Omnis Network Security

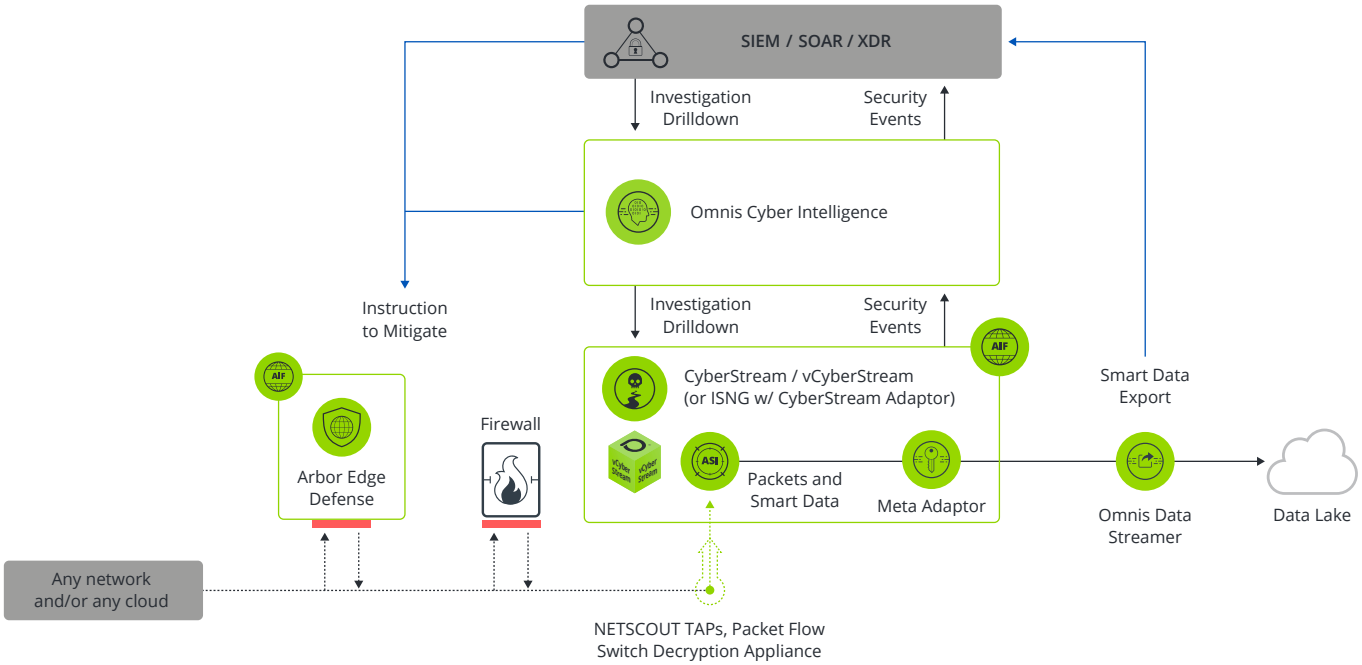
Modern-day enterprise networks are incredibly complex, encompassing a variety of components such as internal networks, branch offices, virtual environments, and public clouds. Unfortunately, this expands the threat landscape, resulting in a surge in cyber-attacks. To compound the issue, the proliferation of security tools has led to siloed data, making it difficult for organizations to gain a comprehensive and consistent understanding of their networks. This lack of visibility poses significant challenges for cybersecurity teams in swiftly detecting and responding to threats. To address this challenge, NETSCOUT offers the Omnis™ Network Security solution.

NETSCOUT has been a trusted provider of comprehensive network and application layer visibility for over three decades. NETSCOUT's expertise lies in offering organizations a clear network packet-level view of their entire digital infrastructure, regardless of its location (whether it's a legacy system, virtual environment, or hybrid cloud) and aptly terms this comprehensive visibility "Visibility without Borders." NETSCOUT firmly believes that achieving this level of visibility is a foundational requirement for effective threat detection and response, which provides "Security Without Borders." By implementing Omnis® Network Security, organizations can obtain the network visibility necessary to protect themselves from threats they can't afford to overlook.

Our portfolio of network-based cybersecurity solutions and products is designed to provide the scale, scope, and consistency required to secure today's digital infrastructure. With NETSCOUT Omnis Network Security, you can achieve "Security Without Borders", enabling your organization to stay one step ahead of cyber threats.

FEATURES AND BENEFITS

- Cost-effective and scalable network instrumentation ensures extensive network visibility while keeping expenses low.
- Multiple methods of network-based threat detection using, curated threat intelligence, ML based behavioral analysis, open source, and advanced analytics.
- Contextual investigations by leveraging locally stored metadata and packets.
- Remediation at the perimeter through the utilization of state-of-the-art stateless packet processing technology or compatible third-party blocking devices such as firewalls.
- Supports open standards, and offers APIs for seamless security ecosystem integration and enhanced collaboration between technology operations (TechOps) teams.



Our suite of powerful technologies includes:

CyberStream

Our network sensors use scalable Deep Packet Inspection (DPI) and multiple methods of threat detection to protect your entire digital infrastructure from cyber attacks. Long term, local storage of metadata and packets enable contextual network investigation or hunting.

Omnis Cyber Intelligence (OCI)

A central console that offers seamless management, visualization, and workflows for real-time and historical threat detection and investigation. OCI empowers you to stay proactive and respond effectively to security events.

Adaptive Service Intelligence (ASI)

Our patented technology that converts raw packets into a rich source of layer 2-7 metadata called Smart Data. ASI enhances your network's intelligence, enabling accurate and efficient threat detection.

ASI Flow

ASI Flow-based behavioral analysis to that uses ML to create deterministic signatures, resulting in fewer false positives. This allows for precise threat identification, minimizing unnecessary alerts and improving efficiency.

ATLAS Intelligence Feed (AIF)

A global threat intelligence feed covering over 50% of all internet traffic. AIF keeps you informed about emerging threats and provides valuable insights to bolster your security strategy.

nGenius Decryption Appliance (nDA)

Offering high-performance visibility into encrypted traffic, including TLS/SSL and SSH. With flexible deployment options, nDA ensures optimal performance of downstream service and security assurance tools.

Omnis Data Streamer (ODS)

Exporting patented ASI data to a data lake, ODS allows you to combine it with other data sources for custom analysis. Gain deeper insights into your network's security posture and make informed decisions.

Arbor Edge Defense (AED)

Acting as the first and last line of smart, automated perimeter defense in your network, AED blocks inbound DDoS attacks, cyber threats, and outbound Indicators of Compromise, providing robust protection for your organization.

Benefits

Comprehensive Network Security and Visibility

- At NETSCOUT, we understand the importance of comprehensive network security and visibility. That's why our CyberStream and vSTREAM platforms, powered by Adaptive Service Intelligence (ASI) technology, offer unparalleled Visibility without Borders. This level of visibility enables security without borders, ensuring your network remains protected across your entire digital infrastructure.

Multidimensional Hierarchical Detection

- Our multidimensional threat detection capabilities provide real-time security using targeted machine learning techniques. By utilizing IoCs, policies, signatures, unexpected traffic, and behavior analysis, we ensure comprehensive security coverage while minimizing false positives.

Investigation and Threat Hunting

- Omnis Cyber Intelligence can leverage CyberStream long term, local storage of network metadata and packets for historical investigation and proactive threat hunting to gather evidence of cyber threats.

Security Ecosystem Integration

- Integration is key in today's complex cybersecurity landscape. Our Omnis Network Security solution seamlessly integrates with other cybersecurity tools, including SIEM, EDR, SOAR, and XDR systems. With tri-directional integration, we enhance workflows, collaboration, and response times, enabling faster incident detection and response. Additionally, Omnis Data Streamer enables our patented Smart Data can be exported into any third-party data lake for further analysis and correlation.

Smart Edge Protection

- Detection is not enough. After a threat has been detected and confirmed with Omnis Cyber Intelligence, it can issue a blocking policy in a network edge devices such as a firewall or our own Arbor Edge Defense to stop the threat before further impact occurs.

Choose NETSCOUT Omnis Network Security for comprehensive, scalable, and consistent protection that secures your digital infrastructure in today's ever-evolving threat landscape.

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

SECSB_036_EN-2302 08/2023