Omnis CyberStream and Omnis Cyber Intelligence

Advanced, DPI-Powered Network Visibility, Threat Detection and Investigation

Omnis® CyberStream and Omnis® Cyber Intelligence form a highly scalable and cost-effective platform for comprehensive, deep-packet inspection (DPI)-powered network visibility, real-time and retrospective threat detection, investigation, and hunting. The solution's Adaptive Threat Analytics capabilities continuously and cost-effectively capture and locally store all metadata and packets independent of detected threats, enabling security teams to investigate and hunt more efficiently, determining and reducing incident response time, meeting compliance requirements, and reducing the risk of a successful cyberattack.

Main Features & Benefits

Visibility Without Borders

Highly scalable architecture and continuous, cost-effective, deep packet inspection, provide a "Visibility Without Borders" platform that is an essential and foundational component for a more effective threat detection, investigation, and incident response.

Adaptive Threat Detection @ Source

At the source of packet capture, Adaptive Threat Detection utilizes multi-dimensional and deterministic ML techniques to detect threats and minimize false positives.

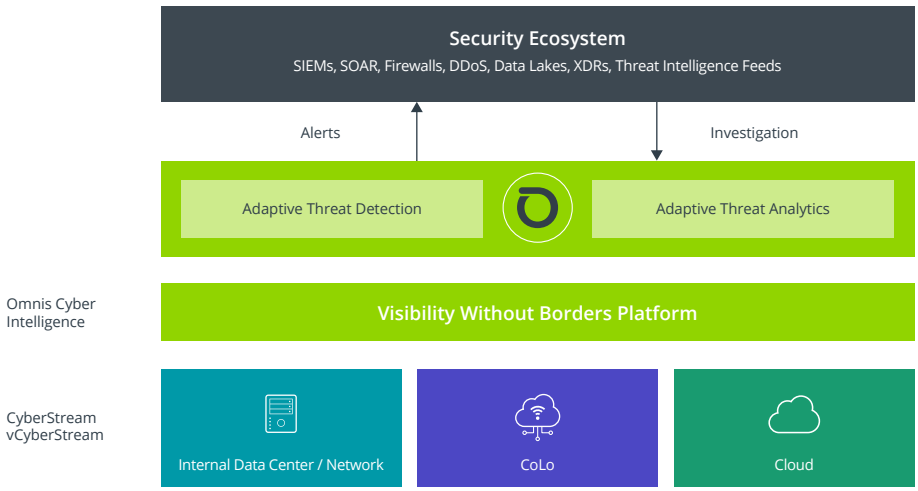
Adaptive Threat Analytics

Network instrumentation continuously captures and locally stores metadata and packets independently of detections, enabling rapid retrospective investigations or proactive threat hunting.

Security Ecosystem Integration

Support for standard Syslog formats, STIX/TAXII intelligence feeds, and an open API allow easy integration into an existing cybersecurity stack to enhance threat detection, investigation and incident response.

Omnis Cyber Intelligence Architecture



Comprehensive Network Visibility and Adaptive Threat Analytics

Omnis Cyber Intelligence is built on a highly scalable architecture that provides continuous, cost-effective, packet-level visibility across an organization's entire digital infrastructure, including on-premises, data centers, co-locations, and public cloud platforms like AWS, Google Cloud, and Microsoft Azure. This "Visibility Without Borders" is an essential and foundational component of any threat detection, investigation, and incident response process.

At the source of packet capture, Omnis CyberStream network instrumentation conducts real-time Adaptive Threat Detection using targeted ML techniques that are more deterministic and less prone to false positives. Adaptive Threat Detection utilizes multiple methods to detect threats, including known IoCs from NETSCOUT's ATLAS Intelligence Feed, Suricata-based IDS signatures, network behavioral analytics, and custom policies to help ensure comprehensive security coverage.

Omnis Cyber Intelligence's Adaptive Threat Analytics leverage CyberStream network sensors which continuously and locally store network metadata and packets independent of detections. Built-in packet decodes and flexible ad hoc querying of historical metadata facilitate rapid investigation of threats detected by Omnis Cyber Intelligence or 3rd parties (e.g., EDR, SIEM, XDR, etc.), and proactive hunting of previously missed threats to gain knowledge that determines and enables more efficient incident responses.

Omnis CyberStream

CyberStream network instrumentation, in real-time, up to 100 Gbps 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, to help provide comprehensive network security.

Omnis CyberStream appliance uses FIPS-140-2 approved cryptographic hash algorithm for generating account password hashes.

Adaptive Threat Analytics that continuously capture and locally store metadata and packets independently of detections, enabling rapid retrospective investigations or proactive hunting..

Omnis Cyber Intelligence

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

- **Historical Investigation –** Empowers users with workflows for historical investigation, including host investigation, session analysis, and packet decodes. These capabilities can enable in-depth analysis, aiding incident response and forensic investigations.
- **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 –** Helps with 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 –** Helps provide 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.

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).

Adaptive Threat Analytics offers a threat investigation or hunting platform that enables more efficient incident response and reduces the risk of a successful cyber attack.

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 help 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 assists 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 AI Insights add-on exports ASI Flow metadata using JSON (Kafka), AVRO (Kafka), and CSV formats for custom enrichment and analysis. Refer to the Omnis AI Insights Data Sheet for more details.
- **Block Threats –** Leverage integration capabilities with SOAR, AED, SIEM, and Firewall to actively block identified threats. This enhances proactive threat mitigation and response capabilities across integrated security tools.

Key Features

Comprehensive 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.

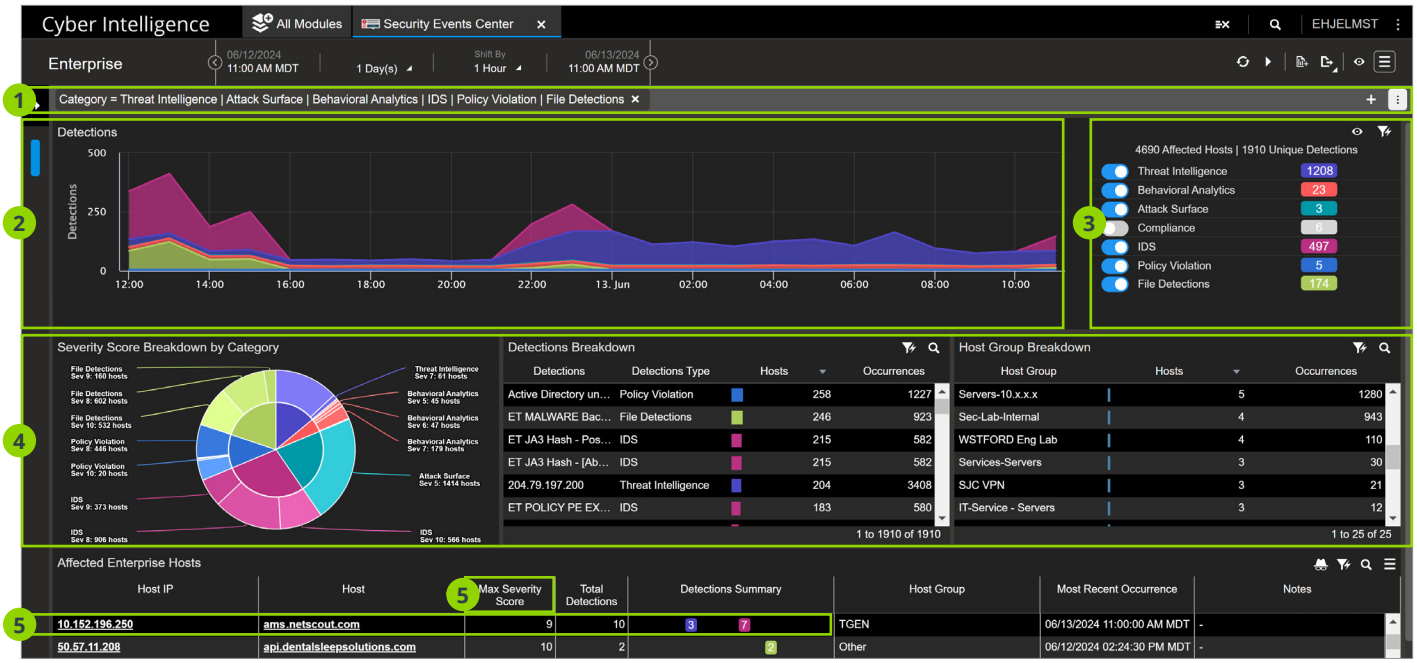


Figure 1: Omnis Cyber Intelligence's Security Events Center is the starting point for all threat detection and investigation.

1. Filter

- Apply filters from the summaries and time chart

2. Overtime Chart

- Count of event types per category
- Focus on a specific time by selection

3. Multidimensional Threat Detections

- **Threat Intelligence:** Identification of indicators of compromise (IoCs) through traffic analysis
- **Behavioral Analytics:** Recognition of anomalous traffic patterns indicative of potential threats
- **Attack Surface Events:** Detection of changes in the network environment that may signify emerging threats
- **Compliance Events:** Highlighting of insecure practices or protocols for remediation
- **IDS Events:** Signature-based detection of known attacks, augmented by custom rules
- **Policy Violations:** Identification of actions or patterns violating internal security policies
- **File Extraction Detection:** Flagging of malicious file transfers or downloads for further investigation

4. Summaries

- Breakdowns on important entities
- Search and Filter options
- Show/hide summaries pane

5. Host Table

- One row per host with Host IP as well as Hostname capability
- Breakdown of detections per category
- Example: Host 10.152.196.250 has 10 detections with 2 different detection types and a max severity of 9, increasing the likelihood this is a legitimate threat

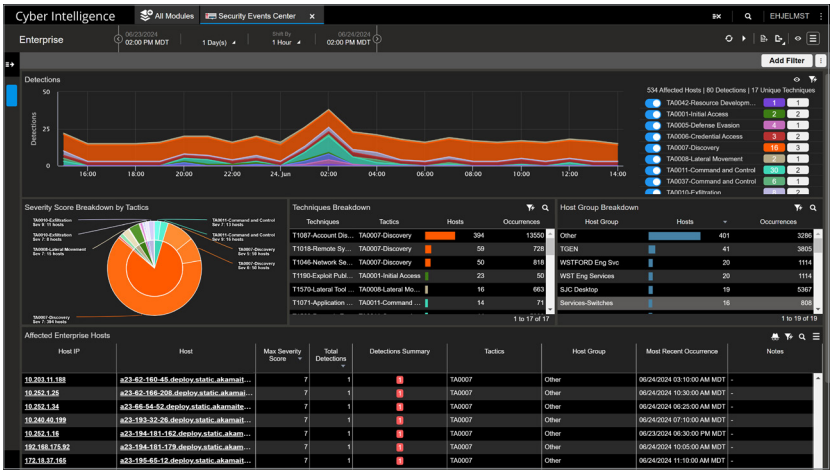


Figure 2: Security Events Center can be toggled to visualize all events mapped to Mitre ATT&CK.

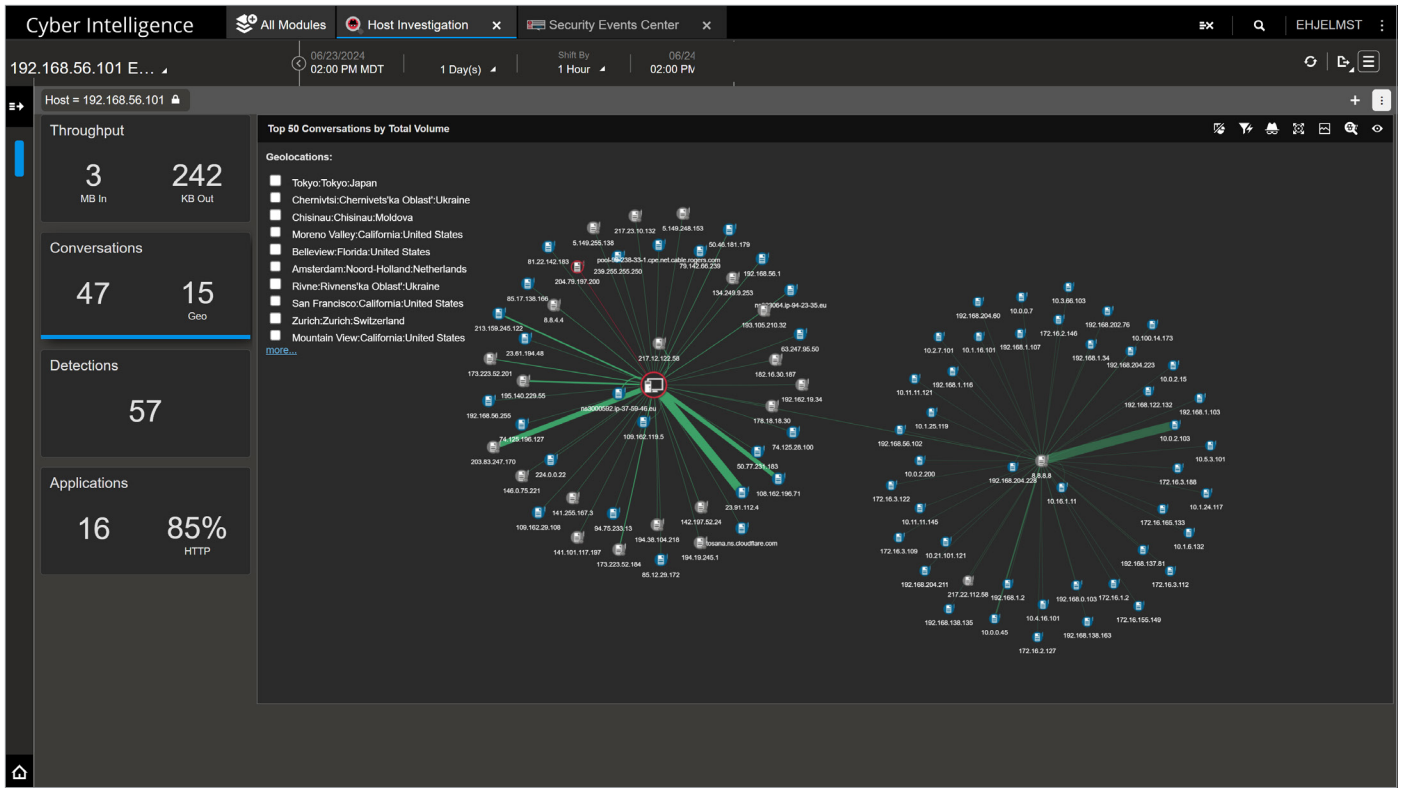


Figure 3: Omnis Cyber Intelligence's Host Investigation dashboard helps enable quick, ad-hoc, historical investigation of all hosts on the network.

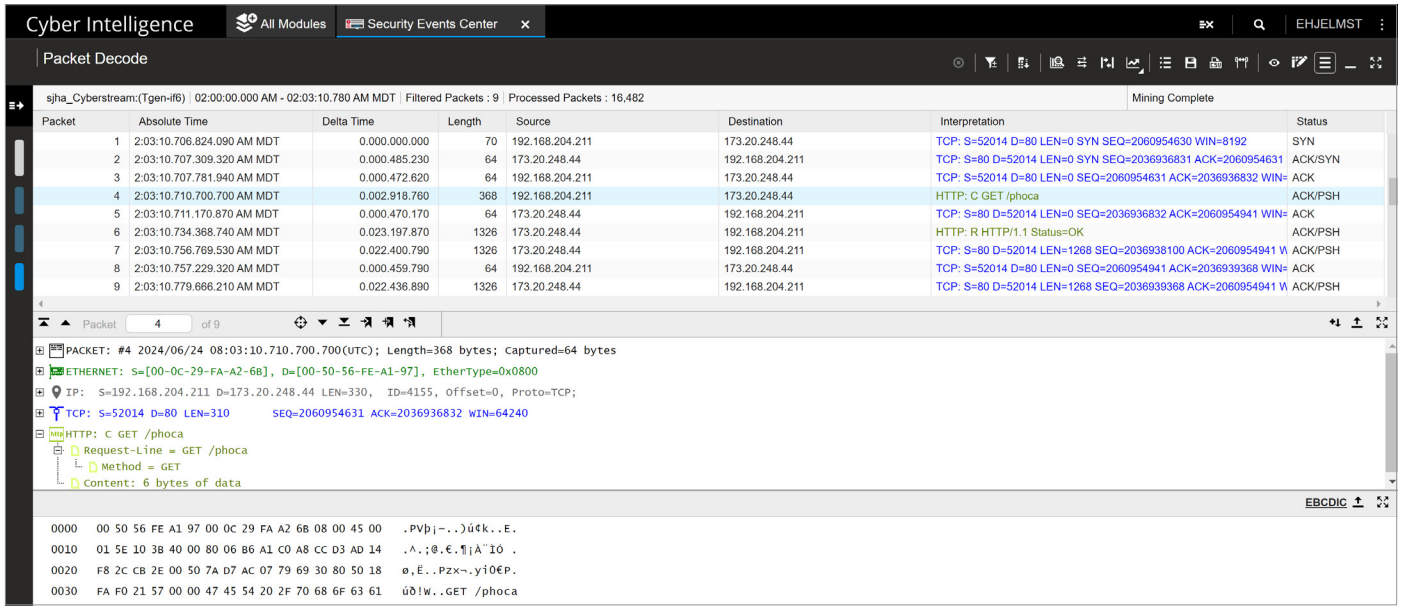


Figure 4: Quick on-click access to host investigation metadata and packets.

SKUs

CyberStream	
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

Specifications

Omnis Cyber Intelligence

Network Ports	2 Port 10Gb Ethernet (RJ45) 2 Port 1Gb Ethernet (RJ45)
iDRAC (IPMI)	1 Port Gigabit Ethernet (RJ45)
Storage	Standard: 16TB (4x 4TB RAID 5) Enhanced: 24TB (6x 4TB RAID 5)
Embedded OS	Oracle Linux 64 bit
Operating Environment	Secure, hardened, embedded Linux operating system
CPU	Standard: Single 20-Core 2.0GHz Enhanced:Single 24-Core 2.0GHz
Memory	Standard: 64GB Enhanced: 128GB
Rack Unit	2 Rack Unit (2RU)
Dimensions	3.4 in (87 mm) Height 19 in (482 mm) Width 28.4 in (722 mm) Depth
Weight	42.3 lbs (19.2 kg)
Power Rating (AC)	1100W AC: 100–240VAC auto ranging, 50-60Hz
Maximum Consumption (AC)	10-5A
Heat Dissipation (AC)	2891 BTU/Hr
Operating Temperature	10° to 35°C (50° to 95°F)
Storage Temperature	-40° to 65°C (-40° to 149°F)
Operating Relative Humidity	8% RH with -12°C (10.4°F) minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point. Atmosphere must be non- condensing at all times.
Storage Relative Humidity	5% to 95% (non-condensing with 27°C (80.6°F) maximum dew point)
Operating Vibrations	0.21 Grms at 5 Hz to 500 Hz for 10 minutes in all operation orientations
Storage Vibration	1.88 Grms at 10Hz to 500Hz for 15 minutes (all six sides tested)
Operating Shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms
Storage Shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms
Operating Altitude	Up to 3048 m (10,000 ft)
Storage Altitude	Up to 12,000 m (39,370 ft)
Regulatory and Agency Approvals	E88S, FCC (US only) Class A, ICES (Canada) Class A, CE Mark (EN55032 Class A, EN55035, EN61000-3-2, EN61000-3-3), VCCI (Japan) Class A, BSMI (Taiwan) Class A, RCM (Australia/New Zealand) Class A, NRCS LoA (South Africa) Class A, CCC (China) Class A, KC (Korea) Class A, NOM (Mexico), CM (Morocco), BIS (India), UL/EN/IEC 62368-1, CAN/CSA C22.2 No. 62368-1

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

© 2025 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Omnis, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, InfiniStream, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries.
Third-party trademarks mentioned are the property of their respective owners.

SECPDS_023_EN-2404 04/2025