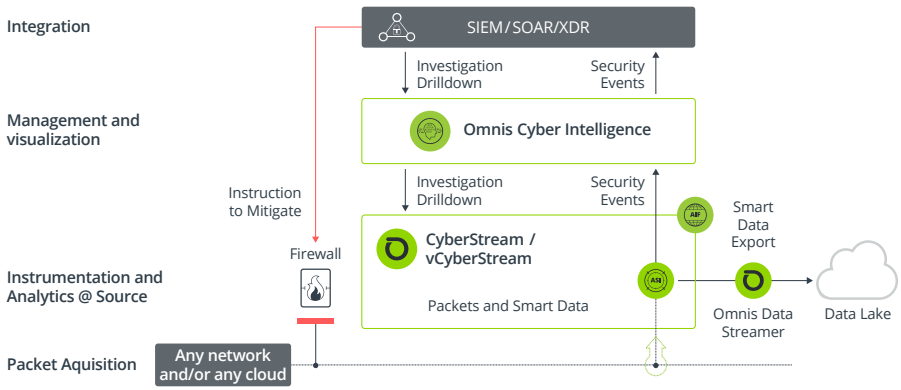
NETSCOUT

TUCANA CYBER SECURITY SOLUTIONS

Omnis CyberStream and Omnis Cyber Intelligence

Advanced, DPI-Based Network Detection and Response

Omnis CyberStream and Omnis Cyber Intelligence form a comprehensive platform for Advanced Network Threat Detection and Response based on Deep Packet Inspection (DPI). The platform enables enterprises to achieve complete security visibility into their network and identify vulnerabilities and threats with high accuracy. Omnis CyberStream combines multiple threat detection techniques to detect known and zero-day threats, leveraging cutting-edge machine learning algorithms for behavioral analytics. Meanwhile, Omnis Cyber Intelligence provides a unified interface for managing all security events and gaining actionable insights. It integrates smoothly with SIEM tools and offers automation through SOAR and XDR, enabling organizations to investigate and respond to security threats with greater speed and efficiency. To export CyberStream's Smart Data, Omnis Data Streamer is available, streamlining data exportation for further analysis and insights.



Comprehensive Network Visibility Without Borders

Omnis Cyber Intelligence and CyberStream network instrumentation deliver unrivaled network security visibility, ensuring comprehensive coverage across any environment. Deployable in on-premises, data center, and private or public cloud environments like AWS, Google Cloud, and Microsoft Azure, this powerful platform captures network packets in real-time, achieving speeds of up to 100 Gbps. Leveraging patented Adaptive Service Intelligence DPI technology, CyberStream extracts and locally stores layer 2-7 metadata and associated packet decodes. This advanced capability establishes a robust Visibility Without Borders platform, empowering real-time threat detection and historical investigation. With CyberStream, effortlessly identify threats and vulnerabilities throughout your network environment, proactively mitigating risks.

Main Features & Benefits

Visibility Without Borders

CyberStream delivers cost-effective and scalable network instrumentation, extending comprehensive packet-level visibility across diverse network infrastructures, including on-prem, virtual, and hybrid cloud environments. This robust visibility empowers threat detection and enables swift incident response, bolstering the overall security posture.

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, reduced response times, operational efficiency, mitigation of false positives, and enhanced compliance and reporting capabilities.

Multi-dimensional Threat Analytics @ Source

CyberStream instrumentation enables real-time threat detection using targeted ML techniques that are deterministic, minimizing false positives. CyberStream utilizes multi-dimensional threat detection methods such as IoCs, policies, signatures, unexpected traffic, and behavior analysis to ensure comprehensive security coverage.

Historical Investigation / Hunting

Continuous packet capture and long-term local, storage of metadata and associated packet decodes on CyberStream, enables historical investigation to quickly eliminate or validate false positives, provide forensic evidence, and reduce Mean-Time-To-Resolution (MTTR).

Ecosystem Enhancement

Support for Syslog, STIX/TAXII intelligence feeds, APIs, and metadata export enable easy integration into an existing cybersecurity ecosystem (e.g. SIEM/SOAR/XDR) providing high fidelity network data, improved threat detection, investigation and response.

Omnis Cyber Stream

CyberStream network instrumentation, in real-time and at source of packet capture conducts multiple methods of vulnerability and threat detection including:

- **IoCs –** Supports up to 2 million from threat intelligence feeds via NETSCOUT ATLAS Intelligence Feed (AIF), 3rd Party (STIX/TAXII) or custom internal feed.
- **Compliance/Policy Violations –** Empowers the custom creation and configuration of policies for each network resource, defining desired behavior. Users can establish thousands of custom policies tailored to their specific needs.
- **Signatures –** Matching to known malicious network traffic or file, and patterns. Out of the box support for tens of thousands of Suricata-based and customers can add additional signatures from multiple sources including commercial, open source or create their own.
- **Unexpected Traffic –** Effectively identifies and flags various anomalies such as malformed packets, unauthorized protocols, weak ciphers, expired/self-signed keys, beaconing, and network scanning activities.
- **Behavior Analytics –** Utilizes sophisticated algorithms to analyze the behavior of hosts and detects any deviations from normal patterns exhibited by peer cohorts.

With Omnis CyberStream's robust feature set, organizations can confidently identify vulnerabilities and threats, ensuring comprehensive network security.

Omnis Cyber Intelligence

Omnis Cyber Intelligence serves as the central console for managing CyberStream, offering comprehensive capabilities for security events management, investigation, and historical analytics.

- **Proactive Hunting –** Leverage local, long-term, storage of historical metadata to conduct unguided hunting looking for evidence of compromise, network, or data breach.
- **Unified and Host-Centric Security Event Display –** Provides a unified view of all security events, ensuring a holistic understanding of the threat landscape. Host-centric display enhances visibility into host-level activities and their corresponding security events.
- **Security Events Dashboard with MITRE ATT&CK Mappings –** Presents a dashboard that showcases all security events, complete with mappings to the MITRE ATT&CK framework. This integration allows for better contextualization and understanding of the detected threats.
- **Sorting of Security Events by Type and Severity –** Enables efficient security event management by allowing users to sort based on their type and severity. This feature streamlines prioritization and response efforts.
- **Security Events Management –** Facilitates effective security events management by offering security event suppression capabilities to reduce false positives. Additionally, users can acknowledge and track the status of security event to ensure prompt handling.
- **Attack Surface –** Provides visibility into the current state of the internet-facing attack surface and compliance status. This feature helps organizations assess their security posture and identify areas that require attention.
- **Historical Investigation –** Empowers users with workflows for historical investigation, including host investigation, session analysis, and packet decodes. These capabilities enable in-depth analysis, aiding incident response and forensic investigations.

Providing all security events into a single user interface increases the capabilities and efficiency of a SOC analyst and reduces the Mean-Time-To-Knowledge (MTTK).

Cybersecurity Ecosystem Integration and Enhancement

Omnis CyberStream and Omnis Cyber Intelligence are designed for seamless integration with other cybersecurity tools, including SIEM, EDR, SOAR, and XDR systems. The solution offers tri-directional integration to enhance workflows, collaboration, and response times for incident detection and response.

- **Send Security Events to Security Stack –** CyberStream sends syslog alerts to SIEM, SOAR, or XDR systems in response to detected threats.
- **Investigate Security Events from Security Stack –** The open API enables network investigation and adds network context to third-party alerts (e.g., from SIEM, EDR) using historical network metadata and locally stored packet data from CyberStream probes.
- **Export –** The Omnis Data Streamer add-on exports ASI Flow metadata using JSON (Kafka), AVRO (Kafka), and CSV formats for custom enrichment and analysis. Refer to the Omnis Data Streamer Datasheet for more details.

Key Features

Network Visibility – Reveals all traffic, devices, users, and suspicious activity including North-South, East-West, on-prem, cloud, IoT, and encrypted traffic.

Attack Surface Monitoring – Monitor network threats between Internet and enterprise DMZ endpoints. Creates inventory of all assets and real time alerts on new assets or abnormal traffic patterns detected in the attack surface.

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.

Intrusion Detection System – Analyzes network traffic for signs of malicious activity and comparison to known signatures. Real time monitoring of network traffic with open source Suricata signature matching.

Malicious File Detection – Identify malicious files by comparing file signatures against a database of known malware signatures. Inspects network traffic for file transfers, extracting metadata such as file type and signature.

Policy Compliance – CyberStream is continuously monitoring the attack surface 24/7. Identifies any changes to the attack surface such as new IP addresses, ports or applications and reports on any violations with easy compliance report generation.

Host Investigation – Tracing network connections retrospectively to uncover security threats. Comprehensive host communication analysis and session analysis to discover all affected hosts and assets.

Security Events Center – Centralizing and managing alerts with SIEM integration. Visibility across all security events with customizable dashboards and reporting.

SKUs

CyberStream	
F-02795-001-1	Certified Omnis CyberStream Software, includes NETSCOUT 4-Port 10G/1G ASI Accelerator NIC, 1-socket, for use with C-02700 series certified appliance hardware
F-09895-001-2	Certified Omnis CyberStream Software, includes NETSCOUT 4-Port 10G/1G ASI Accelerator NIC, 2-socket, for use with C-09800 series certified appliance hardware
F-09807-001-2	Certified Omnis CyberStream Software, includes NETSCOUT 2-Port 40G ASI Accelerator NIC, 2-socket, for use with C-09800 series certified appliance hardware
F-09802-001-2	Certified Omnis CyberStream Software, includes NETSCOUT 2-Port 100G ASI Accelerator NIC, 2-socket, for use with C-09800 series certified appliance hardware
F-05095-001-1	Qualified Omnis CyberStream Software, includes NETSCOUT 4-Port 10G ASI Accelerator NIC, 1 socket
F-05095-001-2	Qualified Omnis CyberStream Software, includes NETSCOUT 4-Port 10G ASI Accelerator NIC, 2 socket
F-05007-001-2	Qualified Omnis CyberStream Software, includes NETSCOUT 2-Port 40G ASI Accelerator NIC, 2 socket
F-05002-001-2	Qualified Omnis CyberStream Software, includes NETSCOUT 2-Port 100G ASI Accelerator NIC, 2 socket
F-0D095-001-1	Dell Omnis CyberStream Software, includes NETSCOUT 4-Port 10G/1G ASI Accelerator NIC (SFP+), 1 socket, for use with C-0D740-XSJx1 or C-0D440-KSJx1 series Dell Appliance hardware.
F-0D095-001-2	Dell Omnis CyberStream Software, includes NETSCOUT 4-Port 10G/1G ASI Accelerator NIC (SFP+), 2 socket, for use with C-0D740-BSJx2 series Dell Appliance hardware.
F-0D007-001-2	Dell Omnis CyberStream Software, includes NETSCOUT 2-Port 40G ASI Accelerator NIC (QSFP+), 2 socket, for use with C-0D740-BSJx2 series Dell Appliance hardware.
F-0D002-001-2	Dell Omnis CyberStream Software, includes NETSCOUT 2-Port 100G ASI Accelerator NIC (QSFP28), 2 socket, for use with C-0D740-BSJx2 series Dell Appliance hardware.

Virtual CyberStream	
VCYBR-STR-008	Virtual CyberStream (vCyberStream) - 8 vCPUs
VCYBR-STR-040	Virtual CyberStream (vCyberStream) - 40 vCPUs
VCYBR-STR-120	Virtual CyberStream (vCyberStream) - 120 vCPUs
VCYBR-STR-200	Virtual CyberStream (vCyberStream) - 200 vCPUs

Omnis Cyber Intelligence	
51DD1L	Omnis Cyber Intelligence - Dedicated Global Manager - Standard Appliance
51D51L	Omnis Cyber Intelligence - Full (50) - Standard Appliance
51D21L	Omnis Cyber Intelligence - Full (50) - Standby Appliance
51DH1L	Omnis Cyber Intelligence - Intermediate (25) - Standard Appliance
51D41L	Omnis Cyber Intelligence - Workgroup (10) - Standard Appliance
51DD2L	Omnis Cyber Intelligence - Dedicated Global Manager - Enhanced Appliance
51D52L	Omnis Cyber Intelligence - Full (50) - Enhanced Appliance
51D22L	Omnis Cyber Intelligence - Full (50) - Standby Enhanced Appliance
51DH2L	Omnis Cyber Intelligence - Intermediate (25) - Enhanced Appliance
51D42L	Omnis Cyber Intelligence - Workgroup (10) - Enhanced Appliance
91DD0L	Omnis Cyber Intelligence - Dedicated Global Manager - Software - (Linux)
91D50L	Omnis Cyber Intelligence - Full (50) - Software - (Linux)
91D20L	Omnis Cyber Intelligence - Full (50) - Standby Software - (Linux)
91DH0L	Omnis Cyber Intelligence - Intermediate (25) - Software - (Linux)
91D40L	Omnis Cyber Intelligence - Workgroup (10) - Software - (Linux)
91DV0L	Omnis Cyber Intelligence - Entry (5) - Software - (Linux)

Omnis Adaptor	
9V2WB0	Omnis CyberStream Adaptor for vSTREAM - 8 vCPUs
9V2VB0	Omnis CyberStream Adaptor for vSTREAM - 40 vCPUs
9V2FB0	Omnis CyberStream Adaptor for vSTREAM - 120 vCPUs
9V2HB0	Omnis CyberStream Adaptor for vSTREAM - 200 vCPUs
982WBH	Omnis CyberStream Adaptor - One 4-port 10G/1G 1-Socket for InfiniStreamNG
982VBH	Omnis CyberStream Adaptor - Five 4-port 10G/1G 1-Socket for InfiniStreamNG
982HBH	Omnis CyberStream Adaptor - Twenty-five 4-port 10G/1G 1-Socket for InfiniStreamNG
982WCH	Omnis CyberStream Adaptor - One 4-port 10G/1G 2-Socket InfiniStreamNG
982VCH	Omnis CyberStream Adaptor - Five 4-port 10G/1G 2-Socket for InfiniStreamNG
982HCH	Omnis CyberStream Adaptor - Twenty-five 4-port 10G/1G 2-socket for InfiniStreamNG
982WCF	Omnis CyberStream Adaptor - One 2-port 40G 2-Socket InfiniStreamNG
982VCF	Omnis CyberStream Adaptor - Five 2-port 40G 2-Socket for InfiniStreamNG
982HCF	Omnis CyberStream Adaptor for twenty-five 2-port 40G 2-Socket InfiniStreamNG
982WCG	Omnis CyberStream Adaptor - One 2-port 100G 2-Socket InfiniStreamNG
982VCG	Omnis CyberStream Adaptor - Five 2-port 100G 2-Socket for InfiniStreamNG
982HCG	Omnis CyberStream Adaptor - Twenty-five 2-port 100G 2-Socket for InfiniStreamNG

NETSCOUT

TUCANA CYBER SECURITY SOLUTIONS
www.tucana.com info@tucana.com

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