

Omnis Cyber Intelligence and CrowdStrike

Remediate Threats Detected by Omnis Cyber Intelligence With CrowdStrike

HIGHLIGHTS

The Power of CrowdStrike

- **AI-Driven Detection and Response:** Utilizes advanced AI for real-time endpoint threat detection and response.
- **Comprehensive Endpoint Visibility:** Provides robust monitoring of endpoint behavior across systems to prevent malware, ransomware, and fileless attacks.
- **Centralized Threat Management:** Offers a unified platform for managing endpoint threats with automated forensics and streamlined incident response.

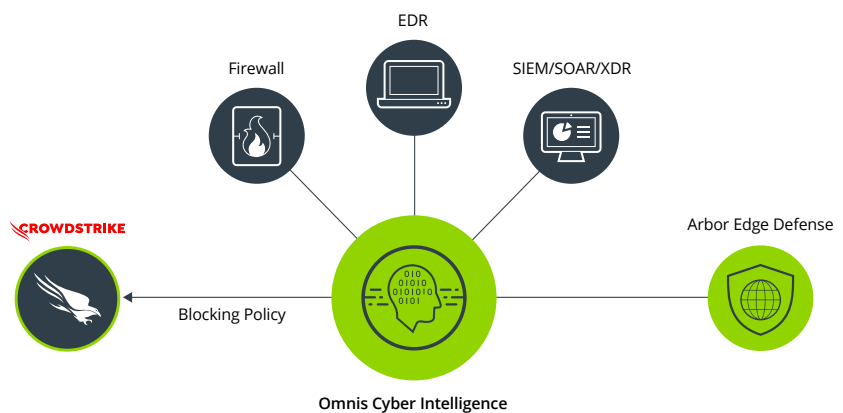
The Power of Omnis Cyber Intelligence

- **Network-Wide Visibility:** Extends packet-level insights across on-premises, virtual, and cloud environments.
- **Multi-Vector Threat Analytics:** Combines IoCs, behavioral analytics, and anomaly detection to uncover both known and zero-day threats.
- **Historical and Real-Time Analysis:** Facilitates proactive threat hunting and historical investigations with continuous packet capture and MITRE ATT&CK mappings.

The Power of Omnis Cyber Intelligence and CrowdStrike Integration

- **Seamless Ecosystem Integration:** Integrates with SIEM, SOAR, and XDR, allowing streamlined workflows and comprehensive security coverage across all vectors.
- **Unified Threat Intelligence:** Correlates endpoint and network data for richer threat insights and context.
- **Faster, Informed Responses:** Enables cross-domain alert investigation and response, enhancing SOC efficiency and reducing MTTR.

Faced with today's increasingly sophisticated cyber threats, organizations depend on integrated security platforms that offer unified network and endpoint visibility with coordinated threat mitigation. NETSCOUT's Omnis® Cyber Intelligence and Omnis® CyberStream deliver packet-level insights and threat analytics across networks, while CrowdStrike provides endpoint-focused threat intelligence and response capabilities. Together, they form a cohesive framework that enhances detection accuracy, shortens response times, and delivers a multi-layered defense against complex threats.



Omnis Cyber Intelligence Open Integration Architecture

Omnis Cyber Intelligence's Open Integration Architecture allows seamless alignment with existing security ecosystems, integrating with endpoint detection and response (EDR), SIEM, SOAR, XDR, and specifically with CrowdStrike, to enhance network and endpoint threat visibility.

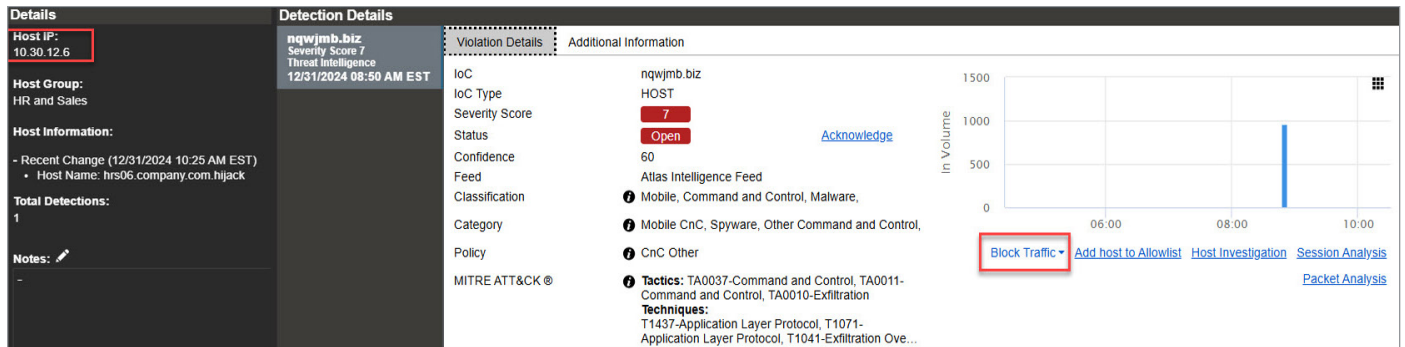
Overview of CrowdStrike Integration

The integration between NETSCOUT's Omnis Cyber Intelligence and CrowdStrike facilitates halting the progression of attacks during the investigation of suspected compromises by combining network-wide observability with precise endpoint control.

- **Detailed Investigation Support:** Omnis Cyber Intelligence provides visibility into all network traffic, enabling analysts to uncover the root cause of security incidents, assess the risk, and identify compromised data during an investigation.
- **Quarantine Functionality:** When malicious activity is detected, Omnis Cyber Intelligence's integration with CrowdStrike allows analysts to quarantine affected systems directly, halting the spread of attacks while the investigation proceeds.
- **Seamless Recovery:** Once the investigation is complete, systems can be easily un-quarantined as necessary, ensuring minimal disruption to operations.

Use Case

Today's threat landscape requires vigilance across both endpoints and networks. With Omnis Cyber Intelligence's DPI capabilities, threats are detected within the network and analyzed for anomalies. When Omnis Cyber Intelligence identifies an Indicator of Compromise (IoC), it uses the "Block Traffic" feature to send IoC-related information to CrowdStrike (e.g. IP address of internal compromised endpoint, IP address or domain of known bad external host). In turn, a SOC analyst can use CrowdStrike to quarantine the compromised endpoint and start other remediation efforts. The combination of network and endpoint perspectives streamlines threat hunting and enables comprehensive incident response, ensuring faster mitigation across the security stack.



Integrating Omnis Cyber Intelligence and CrowdStrike creates a multi-dimensional security solution that improves detection accuracy, expedites response actions, and enhances SOC efficiency. Together, Omnis Cyber Intelligence's network visibility and CrowdStrike's endpoint insights provide a resilient defense capable of adapting to advanced and persistent cyber threats.



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