Omnis Intrusion Detection System

Omnis IDS – Enabling Security Without Borders

It is said that there are two types of companies –those that have been hit with a security incident and others which don't realize they already have. Security incidents are intensifying worldwide, and that was never more evident than this past year, as everyone's work routines changed during the COVID pandemic. Security breaches were more sophisticated, their ability to elude discovery was greater, and their dwell time was reportedly between 49 and 150 days, according to the 2020 Verizon DBIR study.

Despite active programs and tool deployment, security risks and threats still pose significant impact on the targeted organizations, including loss of confidential data, compromise of proprietary intelligence, theft of customer and corporate financial information, and frequent disruption of user access to corporate applications. Financial impact can be significant for organizations targeted with ransomware attacks that damage or prevent access to critical data. Not only can the repercussions from cybersecurity attacks be swift and expensive, they can also become such a public exposure that the corporation's reputation and customer confidence are seriously damaged.

NETSCOUT® has developed an innovative, open-source based approach to provide a security solution that is consistent and effective in any infrastructure your organization may have deployed today and into the future. Omnis™ Intrusion Detection System (IDS), a key component of NETSCOUT's Omnis™ Security platform, is helping to extend the Visibility Without Borders approach to deliver Security Without Borders.

Problems Solved by Omnis IDS

Risks are different in today's networks. Everything is at a bigger scale, and the perimeter is more dynamic. Organizations are no longer protected by the traditional security stacks, many of which are outdated and siloed in nature, making them ever-less effective than before in identifying risks and threats. Over time, gaps in visibility and coverage have occurred as organizations have accelerated many of their digital transformation initiatives and application migrations to the cloud. The resulting threat landscape in the hybrid cloud environment is now larger and more complex than ever, making it more difficult to shield an organization from cyberattacks.

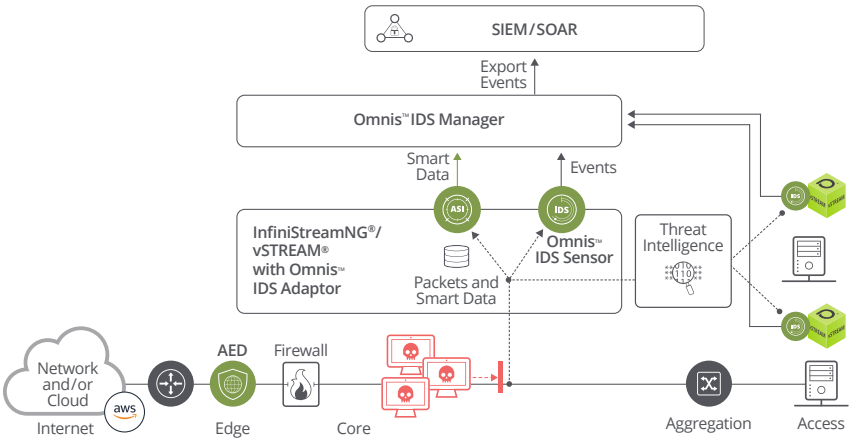

Figure 1: As strategically deployed Omnis IDS sensors monitor network traffic in real time, they leverage the Suricata rules engine as well as support for highly curated open-source, commercial, private, and customized ruleset technology to detect threats and send contextually rich alerts to the Omnis IDS Manager application and/or a SIEM.

NETSCOUT's Omnis IDS provides visibility for ubiquitous security intrusion detection with scale, scope, and consistency across your organization's entire digital infrastructure. Intrusion detection systems are a crucial part of any cybersecurity strategy, and the Omnis IDS solution provides an additional line of defense, making it more challenging for attackers to infiltrate an enterprise's network undetected.

Omnis IDS is comprised of Omnis™ IDS Sensor, Omnis™ IDS Virtual Sensor, Omnis™ IDS Sensor Adaptor for InfiniStreamNG appliances (Omnis IDS Sensors), and Omnis™ IDS Manager and is designed to provide packet monitoring visibility in on-premises, private, and hybrid cloud environments, including AWS. (Figure 1) Using the Suricata threat detection engine provides capabilities including deep packet inspection and pattern matching which makes it incredibly useful for threat and attack detection. Suricata can also help security teams in the race against time between a new vulnerability being announced and a patch working its way through change management. This is made possible with Suricata's rules engine and support for highly curated threat intelligence for open-source, commercial, private, and customized rulesets technology. The Omnis IDS Sensors, strategically deployed throughout the enterprise environment, monitor the network traffic in real time to detect security threats and send contextually rich alerts to the Omnis IDS Manager application and/or a SIEM. (Figure 1).

The Omnis IDS solution provides monitoring and threat detection for known cybersecurity risks and attacks, including:

- Malware
- Ransomware
- Network Trojans
- Brute-force attacks
- Lateral movements
- Privilege escalations
- Command & control exploits
- Corporate privacy violations

How Omnis IDS Supports Cybersecurity Processes

NETSCOUT Omnis IDS Sensors monitor network traffic for comparison to a database of signatures to detect known security threats, sending alerts to the Omnis IDS Manager for security analysts to evaluate a specific security event. Omnis IDS Manager expedites security threat detection with the following key analysis layers:

Omnis IDS Explorer provides a "see-everything," single-page dashboard with significant depth and breadth of information related to potential events and specific details and evidence for actual security incidents. Using this as a starting point, security analysts will evaluate detected threats with an easy-to-use Filters and Attributes window and readily available particulars found in Total Events and Threats windows for quick situational status.

- The **Explorer dashboard** is best used to identify and respond to specific security incidents with immediate access to relevant information, including a graph displaying Events and Bytes Timeline. Configurable views, charts, and analysis, in the form of widgets, based on filter attributes, are available pertaining to: IDS Classification; IDS Messages; Applications in Use; IP, Country, and Port Initiators; IP and Port Responders; and many other essential data points. (Figure 2).
- The full **Event List** is part of a threat summary that displays Event Context for each observed event. Different views and various column header attributes can be added or modified based on what is required for viewing and quick access. These may include IP and Port Initiators and Responders, and Application, Bytes and IDS Message Details for each event. (Figure 3).
- **Event Context** views provides further drill down in Omnis IDS Manager from the Event List to see specific data for individual events. Details regarding classification of a threat, the threat signature, initiator and responder IP addresses, and conclusive event evidence are displayed here.
- **SIEM Integration** ensures seamless operation with existing security stacks and workflows that employ SIEM / SOAR tools, such as Splunk, as well as with Omnis™ Cyber Investigator for additional investigation, response, and containment. The NETSCOUT Omnis Application for Splunk provides an efficient way to share event data for further evaluation using Splunk SIEM technology. (Figure 4).

Ease of Configuration

In the course of maintaining as many as a million rules, speed and efficiency in making changes to an IDS system are essential for reducing maintenance time for the Security Operations (SecOps) team. Unlike many homegrown, open-source IDS systems, the Omnis IDS solution offers simplified installation and configuration capabilities, making deployments streamlined and effective. The user-friendly, intuitive GUI dramatically reduces time and effort needed to configure filters; add, modify or disable signatures, and add rulesets; perform sensor management; and evaluate sensor health. Combined, this all helps organizations achieve SecOps efficiencies that have been lacking in other outdated and home-grown tools.

Benefits of Omnis IDS

IDS systems are the workhorse of any network detection and response solution, helping the SecOps team find that elusive needle in the haystack. With the increasing sophistication of attacks today, combined with the complexity of the enterprise deployments, the ever-increasing volume of traffic to monitor, and the criticality of the services supporting essential business operations, the IDS is more important than ever as a front-line defense in detecting and alerting of cybersecurity threats. The Omnis IDS is uniquely positioned to be that workhorse for organizations as part of the Omnis Security platform, with the following benefits:

- **Security Without Borders** protection by delivering complete visibility throughout your on-premises, hybrid, and cloud, including AWS, by deploying NETSCOUT's highly scalable network instrumentation throughout the entire network to obtain cost-effective, holistic digital infrastructure visibility.
- **Reduced time to detect risks to the corporate environment** by leveraging the powerful threat detection capabilities supported by Suricata advanced analytics open-source, commercial, private, and customized ruleset technology to automatically identify risks at scale.
- **Achieve SecOps efficiencies** over other homegrown, open-source IDS alternatives, with a common, consistent, easy-to-use solution that can be seamlessly integrated into existing security tools and processes.

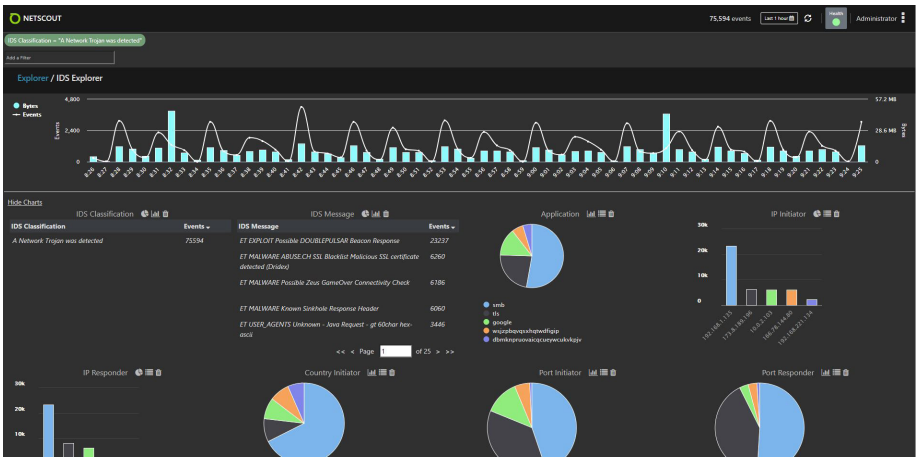

Figure 2: Omnis IDS Manager showing IDS Explorer Screen with view of the Event Timeline graph and configurable widgets related to event details.

- **Enhance IT, NetOps, and SecOps collaboration** by leveraging the integrated capabilities of the Omnis IDS solution with the overall Omnis Security platform supporting cybersecurity, network operations, and compliance management workflows via integration with NETSCOUT Cyber Investigator, Arbor Edge Defense (AED), and alert forwarding to third-party SIEM and SOAR solutions.
- **Faster response to serious threats** by leveraging powerful detection, investigative, and contextual forensics analysis capabilities that minimize catastrophic financial and reputational impact to the business from cybercriminals dwelling in the environment over protracted periods of time. Quick access to critical information reduces the time to identify the nature of a security threat to minutes.
- **Extends the value of single vendor partnership and investments** already made in NETSCOUT packet-based smart data visibility and monitoring technology with InfiniStreamNG appliances and vSTREAM® virtual appliances for both security and service assurance activities.

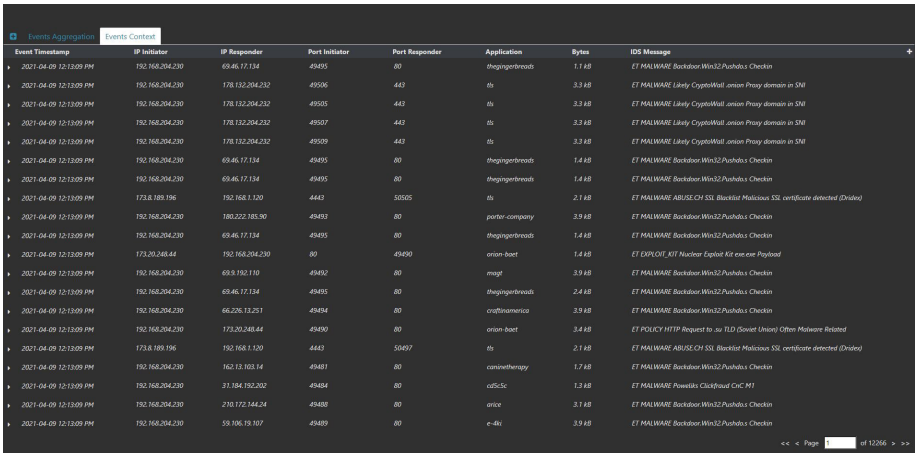

Figure 3: Omnis IDS Manager view of the Event List showing event aggregation and event context for each observed event.

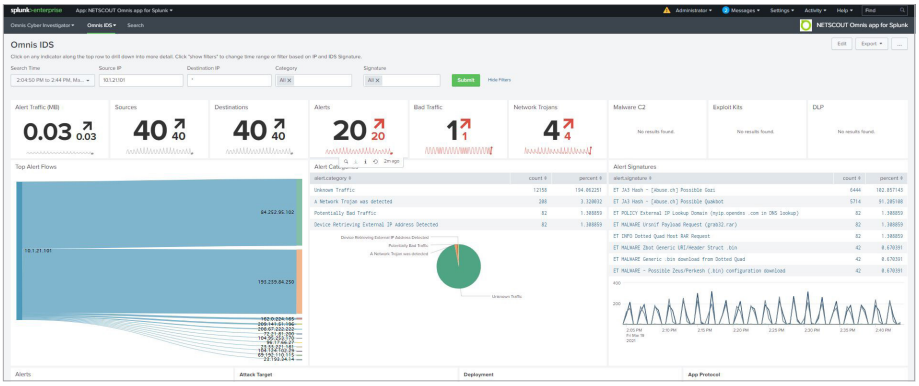

Figure 4: Seamless integration of Omnis IDS with other SIEMs, including Splunk. Screen shows data from Omnis IDS in the NETSCOUT Omnis Application for Splunk.

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

EQL_095_EN-2101 05/2021