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 platform.
- Easily deployed and managed, scaling to any-size enterprise network.

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. Using IDS or an Intrusion Prevention System (IPS) solution to detect and/or prevent network intrusions.
3. 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.

According to the PCI DSS v3.2.1, organizations that handle PCI data must implement an IDS or IPS solution to detect and prevent network intrusions.

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, IDSs have become indispensable in helping to manage these threats and vulnerabilities.

1 Source: PCI DSS v3.2.1
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:

- **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.

**Our Value**

**Assuring Regulatory Compliance:**
Greater visibility across the entire enterprise landscape, using Omnis IDS Sensors makes it easier for SecOps/NetOps to meet security standards.

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.