NETSCOUT

I SOLUTION OVERVIEW I

Omnis Cybersecurity

Omnis Cybersecurity: A Layered Architecture for Network-Centric Threat Detection, Investigation and Response

TABLE OF CONTENTS

Introduction

In today's dynamic threat landscape, security teams are under pressure to detect and respond to attacks faster than ever. Traditional tools, whether based on NetFlow, sampled packets, or log data; often fall short. They can be blind to east-west traffic, miss encrypted threats, or rely on endpoint agents that can be disabled or manipulated.

Omnis Cybersecurity by NETSCOUT takes a fundamentally different approach. It starts with full network packets; the one system that sees everything. Unlike endpoints, where traces of malicious activity can be hidden or overwritten, packet-level visibility offers an immutable, high-fidelity source of truth. By capturing and analyzing this data in real time, Omnis Cybersecurity delivers the visibility, context, and speed needed to detect threats earlier, investigate with precision, and respond with confidence.

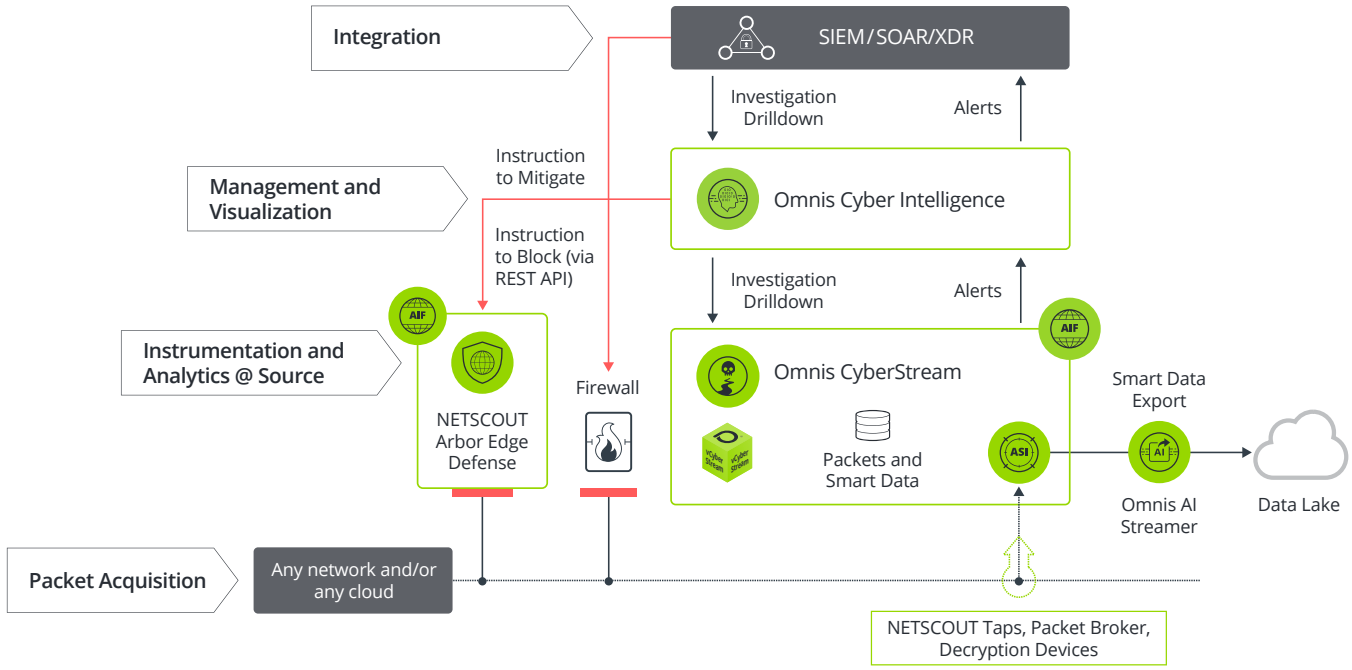
This whitepaper introduces NETSCOUT's layered architecture for network-centric threat detection, investigation and response. It outlines how Omnis Cybersecurity closes visibility gaps, accelerates detection, and integrates seamlessly into existing security ecosystems; empowering teams to meet today's challenges head-on.

Closing the Gaps in Threat Detection, Investigation and Response

As organizations adopt hybrid cloud, remote work, and increasingly complex infrastructures, visibility has become fragmented. Many threats now evade detection by hiding in encrypted traffic, lateral movement, or legitimate applications. NETSCOUT's Omnis® Cybersecurity solution fills these visibility gaps with a packet-based approach to threat detection, investigation and response.

Unlike traditional systems that depend on logs or endpoint agents, Omnis Cybersecurity starts with the network, the one system that sees everything. This paper outlines how NETSCOUT's layered architecture delivers pervasive visibility, real-time detection, forensic investigation, and seamless integration into the broader security ecosystem.

The Omnis Cybersecurity Architecture



Packet Acquisition Layer: Capturing Everything that Matters

At the foundation of the Omnis Cybersecurity platform is a robust packet acquisition layer designed to capture all relevant traffic — regardless of location, speed, or encryption. This layer ensures that security teams have complete north-south and east-west visibility into every packet traversing the network, enabling accurate detection and deep forensic analysis.

NETSCOUT is one of the cybersecurity and network visibility leaders that builds and owns its entire scalable packet acquisition infrastructure, from taps and brokers to decryption appliances. This level of integration ensures compatibility, consistency, and high-quality visibility across any environment (e.g., local data center, Colo, private/public cloud).

By starting with packets, the most reliable and complete source of network truth, Omnis Cybersecurity removes visibility gaps and empowers security teams with trustworthy data for faster, more confident decision-making.

Key Technologies and Components:

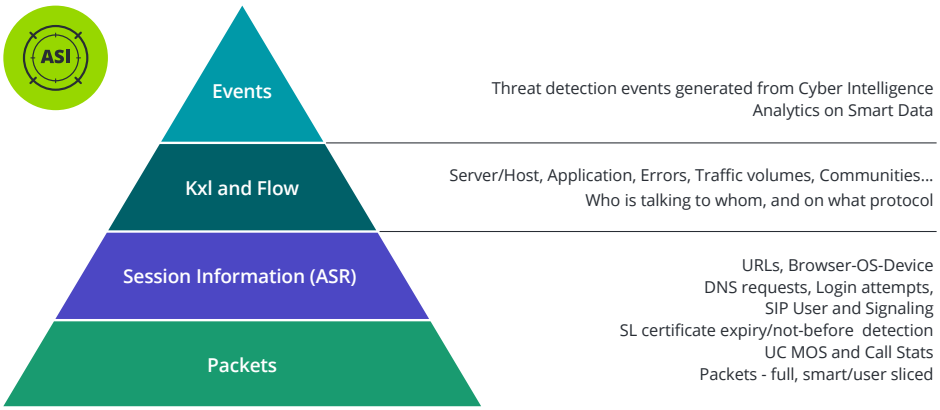
- **Taps, SPANs, and Mirrors:** Physical and virtual taps, SPAN ports, and cloud-native mirroring (AWS VPC, Azure vTap, etc.) ensure total coverage.
- **Packet Flow Switch (PFS):** High-performance packet brokers that deduplicate, filter, and route traffic intelligently to sensors.
- **nGenius Decryption Appliance (nDA):** Offers inline/out-of-band decryption of SSL/TLS and SSH traffic (up to 40 Gbps), supporting legacy and modern encryption standards.

NETSCOUT® stands out as one of the few NDR vendors that builds and owns its entire packet acquisition infrastructure, from physical taps and packet brokers to advanced decryption appliances. This level of vertical integration eliminates common compatibility issues and ensures consistent, high-quality traffic visibility across any environment. The nGenius Decryption Appliance (nDA) further differentiates the platform by delivering high-speed SSL/TLS decryption, including support for TLS 1.1, 1.2 and 1.3, without introducing latency or degrading network performance, capabilities that are rare among competitors.

By removing blind spots, especially within encrypted traffic, NETSCOUT empowers security teams with complete, trustworthy visibility. The result is faster, more accurate threat detection and a stronger foundation for confident decision-making.

Analytics at the Source Layer: Real-Time, High-Fidelity Detection

Omnis CyberStream sensors analyze packet data at the point of capture, minimizing delay and maximizing context. This "analytics at the source" model avoids centralized bottlenecks, improves scalability and enables earlier detection.



Deep Packet Inspection (DPI) and Adaptive Service Intelligence (ASI):

- Converts raw packets into actionable metadata, including:
  - Adaptive Session Records (ASR): Protocol-specific connection metadata.
  - KPIs: Network/application health indicators.
  - Error Indicators: DNS failures, HTTP codes, latency spikes.

Multi-Layer Threat Detection:

- **Threat Intelligence:** Leverages NETSCOUT's global ATLAS® feed and third-party sources.
- **Signature Detection:** Suricata-based IDS built into every sensor.
- **Behavioral Analysis:** Baselines normal behavior to identify anomalies and zero-days.
- **Policy Violations:** Custom rules to enforce Zero Trust and compliance.
- **Protocol/Port Mismatch Detection:** Identifies rogue services or evasive malware on non-standard ports.

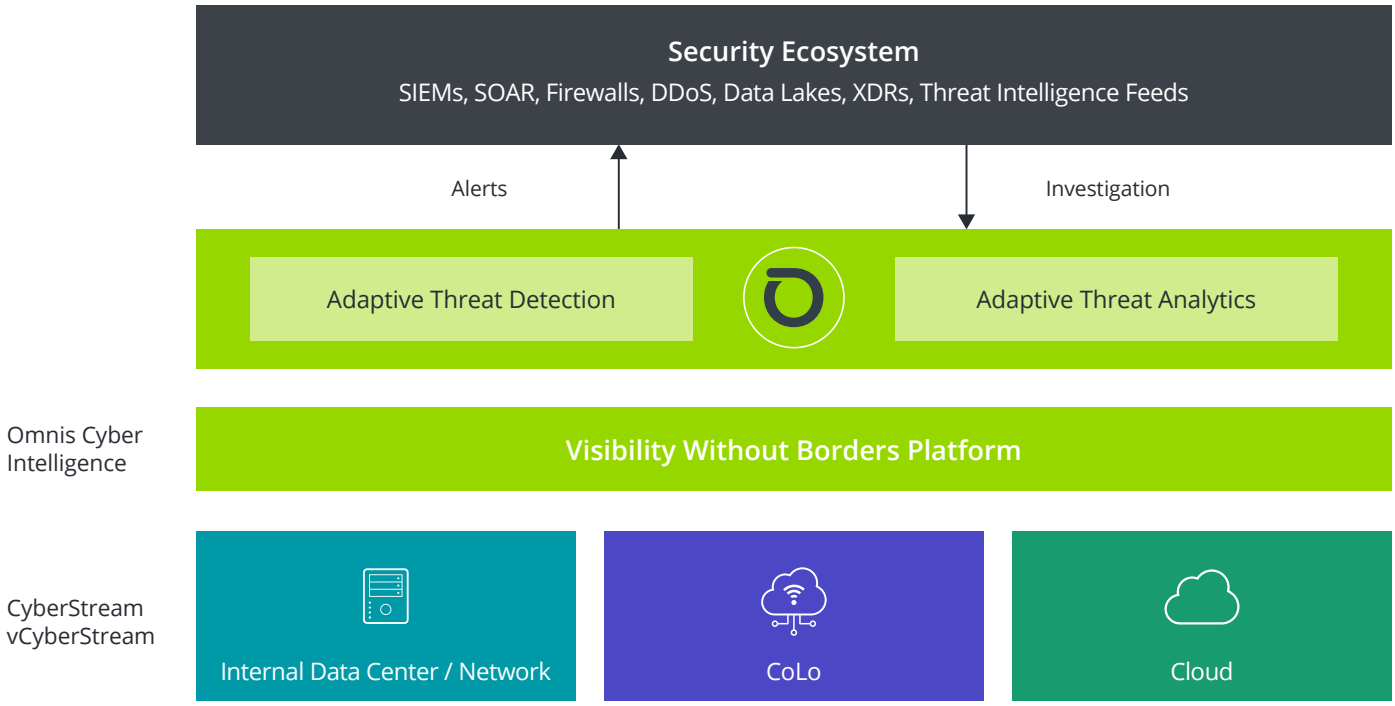
Clustering and Scaling: Omnis CyberStream supports clustered deployment to handle high-throughput environments. By combining NETSCOUT Packet Flow Switches with multiple sensors, traffic can be logically grouped for scalable, distributed visibility. Ideal for environments exceeding 40–100 Gbps. This architecture ensures seamless north-south and east-west visibility across complex networks, enabling faster, broader threat detection and investigation.

Adaptive Storage Technology (AST) & VIP Partitions: Each sensor captures, decodes, and indexes packets continuously, independent of alerts, and can store up to 768 TB locally. AST uses patented compression and indexing to retain 5x more packet data than traditional solutions, making long-term investigation possible without excessive hardware. VIP Partitions reserve storage for critical assets, ensuring extended retention and faster analysis for high-value targets.

Unlike other NDRs that centralize processing and rely on alert-driven capture, NETSCOUT delivers real-time analytics with continuous packet capture to provide full-packet visibility that is independent of alerts. Our ASI engine produces richer metadata and automatically identifies protocols and apps, even on non-standard ports or when obfuscated. This empowers teams with high-fidelity, real-time alerts and deep historical context to enable faster response, true zero-day investigation, and proactive threat hunting at scale.

Enrichment & Visualization Layer: Unified Management, Visibility, Detection, and Investigation

At the core of the solution is Omnis Cyber Intelligence, a central console that brings together packet data, threat detections, and investigative workflows.



Key Functions:

- **Visibility Without Borders:** The Omnis Cyber Intelligence console provides comprehensive visibility into north-south and east-west traffic.
  - Unified view across all CyberStream sensors including on-prem, remote, cloud, or containerized environments.
  - Agentless, passive monitoring preserves privacy and scalability.
- **Adaptive Threat Detection (ATD):** The brain behind real-time alerting, powered by high-fidelity metadata and packet analytics from CyberStream sensors. Unlike generic alerting engines that flood SOC dashboards with raw signatures, ATD provides context-aware, prioritized alerts that are easy to triage.
  - **Multidimensional Threat Detection:** Correlates insights from behavioral analytics, threat intelligence, heuristics, and signature-based detection to form a composite alert. (See Figure 1)
  - **MITRE ATT&CK Alignment:** All alerts are mapped to tactics and techniques in the MITRE ATT&CK framework for standardized, actionable response. (See Figure 2)
  - **Risk and Severity Scoring:** Each alert is enriched with dynamic risk indicators based on impact, spread, behavior, and host criticality.
  - **Real-Time Security Events Center:** An intuitive dashboard for viewing, sorting, acknowledging, and assigning alerts.

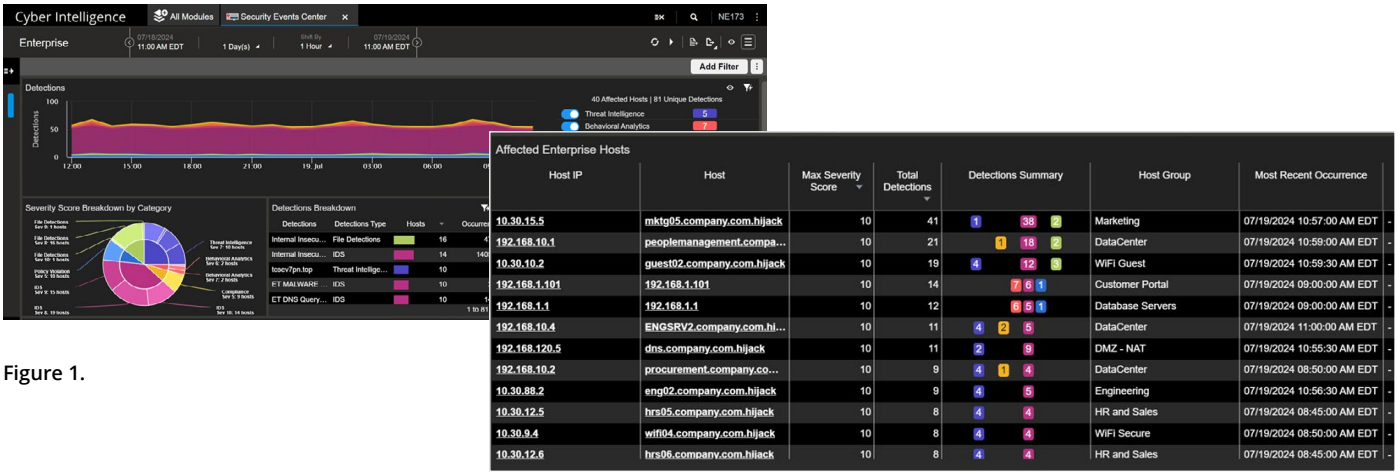


Figure 1.

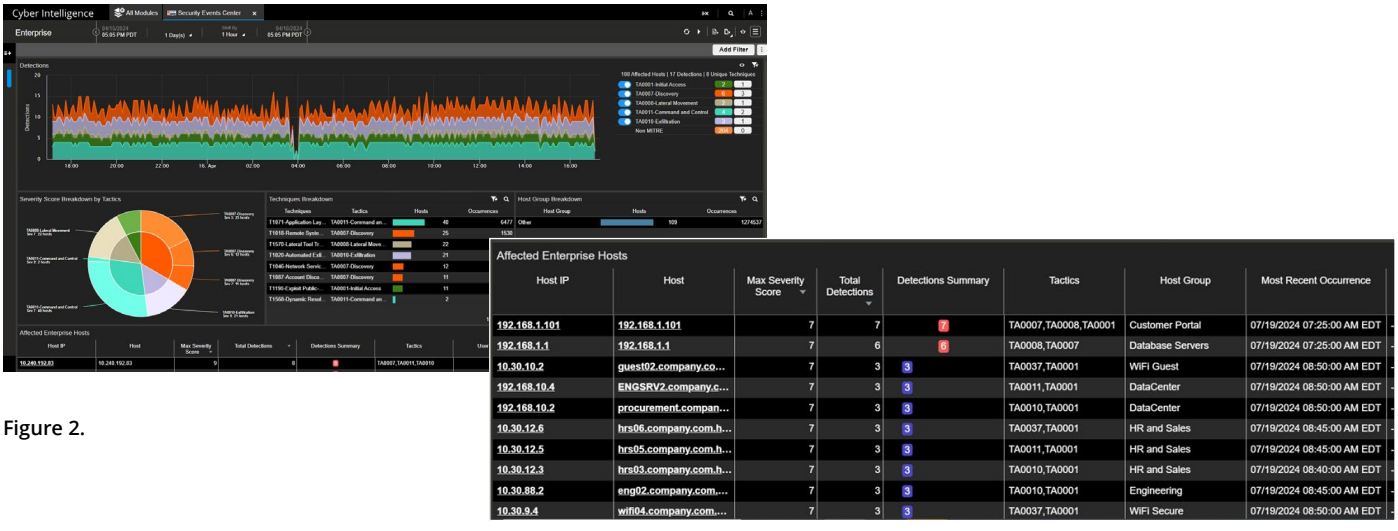
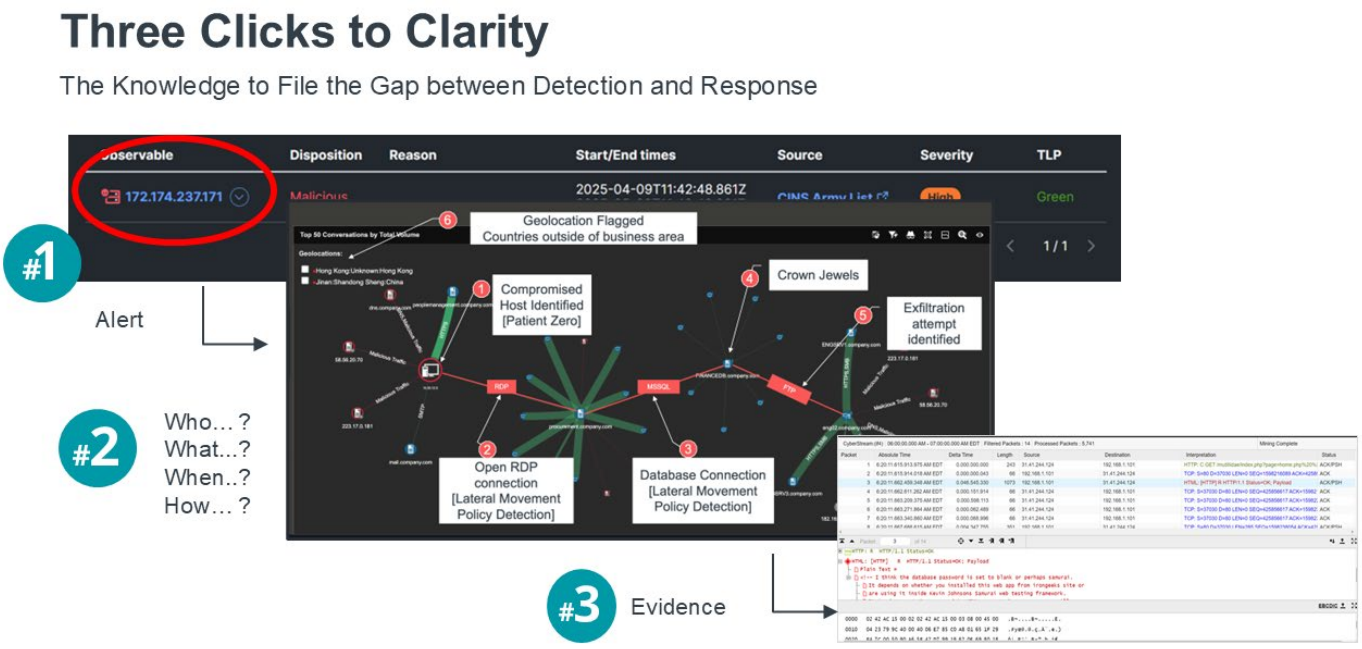


Figure 2.

- **Adaptive Threat Analytics (ATA):** Once a threat is detected, analysts need the ability to quickly validate, investigate, and act. That's where Adaptive Threat Analytics (ATA) comes in. Built into the Omnis Cyber Intelligence console, ATA streamlines the investigative process from alert to evidence.



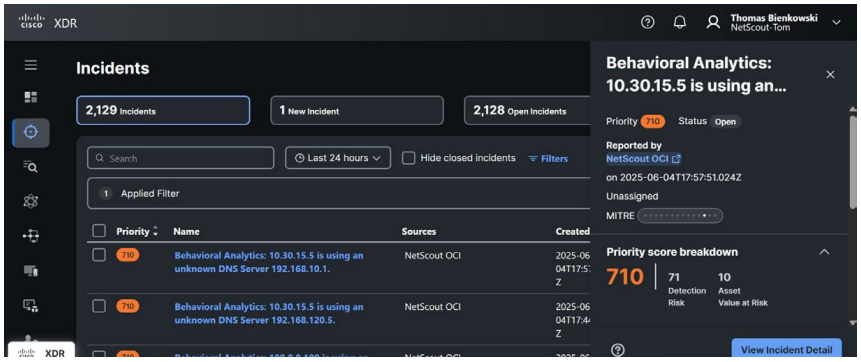
  - **Three Clicks to Clarity:** From alert to session metadata to packet decode in just three intuitive clicks.
  - **Historical Investigation:** Navigate backward in time to understand what happened before, during, and after an alert.
  - **Host-Based Investigation:** Trace communications for a specific IP, user, or asset to visualize lateral movement or discover patient zero.
  - **Unguided Investigations:** SOC analysts can use ATA independently of alerts to proactively search for signs of compromise or suspicious patterns.
  - **Natural Language Metadata Querying:** Analysts can conduct complex searches using plain-language input. Ideal for threat hunting or third-party alert validation.

Omnis Cybersecurity sets itself apart by unifying Adaptive Threat Detection (ATD), Adaptive Threat Analytics (ATA), and its Visibility Without Borders architecture into a single, streamlined investigation workflow. ATD reduces alert fatigue by correlating rich metadata across multiple engines to deliver only high-fidelity, MITRE-aligned alerts. ATA then enables analysts to quickly pivot from alert to evidence using continuous, detection-independent packet and metadata capture with no external tools required. Combined with agentless, passive visibility across cloud, virtual, and on-prem environments, Omnis Cybersecurity helps security teams detect stealthy lateral movement and investigate threats with unmatched speed and clarity. From alert to resolution, Omnis Cybersecurity empowers analysts of all levels to work faster, smarter, and with greater confidence.

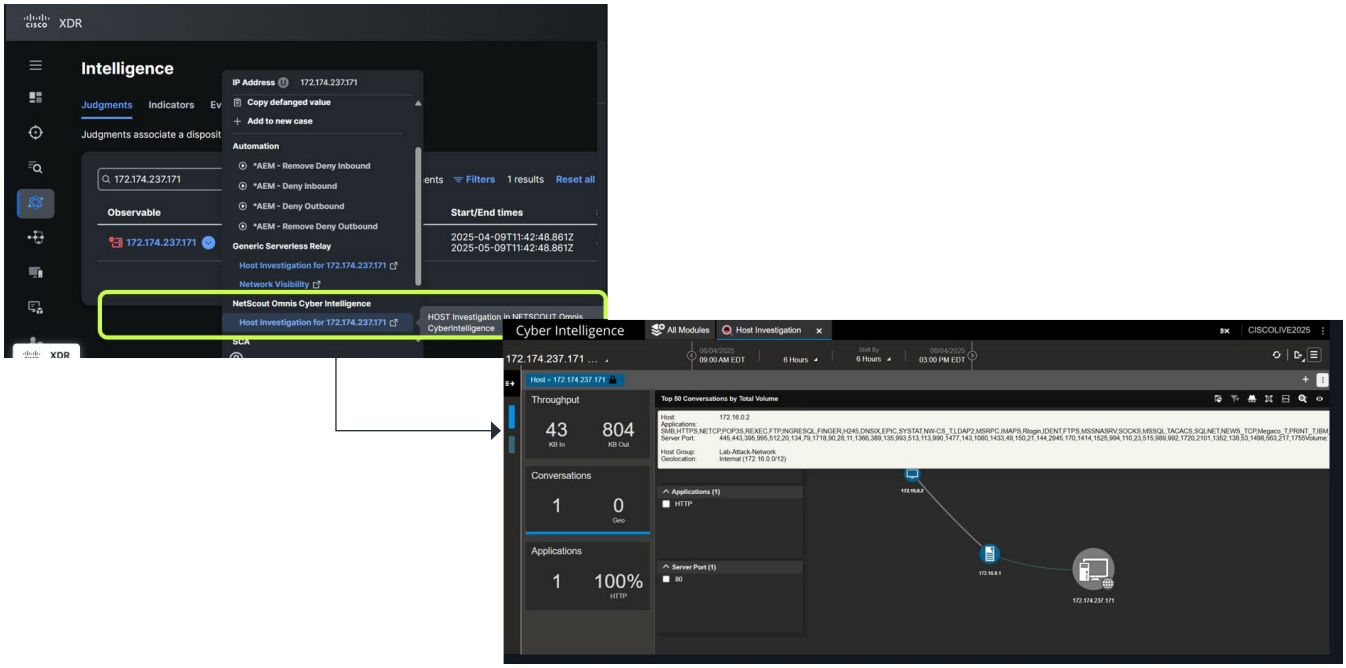
Integration Layer: Powering the Broader Security Ecosystem

Omnis Cybersecurity is built to work alongside and enhance your existing security stack with seamless integration with other cybersecurity tools, including SIEM, EDR, SOAR, and XDR systems.

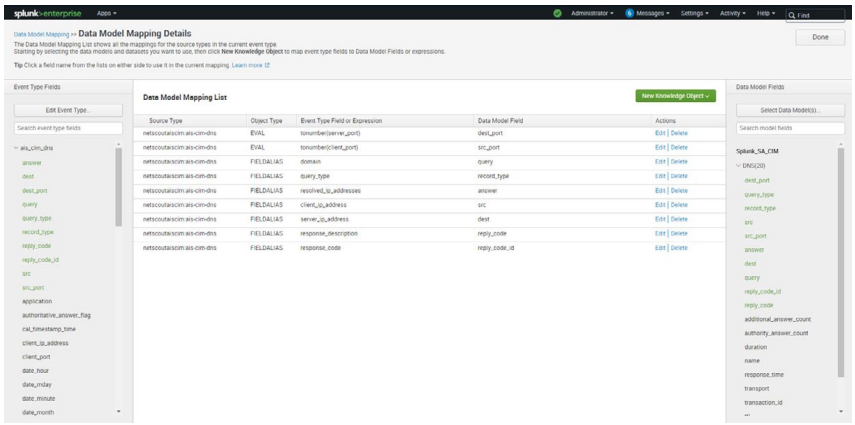
- FEED Framework: "Framework for Extensible EcoSystem Integrations and Dispatch" (FEED)
  - Generic scripting language that enables interface with third-party systems via a fully documented REST API.
  - Supports the Open Integration Framework and is field programmable.
- Enables tri-directional integration. It can ingest alerts, investigate them using network context, and send back detections or remediation commands.
  - **Send Alerts and Trigger Response:** Omnis Cyber Intelligence delivers SYSLOG-formatted alerts to SIEM, SOAR, or XDR platforms for correlation, and can initiate remediation by sending commands to firewalls, EDRs, or NETSCOUT's Arbor Edge Defense® via the FEED scripting framework.



  - **Ingest Threat Intelligence and Enrich Alerts:** Omnis consumes STIX/TAXII feeds and Suricata rules, while its open API enables investigation of third-party alerts using Omnis' scalable and continuously stored packets and metadata context.



– **Export Enriched Metadata:** With the Omnis AI Streamer add-on, curated ASI-derived metadata is exported to external data lakes or AI pipelines in formats like JSON, AVRO, and CSV for advanced analysis.



Key Use Cases

- **Real-Time Threat Detection in Hybrid Cloud:** Detect and prioritize emerging threats across cloud, data center, and remote networks with no agents or blind spots
- **Accelerated Investigation Workflows with ATA:** Omnis Adaptive Threat Analytics (ATA) streamlines the investigative process from alert to evidence. Analysts can pivot from high-fidelity alerts to session metadata and full packet decode in just three clicks. Host-based and historical investigations reveal lateral movement, patient zero, and pre-attack behaviors with unmatched speed and clarity.
- **Third-Party Alert Validation and Enrichment:** Security teams can validate alerts from SIEM, EDR, or XDR platforms using independent, packet-level evidence. This reduces false positives, improves triage accuracy, and strengthens incident response confidence. Omnis also enriches alerts with context from threat intelligence feeds and continuously captured metadata.
- **Proactive Threat Hunting:** Analysts can conduct unguided investigations using natural language queries to search for suspicious patterns, anomalies, or indicators of compromise — even in the absence of alerts. This enables proactive defense and early detection of zero-day threats.
- **Compliance and Forensic Readiness:** With continuous packet capture and long-term retention powered by Adaptive Storage Technology (AST), Omnis supports forensic investigations, audit trails, and compliance reporting. VIP Partitions ensure extended visibility for critical assets and high-value targets.

Omnis Cybersecurity by NETSCOUT redefines what modern detection, investigation and response should look like. By starting with packets, which is the single source of truth, it offers unmatched comprehensive network visibility, accurate detections, and decisive investigation capabilities for appropriate response. Designed for scale, speed, and ecosystem fit, it empowers security teams to meet today's evolving threat landscape head-on.

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

SECWP_036_EN-2601 02/2026