

# NETSCOUT Cyber Investigator

## Cyber Threat Investigation Platform

### HIGHLIGHTS

#### Smart Instrumentation

Leveraging highly scalable (1–100 Gbps packet capture rates and up to 128TB of local metadata and packet storage) CyberStream instrumentation available as COTS and virtual form factors. NETSCOUT® Cyber Investigator (NCI) gains pervasive visibility across an organization's entire network, including hybrid cloud environments.

#### Smart Data

In real time and local to instrumentation, NETSCOUT's patented Adaptive Service Intelligence™ (ASI) technology and ATLAS® Threat Intelligence add context, analytics and threat intelligence, turning massive amounts of wire data into actionable insights for efficient cyber threat detection and investigation.

#### Smart Investigation

An intelligent and efficient meta-data and packet retrieval system, along with a dynamic, flexible UI, enable guided contextual or ad hoc unguided investigations to determine extent of breach and remediation.

#### Integration

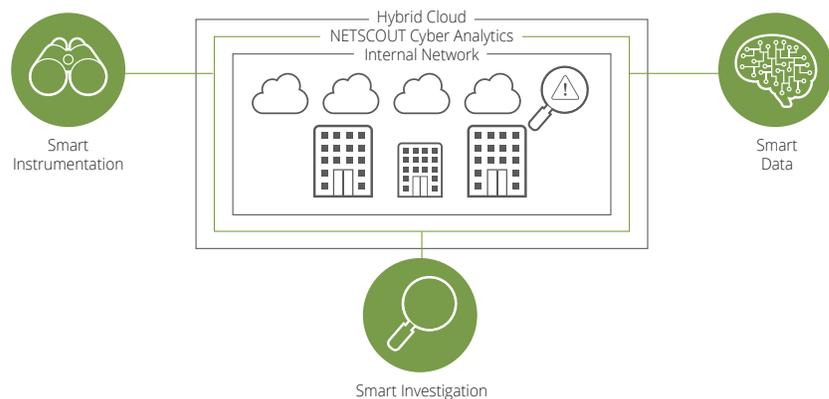
Support for Syslog, STIX/TAXII, and a documented API enable NCI to easily integrate into an existing security stack.

#### NetOps and SecOps Collaboration

Support for NETSCOUT InfiniStreamNG®, vSTREAM™ and nGeniusONE® deployments allow NCI to be used by both NetOps and SecOps teams to efficiently detect and investigate cyber threats.

### Product Overview

NETSCOUT Cyber Investigator (NCI) is an enterprise-wide network threat and risk investigation solution that helps reduce the impact of cyber threats on your business. It serves as an early warning system with the ability to promptly and efficiently detect, validate, investigate, and respond to cyber threats. Organizations will benefit from having this cost-effective and highly scalable cyber threat analytics system at their fingertips which can also easily integrate with popular SIEM platforms used by many corporations.



### ASI Technology

Leveraging multi-form-factor, scalable and intelligent CyberStream instrumentation, NETSCOUT Cyber Investigator provides pervasive visibility across an organization's entire network. Whether in an internal corporate network, remote office locations, public, private or hybrid cloud environments; NCI provides pervasive, end-to-end visibility — the foundational requirement for effective cyber security.

### Anywhere, Everywhere Visibility

As CyberStream instrumentation monitors network traffic in real time, it automatically enhances metadata and packets with NETSCOUT's patented Adaptive Service Intelligence (ASI) technology and Active Threat Level Analysis System (ATLAS) global threat intelligence—turning it into “smart data”. Adding this level of context, real-time analytics and threat intelligence turns massive amounts of wire-derived data into actionable insights for efficient cyber threat detection and investigation.

Armed with the pervasive visibility and smart data from CyberStream instrumentation, security teams can seamlessly utilize existing security tools (i.e. SIEM systems) to conduct powerful, guided or unguided investigations using NCI's advanced indexing and retrieval technology combined with an intuitive, dynamic and flexible user interface.

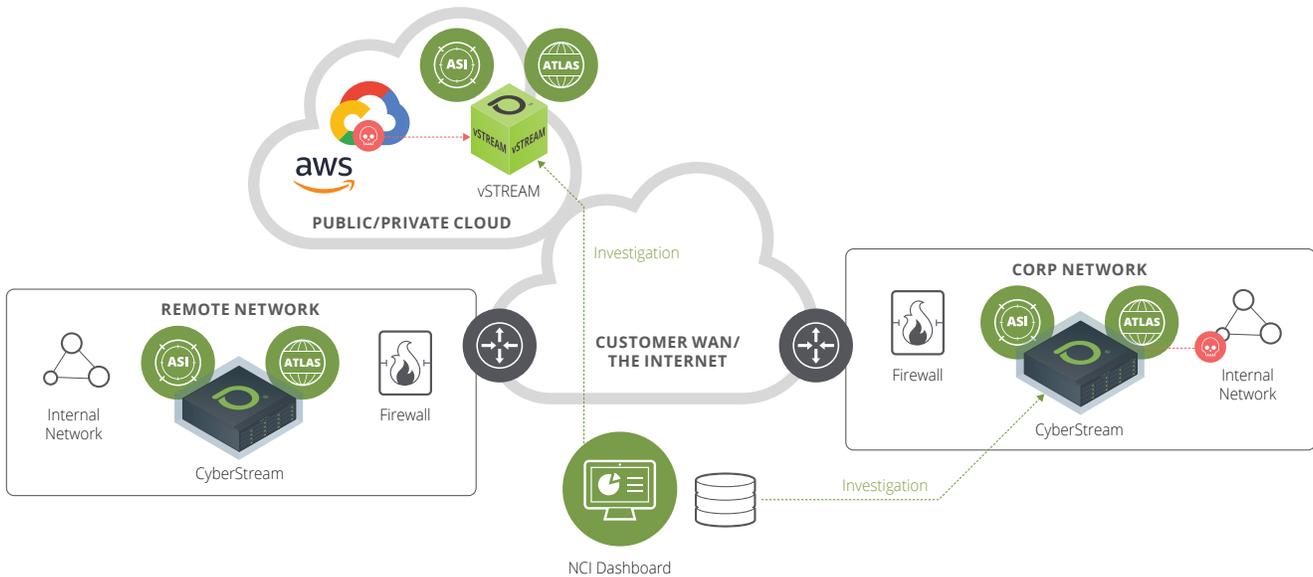


Figure 1: NCI deployment.

The benefits of NETSCOUT Cyber Investigator include:

- Pervasive network visibility, including in hybrid-cloud environments — the foundational requirement for effective cyber security.
- Efficient cyber threat investigation improves cyber security team productivity

### Security Starts With Pervasive Visibility From CyberStream Smart Instrumentation

A foundational requirement for cyber security is pervasive visibility. As modern-day networks include microservice, containerized applications in highly distributed and hybrid-cloud-based environments, gaining proper visibility has become increasingly difficult. NETSCOUT Cyber Investigator leverages highly scalable, multi-form-factor CyberStream instrumentation to gain pervasive visibility across an organization's entire network, including hybrid-cloud environments.

Highlights of CyberStream instrumentation:

- Multiple form factors including COTS and virtual.
- Virtual CyberStream is ideal for monitoring service-critical traffic running within virtualized or cloud infrastructures where it provides visibility into a single VM or VM-to-VM communications.
- Full packet-capture rates of 1, 10, 40, and 100 Gbps; 6TB to 128TB of metadata and packets are stored on CyberStream instrumentation—meaning it is not forwarded to an external cloud, saving on egress costs and meeting compliance requirements.
- Built-in deduplication and compression mechanisms streamline data accumulation for more efficient processing and judicious storage of packets.
- Optionally, data can be exported to internal data lakes for long-term historical analysis.
- For existing NETSCOUT customers, NCI can also leverage InfiniStreamNG and vSTREAM instrumentation.

### Turning Pervasive Visibility Into Smart Data

Gaining pervasive visibility is only the beginning. Adding contextual, real-time analytics and threat intelligence turns massive amounts of wire data into actionable insights for efficient cyber threat detection and investigation.

As CyberStream instrumentation monitors network traffic, it automatically enhances wire-based metadata and packets with NETSCOUT's patented Adaptive Service Intelligence (ASI) technology turning it into "smart data".

### ASI Smart Data

- Provides contextual views into network, service and application performance for both control and user planes.
- Exposes key traffic/performance indicators and Layer 4-7 problem indicators for network, applications and servers.
- Derives per-connection metadata such as URLs, Browser-OS-Device, DNS requests, login attempts, SIP User and Signaling, SSL certificate expiry/not-before detection, Credit Card Account, Merchant ID, Trading CompID, Order ID, Symbol and UC MOS and Call Stats.

### Adding Threat Intelligence to ASI Smart Data

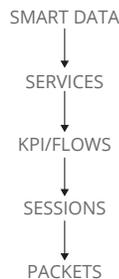
With visibility into 1/3 of the Internet, NETSCOUT Active Threat Level Analysis System (ATLAS) collects, analyzes, prioritizes and disseminates data on emerging threats.

NETSCOUT's ATLAS Security and Engineering Research Team (ASERT) researches malware campaigns and botnets at a global level, providing much-needed context to the overall cyber threat environment.

Highly curated threat intelligence is automatically and at no charge disseminated to NETSCOUT Cyber Investigator customers via the ATLAS Threat Intelligence Feed (AIF), giving it the ability to detect wire-based threats in real time.

### Net/SecOps Collaboration Improves Security

NETSCOUT ASI-enhanced smart data is a common source of data that can be shared with Net/IT/Dev and SecOps teams for network service assurance and security use cases—saving costs, improving efficiency, and reducing to the time to investigate and remediate threats and prevent losses.



### ASI Technology



ASI technology transforms wire traffic into smart data, providing real-time visibility into user experience for the most advanced and adaptable information platform to ensure security, manage risk, and drive service performance.



Figure 2: Main screen of NETSCOUT Cyber Investigator.

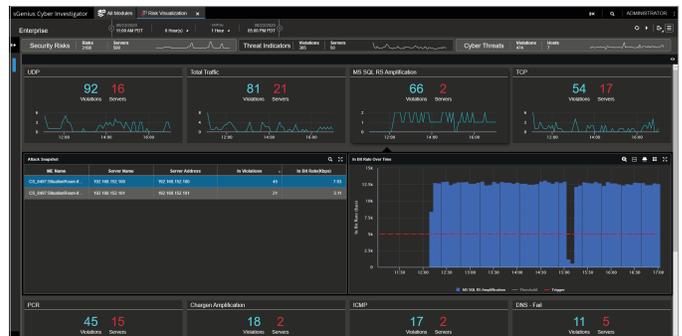


Figure 3: Dashboard exposes risks and other cyber threats.

## Smart Investigation Becomes Part of Security Stack

It's becoming increasingly more difficult for cyber security teams to rely solely upon log-based data for cyber threat detection, investigation and remediation. Security teams realize that wire-based metadata and packets contain the ultimate source of truth. Together, NETSCOUT CyberStream and NETSCOUT Cyber Investigator can be used to conduct powerful contextual guided or unguided investigations.

- Using a powerful indexing mechanism and a dynamic UI, NCI can be used by cyber security teams to conduct guided or unguided investigations:
  - Host Investigations provide visibility in critical and questionable host interactions—both internal and external.
  - Network Investigations provide visibility into server, applications and conversations.
  - All investigations included associated session data and full packets.
- Segregated packet stores for critical and normal data, along with centralized packet indexing, enable fast retrieval and analysis of data.
- Plug and Play launch from major SIEM vendors allow cyber security teams to easily execute guided, contextual investigations from third-party alerts to session data and ultimately packets.
- Support for Syslog, STIX/TAXI for third-party IoC ingestion and ASI-enhanced metadata and packets that can be exported to external data lakes enable NCI to become an integral part of an existing security stack and process.

## Flexible and Scalable Packaging

The NETSCOUT Cyber Investigator is capable of scalability via the nGenius Dedicated Global Manager and the Standby Server. These are optional licenses which can be used to expand your NCI deployment for even more scalability or high availability.

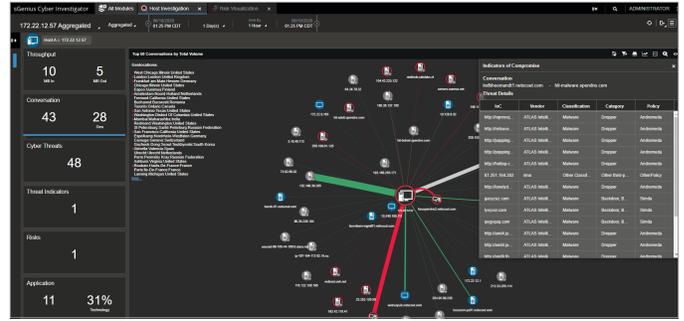


Figure 4: Host investigation with NCI.

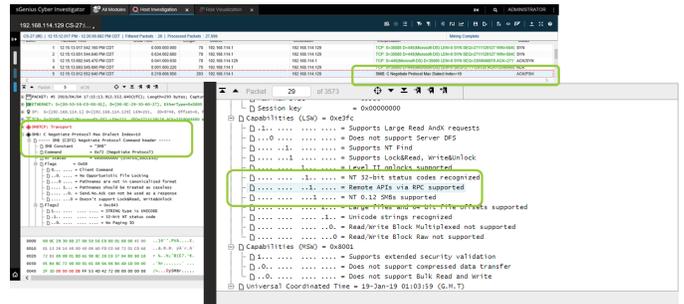


Figure 5: Session and packet view for threat investigation.

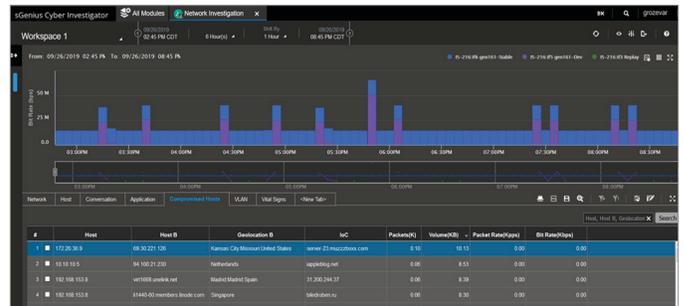


Figure 6: Network investigation with NCI.

Product Type Category	Product SKU	Short Description
Software	91D10L	sGenius Cyber Investigator - Entry (5) - Software - (Linux)
Appliance	51D41L	sGenius Cyber Investigator - Workgroup (10) - Standard Appliance
Appliance	51DH1L	sGenius Cyber Investigator - Intermediate (25) - Standard Appliance
Appliance	51D51L	sGenius Cyber Investigator - Full (50) - Standard Appliance
Appliance	51D21L	sGenius Cyber Investigator - Full (50) - Standby Appliance
Software	91D40L	sGenius Cyber Investigator - Workgroup (10) - Software - (Linux)
Software	91DH0L	sGenius Cyber Investigator - Intermediate (25) - Software - (Linux)
Software	91D700	sGenius Cyber Investigator - Incremental (50) - Software - (Linux)
Software	91D20L	sGenius Cyber Investigator - Full (50) - Standby Software - (Linux)
Software	91D50L	sGenius Cyber Investigator - Full (50) - Software - (Linux)
Software	91DK00	sGenius Cyber Investigator - Intermediate (25) License Upgrade to Full (50)
Software	91DU00	sGenius Cyber Investigator - Workgroup (10) License Upgrade to Full (50)
Software	91D50L-E	sGenius Cyber Investigator - Full (50) - Software - (Linux) - Evaluation
Software	51DD1L	sGenius Cyber Investigator - Dedicated Global Manager – Appliance
Software	91DD0L	sGenius Cyber Investigator - Dedicated Global Manager - Software - (Linux)

**Table 1: Ordering information.**

\* Please consult with your NETSCOUT Sales Professional to determine system requirements suited for deployment in your environment



**Corporate Headquarters**  
 NETSCOUT Systems, Inc.  
 Westford, MA 01886-4105  
 Phone: +1 978-614-4000  
[www.netscout.com](http://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](http://www.netscout.com/company/contact-us)