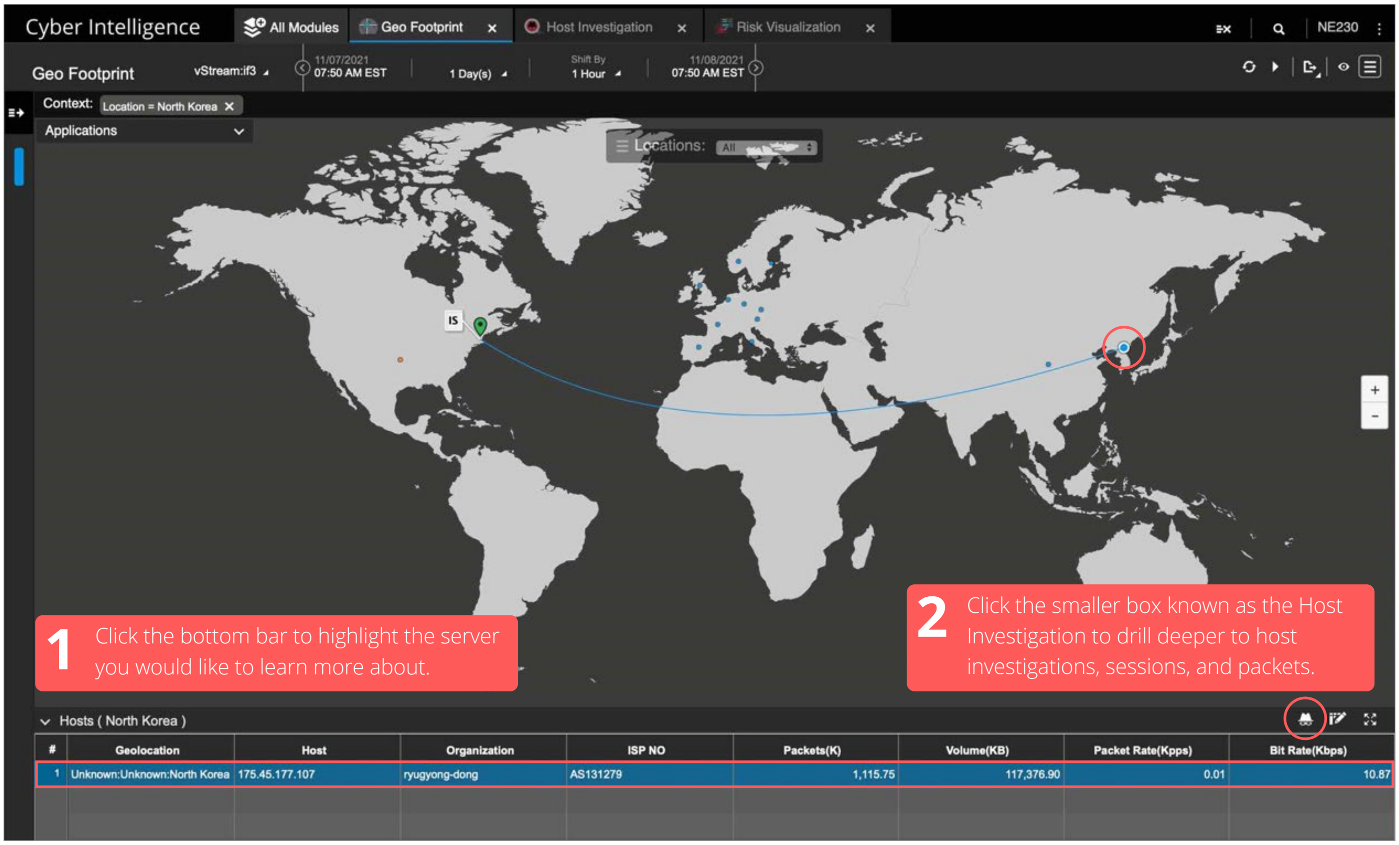
Early Warning Detection

Having the ability for continuous, real time attack surface monitoring allows you the ability to detect questionable behavior and act as your early warning system. As we have come to learn about cybersecurity, its not a matter of if we get attacked but when we get attacked. 100% security is not feasible, and we need to evolve our strategy to also include detection, the earlier the better. Studies show that if you can detect a potential breach in the earlier phases you can drastically reduce the impact and even sometimes stop a threat from ever occurring.

Cyber criminals do their research before executing an attack, hackers need to know what's available to attack before launching any intrusion. Network reconnaissance is analogous to a bank robber casing a bank to find out how many security guards are on duty, how many cameras exist, their placement, and what escape route to use.

Unlike endpoint data, bad actors cannot manipulate network packet data. Network packet-derived data is the ultimate source of intelligence for gaining comprehensive (e.g., broad and deep) network visibility and conducting more effective cyber threat detection and response.

NETSCOUT® Omnis® Cyber Intelligence (OCI) is an advanced NDR solution that integrates with and fills the gaps left by other security tools. NETSCOUT's OCI leverages NETSCOUT CyberStream instrumentation to capture full packets at line rate (e.g., up to 100Gbps). Cyberteams' patented Adaptive Service Intelligence® (ASI) technology automatically extracts a unique, robust set of layer 3- 7 metadata from packets (we call Smart Data). With this Smart Data, security analysts can use NETSCOUT OCI to conduct highly responsive, real-time, and historical analyses to detect and investigate threats quicker. Omnis Cyber Intelligence (OCI) is all about providing a credible network data source to detect the earliest phases of an attack to get ahead of it. Quickly identifying reconnaissance, customers can prepare their environment to block reconnaissance and prepare their defenses in advance of a future attack. NETSCOUT OCI reconnaissance sees evidence of a wide variety of port scanning, obfuscation and brute force attempts at all of our customer deployments, including Telnet Brute Force, Malware Hosts, Tor Exit Nodes, Worms, ASERT Sinkhole activity, etc



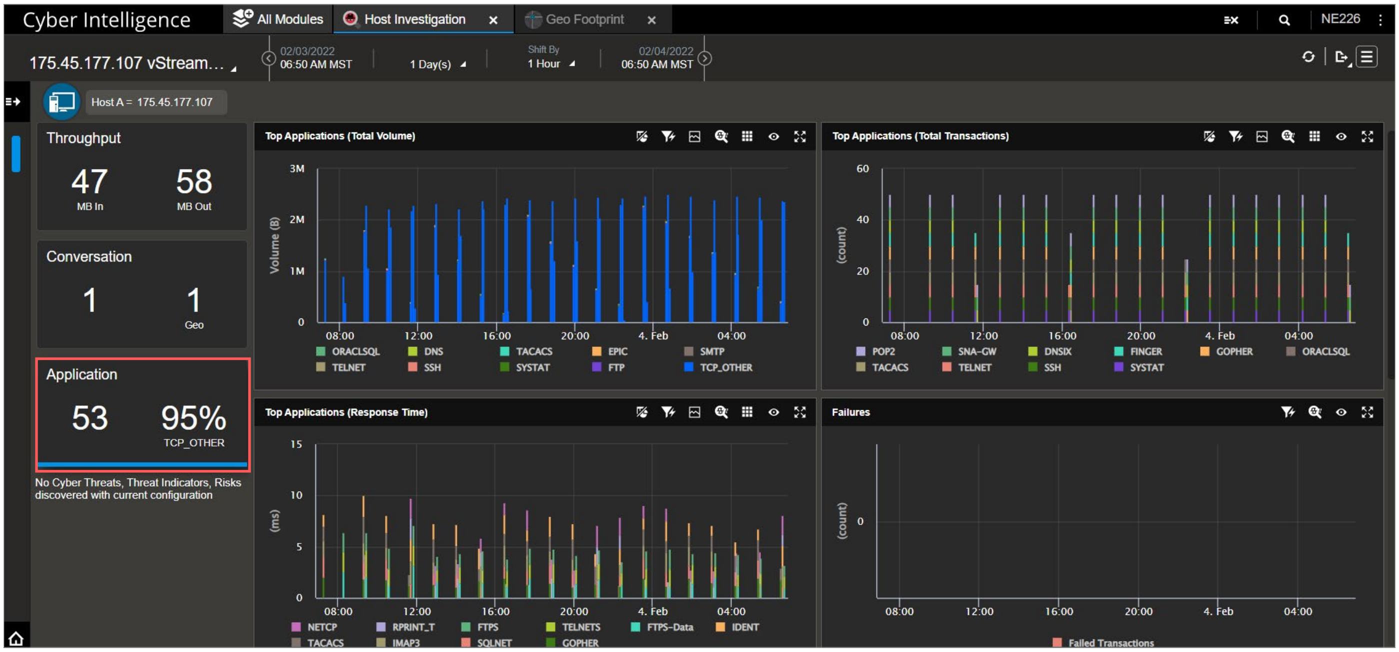
1 Click the bottom bar to highlight the server you would like to learn more about.

2 Click the smaller box known as the Host Investigation to drill deeper to host investigations, sessions, and packets.

Hosts (North Korea)

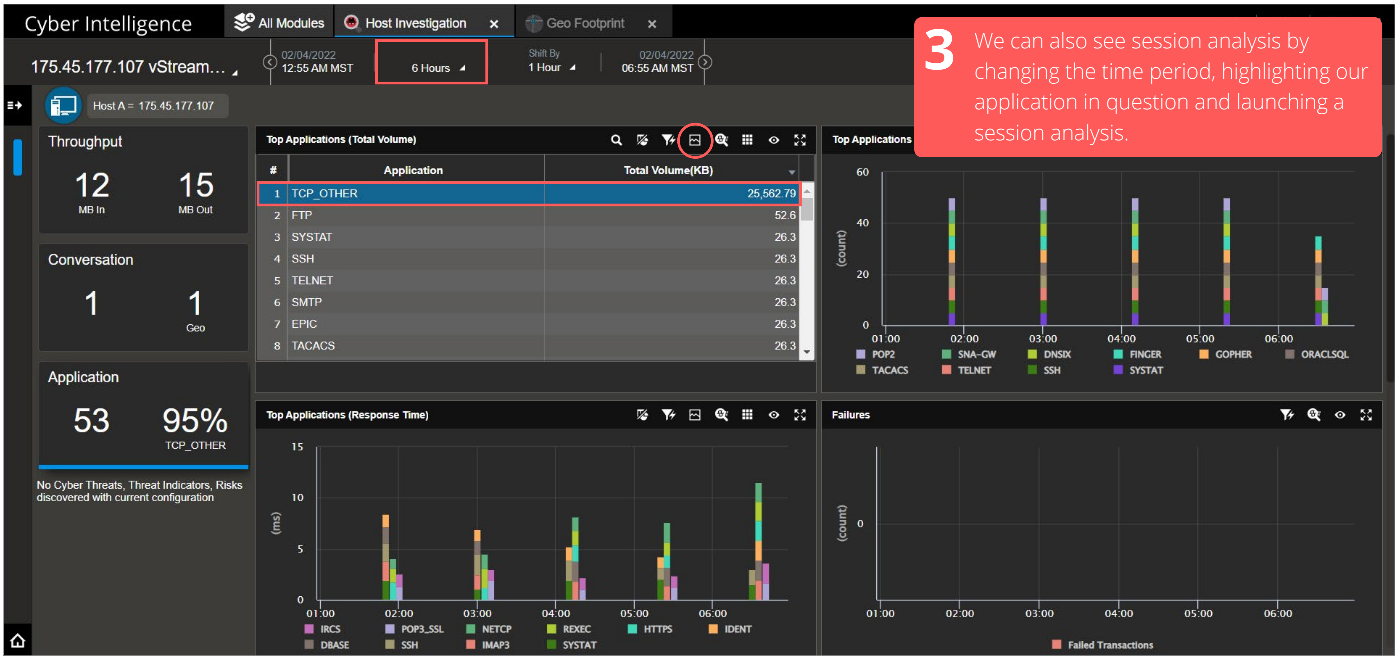
#	Geolocation	Host	Organization	ISP NO	Packets(K)	Volume(KB)	Packet Rate(Kpps)	Bit Rate(Kbps)
1	Unknown:Unknown:North Korea	175.45.177.107	ryugyong-dong	AS131279	1,115.75	117,376.90	0.01	10.87

One good example is a company using the Geo footprint feature and noticing a North Korean IP address sending traffic to the user's web server. This is especially rare because this company has no business in that region of the world.



No Cyber Threats, Threat Indicators, Risks discovered with current configuration

As you can see there are over 50 applications which also doesn't make sense for the web server. We also see the applications throughput rates are low with spikey traffic behavior. These spike rates show similar volume, which is likely reconnaissance and not "real" traffic.

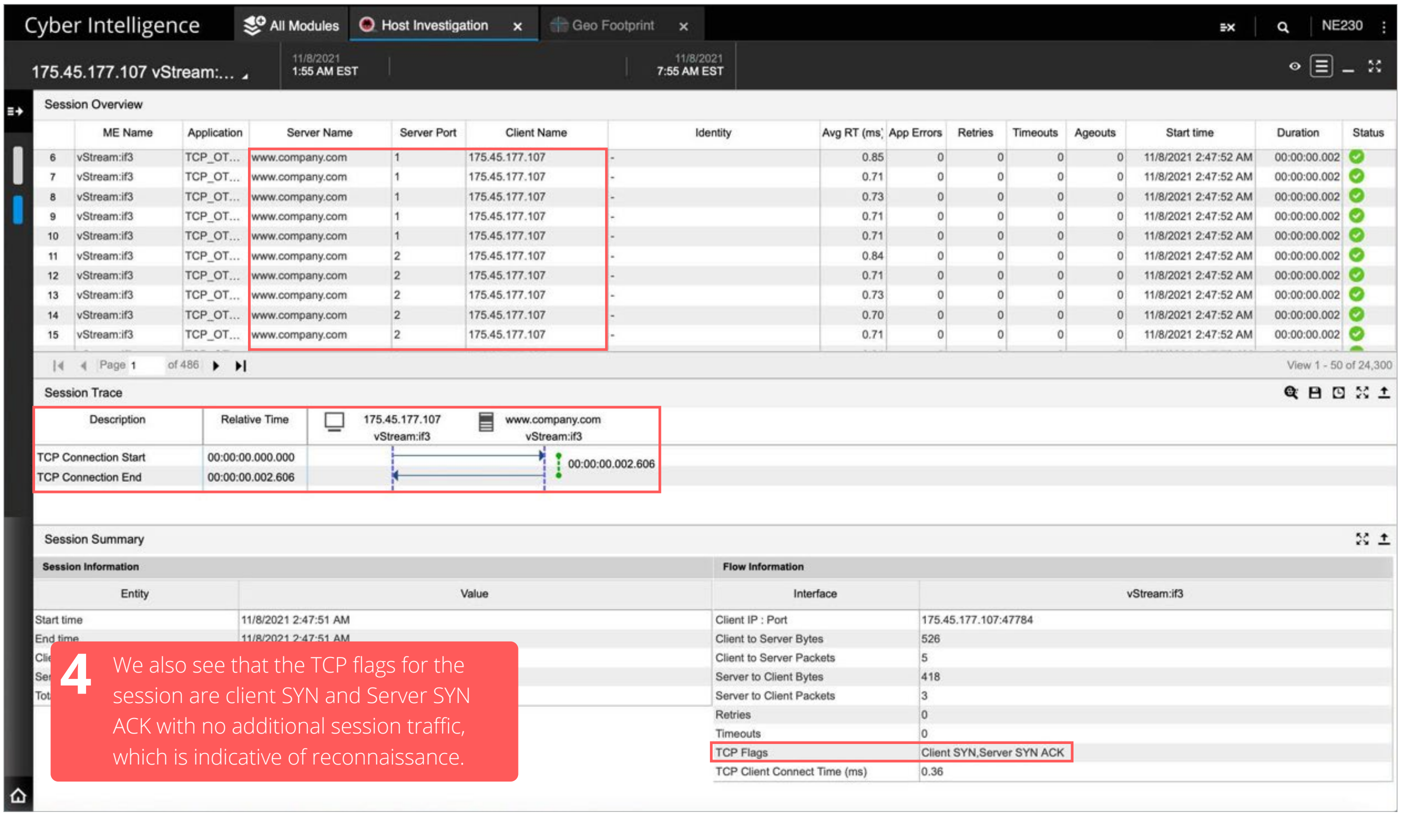


No Cyber Threats, Threat Indicators, Risks discovered with current configuration

Top Applications (Total Volume)

#	Application	Total Volume(KB)
1	TCP_OTHER	25,562.79
2	FTP	52.6
3	SYSTAT	26.3
4	SSH	26.3
5	TELNET	26.3
6	SMTP	26.3
7	EPIC	26.3
8	TACACS	26.3

3 We can also see session analysis by changing the time period, highlighting our application in question and launching a session analysis.



Session Overview

	ME Name	Application	Server Name	Server Port	Client Name	Identity	Avg RT (ms)	App Errors	Retries	Timeouts	Ageouts	Start time	Duration	Status
6	vStream:if3	TCP_OT...	www.company.com	1	175.45.177.107	-	0.85	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
7	vStream:if3	TCP_OT...	www.company.com	1	175.45.177.107	-	0.71	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
8	vStream:if3	TCP_OT...	www.company.com	1	175.45.177.107	-	0.73	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
9	vStream:if3	TCP_OT...	www.company.com	1	175.45.177.107	-	0.71	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
10	vStream:if3	TCP_OT...	www.company.com	1	175.45.177.107	-	0.71	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
11	vStream:if3	TCP_OT...	www.company.com	2	175.45.177.107	-	0.84	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
12	vStream:if3	TCP_OT...	www.company.com	2	175.45.177.107	-	0.71	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
13	vStream:if3	TCP_OT...	www.company.com	2	175.45.177.107	-	0.73	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
14	vStream:if3	TCP_OT...	www.company.com	2	175.45.177.107	-	0.70	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓
15	vStream:if3	TCP_OT...	www.company.com	2	175.45.177.107	-	0.71	0	0	0	0	11/8/2021 2:47:52 AM	00:00:00.002	✓

Page 1 of 486

View 1 - 50 of 24,300

Session Trace

Description	Relative Time	175.45.177.107 vStream:if3	www.company.com vStream:if3
TCP Connection Start	00:00:00.000.000		00:00:00.002.606
TCP Connection End	00:00:00.002.606		

Session Summary

Session Information

Entity	Value
Start time	11/8/2021 2:47:51 AM
End time	11/8/2021 2:47:51 AM
Cli	
Ser	
Tot	

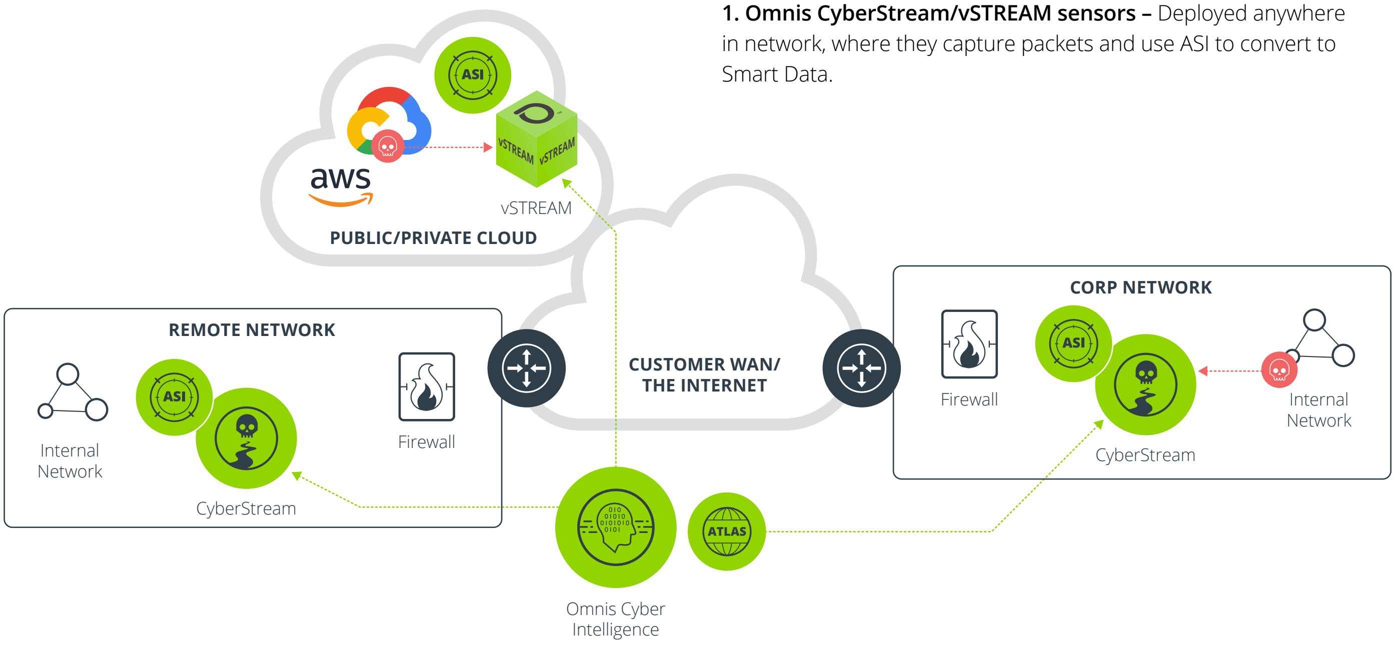
Flow Information

Interface	vStream:if3
Client IP : Port	175.45.177.107:47784
Client to Server Bytes	526
Client to Server Packets	5
Server to Client Bytes	418
Server to Client Packets	3
Retries	0
Timeouts	0
TCP Flags	Client SYN,Server SYN ACK
TCP Client Connect Time (ms)	0.36

4 We also see that the TCP flags for the session are client SYN and Server SYN ACK with no additional session traffic, which is indicative of reconnaissance.

Scrolling through Sessions in the Overview we see that the client is sequentially hitting many low port numbers on the “www.company.com” server, including port 1.

Having this granular visibility within a matter of a few clicks allows you to see questionable activity and act on it if need be. According to NETSCOUT customer deployments, OCI detects more than 50% of previously unknown outbound threats and 95% of otherwise undetected reconnaissance. This company is now able to recognize reconnaissance and block communication before a threat could occur.



1. Omnis CyberStream/vSTREAM sensors – Deployed anywhere in network, where they capture packets and use ASI to convert to Smart Data.

2. Omnis Cyber Intelligence – The central console that analyzes CyberStream/vSTREAM Smart Data; uses behavioral analysis and ATLAS/3rd party intelligence, for threat detection and highly contextual investigation.

Summary

With NETSCOUT OCI, CyberStream instrumentation and patented ASI technology you can quickly identify reconnaissance, look back in time within minutes through a detailed history of both good and nefarious activity and contact trace where the network traffic came from.

No one knows the network better than NETSCOUT. No one has a more scalable, robust, and intelligent source of network packet-derived data than NETSCOUT. Smarter Data = Better Network Detection and Response.

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