenges

Cybersecurity for space missions and satellite communication (SATCOM) is not optional and should be taken seriously. The barrier to entry for threat actors has significantly reduced as well as attack surface has been exposed further, exposing organizations to all kinds of cyberattacks from hobbyist and script kiddies to highly motivated nation state threat-actors.

The main threats that target space and SATCOM infrastructure are not different in many cases from other well-known threats seen in many other fields and in critical infrastructure outside of the space domain. The reason why those are now affecting the space domain so much is mainly due to a dramatic evolution in technology for space infrastructures.

One of main solutions to combat and mitigate these threats is defense in depth and one of key components in detection, mitigation, and effective remediation and incident response is highly scalable and efficient network visibility solution.

CISA and FBI strongly encourages critical infrastructure organizations and other organizations that are either SATCOM network providers or customers to review and implement the following mitigations:

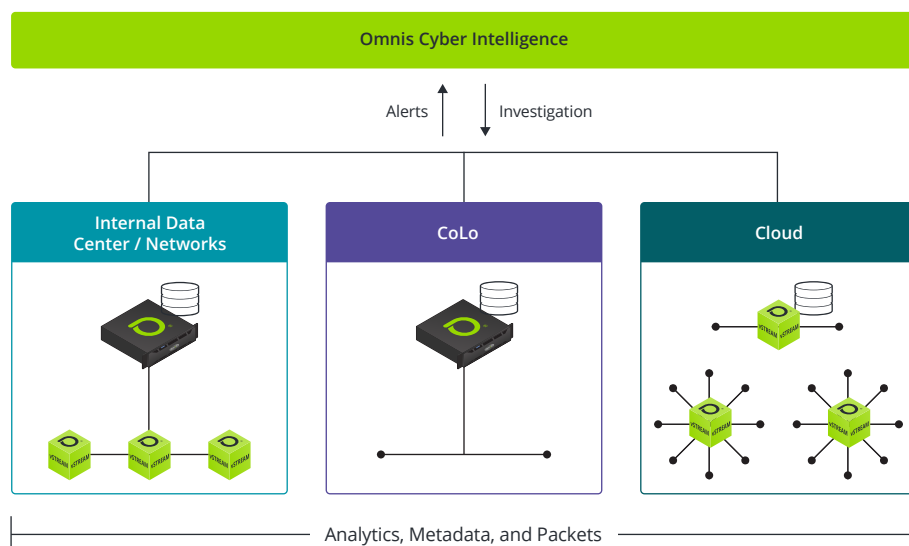
- Put in place additional monitoring at ingress and egress points to SATCOM equipment to look for anomalous traffic, such as:
 - The presence of insecure remote access tools—such as Teletype Network Protocol (Telnet), File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Secure Copy Protocol (SCP), and Virtual Network Computing (VNC)—facilitating communications to and from SATCOM terminals.
 - Network traffic from SATCOM networks to other unexpected network segments.
 - Unauthorized use of local or backup accounts within SATCOM networks.
 - Unexpected SATCOM terminal to SATCOM terminal traffic.
 - Network traffic from the internet to closed group SATCOM networks.
 - Brute force login attempts over SATCOM network segments.

Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a>

Omnis Cyber Intelligence and Omnis CyberStream NDR Platform

A Platform for Advanced DPI-powered Network Threat Detection and Response

Transforming network security, Omnis™ Cyber Intelligence (OCI) and the Omnis™ CyberStream sensors present a powerful solution for eliminating network blind spots. At the core of this comprehensive platform lies deep packet inspection (DPI), offering enterprises unparalleled security visibility to accurately identify vulnerabilities and threats.



Leveraging advanced threat detection techniques and cutting-edge machine learning algorithms, Omnis CyberStream ensures the detection of both known and zero-day threats. The Omnis Cyber Intelligence Network Detection and Response (NDR) platform provides a unified interface for efficient security event management. Seamlessly integrating with SIEM tools and offering automation through SIEM/SOAR and XDR systems, this solution empowers organizations to swiftly investigate and respond to security threats.

Enterprises can now take control of their network security by embracing the capabilities of Omnis Cyber Intelligence and Omnis CyberStream. This comprehensive and proactive protection brings peace of mind and a heightened sense of security.

OCI Maintains Full Control and Flexibility

- No Data Leaves Your Organization
- Analytics @ Sensor
- Define Your Aging and Storage Guidelines
- Offering Reduced TCO

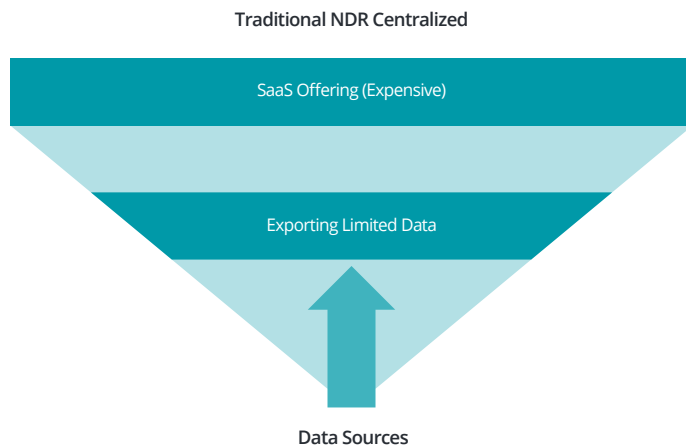
Key Benefits of Omnis Cyber Intelligence

- **Comprehensive Packet-Level Visibility:** Gain complete visibility into your network security, whether it's on-premises, virtual, or in hybrid cloud environments, ensuring no blind spots in your security monitoring.
- **Real-Time Threat Detection:** Multidimensional, real-time threat detection by executing multi-dimensional analytics at the source of capture and uses targeted ML techniques that are deterministic and minimize false positives. These multi-dimensional threat detection methods include IOCs, compliance policies violation, Suricata-based signatures, unexpected traffic, and behavior analysis to ensure comprehensive network security coverage.
- **Enhanced Incident Response:** Empowers incident response teams with real-time and historical data, enabling them to quickly investigate, analyze, and respond to security events, minimizing their impact.
- **Stay in Compliance:** Continuous network monitoring, reporting, long-term retention of network metadata and packets, and detection of unauthorized network activity or zero trust policy violations enable you to meet compliance requirements.

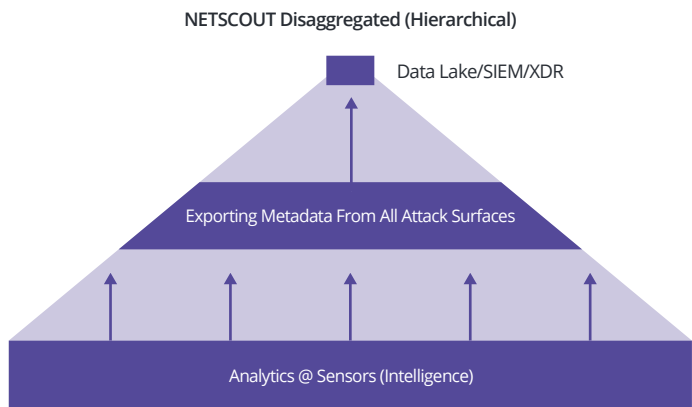
Main Features

- **MITRE ATT&CK Mapping:** Offers a wide range of prebuilt threat detection programs that align with MITRE ATT&CK, accompanied by on-sensor analytics. This approach enables faster detection of known threats and unknown threats, reduced response times, operational efficiency, mitigation of false positives, and enhanced compliance and reporting capabilities with the NDR platform.
- **Historical Investigation / Threat Hunting:** Continuous packet capture and long-term storage of metadata and associated packet decodes, enables historical investigation to quickly eliminate or validate false positives, provide forensic evidence, and reduce Mean-Time-To-Resolution (MTTR).
- **Host Group and Policies:** Network segmentation with host groups and policies for improved security. Logical grouping of network hosts with similar security requirements and characteristics with alerts on any policy violations.

For more information about Omnis Cyber Intelligence, data sheets, white papers and use cases please visit <https://www.netscout.com/product/cyber-intelligence>



The more attack surfaces you protect, the more expensive it becomes.

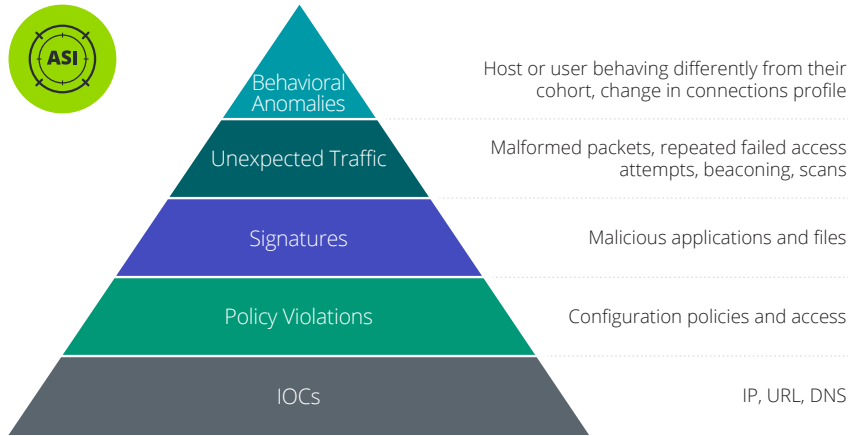


Designed to protect all attack surfaces at a favourable TCO via an innovative architecture and pricing structure.

Main OCI features are mapped to CISA and FBI recommendation for SATCOM and Space mitigation and monitoring requirements

OCI can monitor ingress and egress points to equipment to look for anomalous and malicious traffic, north-south and east-west such as:

- The presence of insecure weak / outdated protocols, weak ciphers, self-signed certificates etc.
- Network traffic from network segment to other unexpected network segments.
- Unexpected traffic, attack surface monitoring, policy violations, scanning, brute forcing, and multidimensional threat detection.
- Network traffic from the internet to closed group networks and from closed to group to internet, including applying behavioral analytics and threat intelligence.
- Brute force login attempts over network segments.
- Monitoring Air-gapped Network without any need to send traffic outside for detection, as Analytics @ Sensor and close to source.



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