NETSCOUT Omnis Intrusion Detection System (IDS)

Smart Security and Visibility

HIGHLIGHTS

- Network intrusion detection in on-prem, private, and hybrid cloud environments
- Identifies lateral movement, brute-force attacks, privilege escalation, ransomware, and command & control exploits
- Uses Suricata and supports open source, commercial, private, and customized rulesets technology for detection
- Quickly assesses threats with automated alert prioritization
- Sends contextually rich alerts and metadata to Omnis IDS Manager, Omnis™ Cyber Investigator, and/or SIEM, including Splunk
- Offered as a standalone solution with Omnis IDS Sensor or an add-on security module for InfiniStreamNG® appliances
- Omnis IDS Manager for centralized management via intuitive Web UI

NETSCOUT's Omnis™ Intrusion Detection System (IDS), a vital part of the NETSCOUT® Omnis Security solution, provides network intrusion detection for enterprises of all sizes. With seamless integration into open security stack, Omnis IDS delivers preconfigured and customizable rule configuration that will bring scalability, visibility, and efficiency to your security program. Based on the leading IDS platform, Suricata and supporting open source, commercial, private, and customized rulesets, Omnis IDS offers a comprehensive, high-performance, cost-effective intrusion detection software-based solution. It can be deployed in on-premises, private, and hybrid cloud environments, including AWS, for quick detection of threats as part of a comprehensive defense in depth strategy.

The Omnis IDS solution incorporates the Omnis™ IDS Sensor, a standalone solution or software module for the NETSCOUT InfiniStreamNG (ISNG) smart visibility appliance, and the Omnis™ IDS Manager components described below.

Omnis IDS Sensor

Omnis IDS Sensors are high-performance software appliances strategically deployed throughout the enterprise environment for collecting and analyzing network packet traffic to detect intrusions. Offered as either a standalone solution or as a software module for ISNG appliances, the Sensor technology uses Suricata and supports open source, commercial, private, and customized rulesets to detect security threat events and initiate alerts.

Omnis IDS Manager

Omnis IDS Manager is a powerful analytics and centralized management system. Multiple Omnis IDS Sensors forward security threat events to the Omnis IDS Manager to apply further analysis and initiate alert triggers. It can be configured to forward security threat events and alarms to third-party security information and event management (SIEM) systems for consolidated security event management.

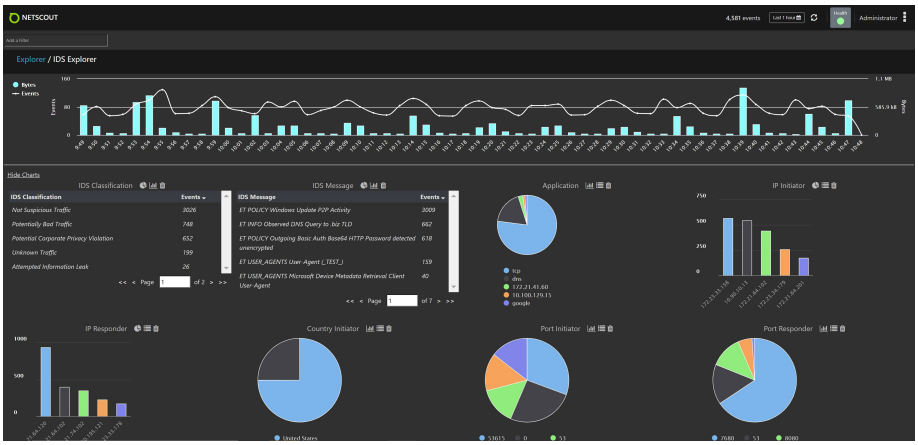

Figure 1: Omnis IDS Manager event analysis.

Key Features

Omnis IDS Sensor

- **Visibility** – As part of a comprehensive visibility plan, Omnis IDS Sensors can be easily deployed to provide packet visibility for insights into the areas of the network deemed critical.
- **Rule Signature Comparison** – Uses Suricata and supports open source, commercial, private, and customized rulesets for the ability to add or remove rules with no disruption of service.
- **Alerting** – Reduces alert fatigue, with the ability to refine tuning to meet the most important, unique needs of the business.

Omnis IDS Manager

- **Centralized Management** – Simplifies and streamlines the deployment and management of the IDS sensors with ability to configure, edit, and customize sensors from a single pane of glass for consistent, reproducible, and predictable deployment of 1 or many IDS Sensors.
- **Centralized Reporting** – Aggregates metadata into a flexible interface for simple visualization and customized prioritization. Provides this information in a consistent view, which gives Security Operations Center (SOC) teams the information they need to understand the attack and respond faster.
- **Central Analysis** – Provides complete visibility into the entire attack chain, and risks associated with it, to alert the Omnis IDS Manager, Omnis Cyber Investigator, and/or a 3rd party SIEM export (Splunk) for correlation, collaboration, and refinement of response efforts.

Omnis IDS Manager

SKU	Description
Q-02700-M10-1	Certified Omnis IDS Manager software for fifty (50) Omnis IDS Sensor interfaces, for use with C-02700 certified appliance hardware.
9824DX	Qualified Omnis IDS Manager software for fifty (50) Omnis IDS Sensor interfaces, for use with qualified physical or virtual servers.
C-02700-XSJA1	Certified ISNG Server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), AC.
C-02700-XSJD1	Certified ISNG Server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), DC.

Omnis IDS Sensor

SKU	Description
Q-02795-010-1	Certified Omnis IDS Sensor software, 10G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-02700 certified appliance hardware.
Q-04895-020-2	Certified Omnis IDS Sensor software, 20G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Q-04895-030-2	Certified Omnis IDS Sensor software, 30G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Q-04895-040-2	Certified Omnis IDS Sensor software, 40G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Q-04807-040-2	Certified Omnis IDS Sensor software, 40G license, includes NETSCOUT 2-Port 40G ASI Accelerator NIC (QSFP+), for use with C-04800 certified appliance hardware.
Q-05095-010-X	Qualified Omnis IDS Sensor software, 10G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+) for use with Dell R740xd or HPE DL380 Gen10 or virtual servers.
Q-05095-020-X	Qualified Omnis IDS Sensor software, 20G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+) for use with Dell R740xd or HPE DL380 Gen10 or virtual servers.
Q-05095-030-X	Qualified Omnis IDS Sensor software, 30G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+) for use with Dell R740xd or HPE DL380 Gen10 or virtual servers.
Q-05095-040-X	Qualified Omnis IDS Sensor software, 40G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+) for use with Dell R740xd or HPE DL380 Gen10 or virtual servers.
Q-05007-040-X	Qualified Omnis IDS Sensor software, 40G license, includes NETSCOUT 2-Port 40G ASI Accelerator NIC (QSFP+) for use with Dell R740xd or HPE DL380 Gen10 or virtual servers.
C-02700-XSJA1	Certified InfiniStreamNG server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), AC.
C-02700-XSJD1	Certified InfiniStreamNG server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), DC.
C-04800-XSJA2	Certified InfiniStreamNG server, 1U, Dual Intel 6152 22-core 2.1GHz CPUs, 384GB RAM, 32TB (4x 8TB), AC Power.
C-04800-XSJD2	Certified InfiniStreamNG server, 1U, Dual Intel 6152 22-core 2.1GHz CPUs, 384GB RAM, 32TB (4x 8TB), DC Power.

Omnis IDS Sensor Adaptor

SKU	DESCRIPTION
9824GX	Omnis IDS Sensor Adaptor, 10G license, for use with 2-socket ISNG 4800/9800 series.

Omnis IDS Virtual Sensor

SKU	vCPU Blocks
9V2WG0	Omnis IDS Virtual Sensor 8-vCPUs
9V2VG0	Omnis IDS Virtual Sensor 5-pack
9V2HG0	Omnis IDS Virtual Sensor 25-pack

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

SPECIFICATIONS

Characteristic	D-02700-XSJA1	D-04800-XSJA2
Packet Capture Ports/Interfaces	4-Port 1/10 GbE SFP/SFP+ (Maximum 10Gbps license)	4-Port 1/10 GbE SFP/SFP+ (Maximum 40Gbps license)
Management Port	2 RJ-45 1/10GBASE-T 1 IPMI 1000BASE-T	2 RJ-45 1/10GBASE-T 1 IPMI 1000BASE-T
CPU	Single Skylake 22-core 2.1Ghz	Dual Skylake 22-core 2.1Ghz
Memory	192GB	384GB
Storage	32TB HDD in RAID 5	32TB HDD in RAID 5
Embedded OS	Solid State Drive (SSD) dedicated to Linux® OS	
Rack Unit	1 Rack Unit (1RU)	
Dimensions	1.7 in (43 mm) Height 17.2 in (437 mm) Width 25.6 in (650 mm) Depth	
Weight	38 lbs. (17.24 kg)	40 lbs. (18.2 kg)
Mounts	Rack mount side rails included	
Power Rating (AC)	700W/750W hot swappable, redundant, auto-ranging 700W: 100-140 VAC, 50-60 Hz, 8.0-6.0 Amp 750W: 200-240 VAC, 50-60 Hz, 4.5-3.8 Amp	
Maximum Consumption (AC)	100V, 3.9A, 400W, 1365 BTU/Hr	
Heat Dissipation (AC)	1999 BTU/hr	
Power Rating (DC)	1+1 hot-swappable, redundant -48VDC, 650W, 20A (x2)	
Maximum Consumption (DC)	12A, 581W	
Heat Dissipation (DC)	1982 BTU/hr	
Vibration	0.25G from 5-200Hz for 15 minutes	
Operating Temperature	41° to 95°F (5° to 35°C)	
Operating Humidity	8% - 90% (non-condensing)	
Altitude	-50 to 10,000 ft (-16 to 3,048 m)	
Mechanical Shock	1 shock pulse up to 20G for up to 2.5 ms	
Regulatory Approvals	Regulatory Model Number: NV51U, FCC Part 15 Class A, CE Mark (EN55032 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3), VCCI (Japan) Class A, RRA (Korea) KC Cert #: R-R-NSZ-NV51U, CCC Class A (China), EAC (Russia), BIS (India), UL- C of C (Mexico), CM (Morocco), UL 60950-1, CAN/CSA C22.2 No. 60950, IEC 60950-1, EN 60950-1, CB Report	

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

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

© 2021 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, 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.

EPDS_042_EN-2101 04/2021