NETSCOUT

NETSCOUT Omnis Intrusion Detection System

IDS Requirements and Business Issues

- Safeguarding networks from attacks and breaches, addressing evolving cybersecurity requirements
- Increased IDS requirements in industry security, with significant non-compliance penalties
- IDS subject matter expertise in short supply
- "Vendor fatigue," with too many tools creating IT functional silos, increasing CapEx/ OpEx and management cycles

The NETSCOUT® Threat Intelligence Report for Second-Half 2020 provided detailed evidence that cybercriminals were further emboldened during the global COVID-19 pandemic, including "a huge upsurge in distributed denial-of-service (DDoS) attacks, brute-forcing of access credentials, and malware targeting of internet-connected devices."

These cyberattacks frequently focused on heavily regulated e-commerce, pharmaceutical, and healthcare organizations, as well as remote educational services that became more vulnerable and exploited during that time.

When breaches do occur, they are time-consuming to contain (as high as 280 days) and costly (averaging $3.86M per incident, globally), according to another report.[1]

These reports only validate what NETSCOUT is hearing from our customers – even before the arrival of the hybrid workforce era, threat detection was already one of the fastest-growing cybersecurity challenges in the information technology (IT) operations arena. Despite the number of security solutions on the market, companies continue to get compromised. That is because security is still too difficult, and complexity becomes the actual threat. Organizations need security that is simple to use, comprehensive in scale, and which offers scale scope and consistency.

In this cyberthreat environment, Intrusion Detection Systems (IDSs) remain an essential SecOps solution required for securing data center, network edge, branch office, and cloud (e.g. AWS) workloads.

Increased IDS use has also been seen in response to IT teams' efforts to meet relevant security and business regulatory compliances governing their industries.

Omnis IDS Extends the Value of the NETSCOUT Single-Vendor Approach and "Smart Visibility" Platform Into Intrusion Detection Services and Regulatory Compliance

Unlike many other security controls, IDS technology is specified by name in several regulatory and best practices frameworks. Several of these standards – such as Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management (FISMA), Payment Card Industry (PCI), and General Data Protection Regulation (GDPR) – are relevant across multiple industry sectors, representing only a subset of regulations that IT teams are working to address across their own network and service environments. As a result, IT teams must secure their corporate operations in compliance with these standards; otherwise, another expensive occurrence could impact the business. In addition to facing non-compliance penalties as high as to $250,000 for HIPAA or $20 million Euro for GDPR failures, the reputational damage from public disclosures of security incidents can also be costly, with recovery processes taking months or longer.

Even with Intrusion Detection Systems and available Security Analyst expertise in place, the nature of many IDS technology solutions themselves add unnecessary levels of workload complexity to short-cycled SecOps teams. Many of these IDS solutions are difficult to manage and scale, offer high false positives, lack easily recognized compliance roles, or perpetuate IT operational silos. As a result, the actual designs of those IDS tools themselves compromise Security Analysts' efficiencies.

[1] Source: IBM Security Report.

Our Approach

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

In providing continuous monitoring and analysis of network activity and data for potential 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 service environment.

Our Solution

Omnis IDS Solution Highlights

- High performance IDS solution using Suricata open source technology
- Omnis IDS Manager for centralized management via intuitive Web UI
- 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, and/or SIEM, including Splunk

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, an open-source, mature, fast and robust network threat detection engine. Suricata inspects the network traffic using a powerful and extensive rules and signature language.

Omnis IDS also offers the benefits associated with reducing "alert fatigue" experienced by many SecOps teams, providing the ability to pick and choose the alerts most relevant to business operations and compliance management activities. Omnis IDS sensors are available on NETSCOUT-Certified and -Qualified software platforms. Additionally, the Omnis® IDS Sensor Adaptor is an add-on to approved InfiniStreamNG® (ISNG) software appliances. In this mode, ISNG continues to produce Adaptive Service Intelligence® (ASI) to fuel nGeniusONE® Service Assurance performance analytics. In parallel, the Omnis IDS Sensor Adaptor installed in the same ISNG collects network traffic, analyzes that traffic, detects intrusions, and produces events to send to the Omnis™ IDS Manager.

The Omnis IDS Manager provides a centralized management interface, equipping SecOps teams with the means to configure, edit, and customize all Omnis IDS Sensors from a "single pane of glass" with no downtime. The Omnis IDS Manager makes the configuration simple and consistent by using templates to configure one or multiple sensors, which saves time and reduces configuration errors. Additionally, Omnis IDS Manager 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 third-party Security Incident and Event Management (SIEM) tools, such as Splunk.

In delivering centralized IDS reporting, Omnis IDS Manager 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 Manager assists SecOps' correlation, collaboration, and refinement of response efforts by forwarding event details and threat reports to SIEM tools.

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 will improve SecOps detection and response capabilities.

Our Value to Information Technology and Security Operations Teams

The Omnis IDS solution provides benefits to organizations across all business and industry sectors by:

- **Improving NetOps and SecOps collaboration,** with Omnis IDS supporting cybersecurity, network operations, compliance management workflows and alert forwarding to SIEM tools.
- **Offering fast and flexible operation,** with Omnis IDS easing the arduous tasks of tuning and maintaining the enterprise IDS platform, while offering best-in-class performance levels.
- **Delivering greater network operations context,** with Omnis IDS alerts automatically correlated with other network events that happen before and after the alert is fired. This additional context enables Omnis IDS to provide richer situational awareness and quicker incident response workflows, all without requiring SecOps management tool architects to cobble together multiple secondary data stores to prop it up.
- **Offering a single-vendor approach to cybersecurity, smart edge visibility, and real-time service assurance,** with IDS Sensor data source technology available on ISNG from NETSCOUT as a trusted vendor. We have a proven record with enterprises, government agencies, and carrier service providers that have relied on us for years to provide market-leading, innovative technologies that help support and protect their businesses.

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