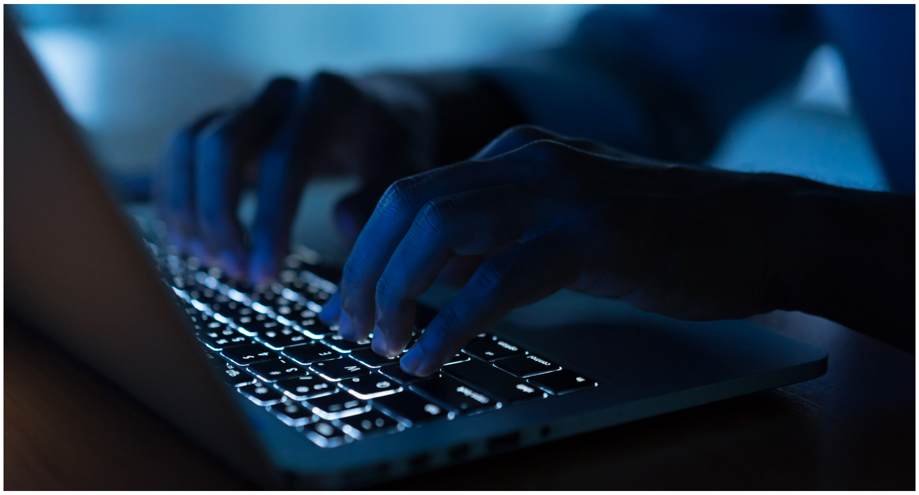
NETSCOUT Omnis Intrusion Detection System for Regulatory Compliance



Omnis IDS Solution Highlights

- Quickly detects intrusions, exploits, and vulnerabilities, providing SecOps with timely analysis needed for both remediation and regulatory compliance.
- Efficient threat metadata generated by open-source Suricata from Omnis® IDS Sensors.
- Evidentiary compliance support from industry-acknowledged Suricata threat detection engine.
- Contextually rich event export to the security ecosystem, including Splunk/ SIEM tools and now integrated into Omnis® Cyber Intelligence advance threat investigation and remediation platform.
- Easily deployed and managed, scaling to any-size enterprise network.

While the origins of Omnis® Intrusion Detection System (IDS) solutions date back to the mid-1980s, this technology remains important and relevant today, with IDS applications enabling Security Operations (SecOps) analysts to quickly identify information about current threats inside the enterprise.

Given the maturity of this technology and intrinsic value it offers in terms of securing enterprise operations, it's no surprise that IDS solutions are identified – by name – as a necessary IT element in achieving compliance with numerous industry and security regulations.

For example, the Payment Card Industry Data Security Standard (PCI DSS) information security standard for organizations that handle branded credit cards contains regulations identifying the needs for IDS solutions[1], specifically:

- Using IDS or an Intrusion Prevention System (IPS) solution to detect and/or prevent network intrusions.
- Monitoring security controls.
- Generating audit trails, sending data to monitoring mechanisms like IDS, and providing historic analysis (e.g., event logs) for post-incident activities.

Monthly PCI non-compliance fines can range from $5,000 to $100,000, depending on a company's size, as well as the complexity and timeframe involved.

As detailed in Table 1, numerous regulatory initiatives obligate enterprises to comply with specific security reporting requirements, heightening the need to step up IDS monitoring and preventive strategies.

In addition to the cybersecurity and standards compliance motivators driving SecOps and Network Operations (NetOps) teams' continued reliance on IDS, numerous regulations identified in Table 1 have prompted organizations to elevate the Chief Compliance Officer role to board-level visibility and influence. With these parties now collectively responsible for organizational regulatory compliance, the need for access to evidentiary compliance provided by IDS tools – including logs, analytics, reports, and forensic data – has never been greater.

While these compliance management activities have raised the profile of IDS tools, the cyberthreat landscape changes coinciding with the hybrid workforce transition further increased their value in light of monitoring tremendous amounts of east-west traffic that didn't previously exist.

Selection, placement, and maintenance of IDS solutions are based on the requirements and current infrastructure of a company. One product may work well for one company and fail for another. Selection is typically the most difficult decision, for products must meet business requirements, function correctly within the intended network infrastructure, and be supportable by current personnel.

Intrusion detection is vital, because it is impossible to keep pace with every current and potential threat and vulnerability in a network. These threats and vulnerabilities advance at lightning speed, and it takes time for vendors to catch up with patches and updates (and for administrators to apply those updates). Therefore, IDS's have become indispensable in helping to manage these threats and vulnerabilities.

[1] Source: PCI DSS v3.2.1

Table 1: Defining the Need for IDS – Regulatory Compliance Requirements and Non-Compliance Penalties

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: This security and privacy controls standard requires all U.S. federal information systems (except those pertaining to national security) to "connect and configure individual intrusion detection tools into a system-wide intrusion detection system."

Federal Information Security Management Act (FISMA): Companies that provide services to the federal government must comply with FISMA. Based on NIST 800 (see above), FISMA requires companies to self-assess and manage risks associated with cybersecurity, as well as perform annual audits and semi-annual risk assessments of insurance system and communications protection. Failure to comply can result in loss of government funding or participation in future contracts, as well as potential government hearings and reputational damage[1].

Health Insurance Portability and Accountability Act (HIPAA): Requires that healthcare and insurance organizations "Information systems housing PHI must be protected from intrusion." Notification of breaches must be provided to the Department of Health and Human Services, which can result in financial penalties for non-compliance of up to $250,000 and criminal penalties.

National Association of Insurance Commissioners (NAIC): The Insurance Data Security Model in 2017 is the basis of multiple current state laws (and which is before other state legislatures for consideration) requiring the implementation of an information security program that covers data security, investigation, and notification to regulators of security breaches and events within 72 hours.

Gramm-Leach-Bliley Act Requirements (Financial Services Modernization Act of 1999): Financial companies must meet specifications for secure handling of non-public personal and financial information.

Securities and Exchange Commission (SEC): Upgraded guidance requires publicly traded companies to disclose security breaches and service outages caused by cyberattacks within 72 hours, holding board of directors and executives responsible for cybersecurity disclosures.

General Data Protection Regulation (GDPR): Foreign companies processing data belonging to EU residents are required to comply with GDPR. The data protection laws and requires disclosure of breaches within 72 hours; otherwise, insurance companies risk fines ranging from 10,000,000 EUR or 2% revenue for low-level failures to 20,000,000 EUR or 4% revenue for high-level failures.

[1] Reference: https://blog.rsisecurity.com/penalties-for-non-compliance-with-fisma-and-how-to-avoid-them/

Our Approach

The Omnis Intrusion Detection System (IDS) is a foundational and intrinsic element of the NETSCOUT® Omnis cybersecurity defense-in-depth portfolio, providing ubiquitous security intrusion detection with scale, scope, and consistency.

In providing continuous monitoring and analysis of network activity and data for potential exploits, vulnerabilities, and attacks in progress, Omnis IDS protects enterprises from infiltration by unwanted and untrusted external networks (i.e., north/south traffic), while tracking hard-to-see lateral movement (i.e., east/west traffic) throughout the services environment.

Our network-based IDS was designed for deployment on the external demilitarized zone (DMZ) segment, then the DMZ segment, which enables monitoring of all external and DMZ malicious activity.

Omnis IDS monitors all external network segments, including inbound and outbound traffic to ensure all devices connected to external hostile networks are monitored and checked. In this manner, Omnis IDS meets industry standards regarding the tracking of malicious activity at the extranet, Intranet, and DMZ environments. Omnis IDS also supports use at all entry points to ensure monitoring of all malicious attempts on company resources, including both well-known network connections and all known external connections.

Many organizations will find that the Omnis IDS is a more attractive technology alternative for replacing their sometimes-cumbersome and time-intensive homegrown, open-source deployments. With a fully integrated, open architecture that seamlessly operates with existing enterprise security stacks, the Omnis IDS solution improves SecOps detection and response capabilities.

Our Solution

The Omnis IDS solution provides the holistic network traffic visibility necessary for expedient, effective threat detection and response by taking advantage of Omnis® IDS Sensors deployed across the enterprise. Omnis IDS Sensors leverage Suricata's open-source threat detection engine to equip SecOps with the ability to use both commercial and custom rules, thereby providing the ability to make changes without disrupting threat detection services. The use of Suricata in Omnis IDS also maximizes superior network packet acquisition by Omnis IDS Sensors, making it well-suited for SecOps cyberthreat and attack detection activities. In addition to the performance and adoptability offered by Suricata, this open-source threat detection engine has earned acceptance from industry Compliance Auditors and Security Analysts.

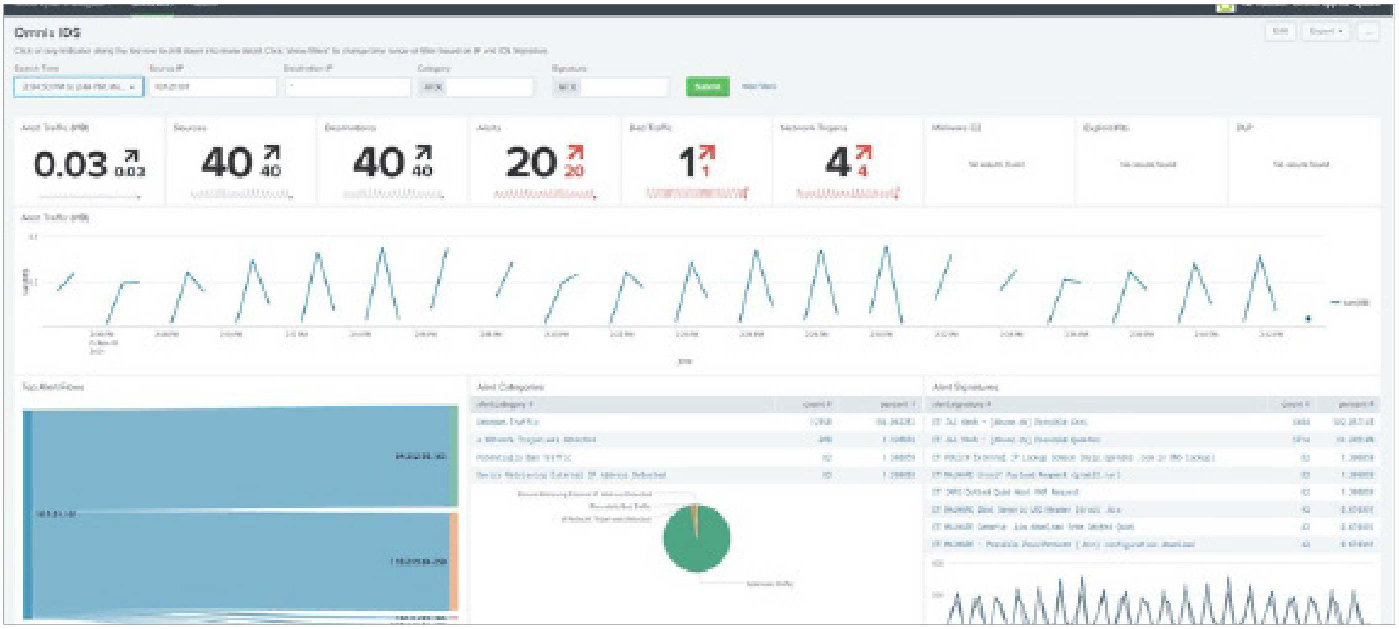


Figure 1: Omnis IDS integrates with Splunk Enterprise SIEM, enabling SecOps resources to use well-established workflows and Suricata-generated threat metadata to enhance remediation efficiencies.

The Omnis® IDS Explorer provides a centralized graphical console for Omnis IDS, equipping SecOps, NetOps, and other Technology Operations teams with the means to configure, edit, and customize all sensors from a "single pane of glass," with no downtime. The Omnis IDS Explorer solves the frequent troubleshooting quandary of finding the threat in the "haystack" of event logs and false positives by providing analyst-definable features in the Event/Bytes Timeline, Filter Attributes, and Event List/ Log features, all of which support intuitive workflows to quickly pinpoint the threat and forward event details to the NETSCOUT Omnis® Cyber Intelligence network threat and risk investigation platform.

In delivering centralized IDS reporting, Omnis IDS Explorer that is integrated into Omnis Cyber Intelligence aggregates data for simple visualization, views, and customized prioritization, which provides SecOps teams with the information needed to understand the attack and respond faster. By offering complete visibility into the entire attack chain and risks associated with it, Omnis IDS Explorer assists SecOps' correlation, collaboration, and refinement of response efforts by forwarding event details and threat reports to third-party SIEM tools, including Splunk Enterprise as exhibited in Figure 1.

Our Value

With Omnis IDS and NETSCOUT cybersecurity solutions, enterprises benefit from:

- **Assuring Regulatory Compliance**: Greater visibility across the entire enterprise landscape, using Omnis IDS Sensors makes it easier for SecOps/ NetOps to meet security standards.
- **Easier evidentiary compliance across industry security standards (e.g., PCI and HIPAA)**: Provides effective IDS at scale, using Suricata-generated analysis, alerts, and reports, which is a format already accepted by Compliance Management auditors.
- **Integration with security ecosystem:** Omnis IDS alerts and reporting can be forwarded to your currently deployed SIEM solution to enhance the value of existing remediation workflows, as well as with the Omnis Cyber Intelligence solution to extend your investigation and reporting capabilities.
- **Reduced financial loss**: Rapid, focused detection and logical, intuitive workflows for threat investigation minimize exposure to security threats and costly repercussions, such as non-compliance penalties, remediation costs, and damages to customer loyalty and reputation.

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