# The Benefits of NetFlow in Network Traffic Analysis

## How Netflow Works

There is a vast and growing array of network monitoring tools and software out there. New software, tools, and utilities are launching almost every year to compete in an ever-changing marketplace of technology monitoring. These new tools reinforce some of the most needed features, such as more granular and in-depth traffic data and better views of bandwidth usage.

One such aid to these needs is NetFlow, a protocol that collects and records all active IP network traffic going to and from a router or switch that is Netflow enabled. The protocol allows you to drill down into your network traffic to see where the traffic source is coming from and its destination, which can greatly aid in troubleshooting slow LAN or WAN network connections.

The protocol was conceived at Cisco Systems and is part of the Internet Engineering Task Force (IETF) standard. It is now a significant standard widely implemented by other network equipment vendors and included in almost every business-grade router and switch that manufacturers produce.

Before Netflow, SNMP was used for network monitoring and analysis, but SNMP didn't provide in-depth insight into bandwidth use that was needed. With NetFlow, data such as the traffic's point of origin, destination, and traffic paths on the network, class of service, and the causes of congestion can be determined. Netflow is used for finding bandwidth hogs, hunting down network threats, isolating application slowness issues, and even for usage-based billing by some ISP'

## How Does NetFlow Work?

NetFlow follows a simple process of traffic collecting, sorting, and analysis. The central monitoring setup consists of three functional components; a NetFlow Exporter for tracking and exporting the data, a Netflow Collector for receiving, pre-processing and storing the flow data, and a NetFlow Analyzer that processes the data for traffic analysis and presentation in an easy-to-understand format. Let's look at each component in more detail.

## NetFlow Exporter

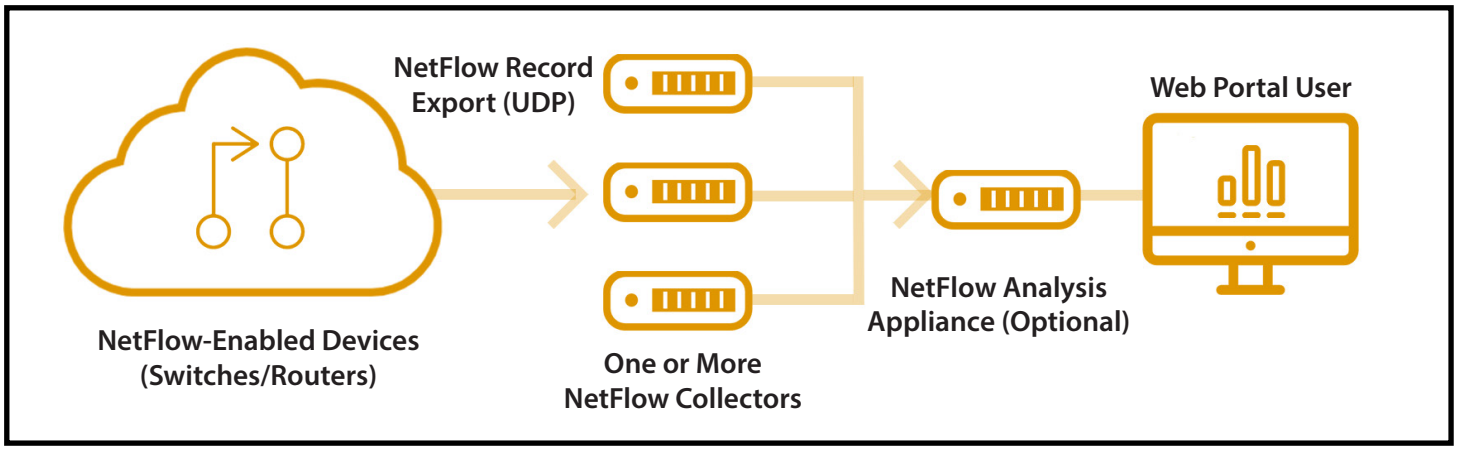
This can be a NetFlow-enabled router or switch that tracks key statistics and other information about IP packet flows and generates flow records that are sent to a flow collector. As data is forwarded through a router or switch, it is examined for a specific set of IP packet attributes. These packets are then tallied, and those with the same IP attributes are grouped into what's called a "Flow". The IP Flow is made up of five to seven attributes:

- **IP source address**
- **IP destination address**
- **Source port**
- **Destination port**
- **Layer 3 protocol type**
- **Class of Service**
- **Router or switch interface**

The Flow Records are then exported from the router towards one or more flow collectors.

## NetFlow Collector

The NetFlow collector is an application that receives the flow record packets. The Collector will continuously analyze and archive the flows for future reference and organize the flow records into a format that network engineers use to further analyze for source, destination, and other attributes. The Collector provides details on things like threats detected, network topology, and top interfaces. Collectors can be hardware-based collectors or software-based collectors, with software solutions being more common than hardware devices.




## A NetFlow Collector's primary functions include:

- **Receiving flow from the NetFlow-enabled device**
- **Unpacking the binary data into text or numeric formats**
- **Reducing data volume by filtering and aggregation**
- **Storing the resulting data in flat files or SQL database**
- **Sending the flow data to the NetFlow Analyzer application**

The NetFlow Collector and the third component, the Netflow Analyzer application, are two functions of a NetFlow system. NetFlow runs both functions on the same server when the volume of flow data from the exporter is low and localized. When flow data is high, or sources are geographically dispersed, the collector and analyzer functions run on separate and geographically-distributed servers. In these cases, collectors synchronize the data to a centralized analyzer server.

## The NetFlow Analyzer

The NetFlow analyzer, whether implemented with the Collector or as a separate application on another server, is a software analysis application that captures data from continuous streams of network traffic. It performs the necessary traffic analysis, converts the raw numbers, and then breaks the analysis down into an easily digestible format.

The analyzer provides visualizations such as tables and graphs to enable network operators and engineers to analyze the flow data that's coming from the flow collector, and determine precisely how the network is being used, by whom, and for what purpose. Monitoring this information helps network engineers discover certain traffic patterns, see the network bandwidth performance, and find the users, devices, and applications that are consuming the most network bandwidth.

## Insights Gained from the NetFlow Analyzer

A NetFlow analyzer can provide insights from the incoming flow data such as:

- **Flow record data across the flow-monitored systems**
- **Traffic flows by specific protocol, application, domain, ports, and IPs.**
- **Top talkers, IP addresses, and independent systems**
- **Sources and destinations by geographical location**
- **Which users, applications, and protocols are using the most bandwidth**
- **Protocols that are heavily used over the network**
- **Which endpoints attacks are originating from**
- **Who on the network is using forbidden applications**

## Why Use NetFlow: Key Applications of NetFlow

Network analysis tools can assist with various tasks, from troubleshooting and monitoring network availability, to detecting spyware and unauthorized, potentially malicious activity. Software applications with network analyzer functions are also used to locate applications that create bandwidth bottlenecks and can even help determine which parts of the network have been targeted by a DDoS attack—and the source of the attack.

Businesses and users can use flow analysis to visualize traffic patterns for the entire network. With this overall view of traffic flow, network operations and security operations teams can monitor when and how frequently users access an application in the network, and then profile the use of network and application resources to detect any potential security violations.

### Bandwidth Utilization

NetFlow data allows network admins to view a complete report on traffic flows by specific devices, specific protocols, and specific applications, to understand where bandwidth is getting consumed. By identifying the top talkers, network admins can see who the top consumers of bandwidth are and validate if that is relevant traffic.

### Network Visibility

NetFlow provides complete visibility into the network. Users can specify the traffic sections to monitor based on the tracks sent by NetFlow data. For instance, classifying Internet traffic by ports or protocol used gives network admins the ability to view the bandwidth usage by source and destination. From the NetFlow data, network admins can correlate IP addresses with users who accessed them. This can help prevent exposure of the network to a risk of malware, and provide a clear view of IP addresses users communicated with and which applications they accessed.

### Troubleshooting

NetFlow monitoring aids troubleshooting analytics. When a user complains that email is slow, it could be a problem in the mail server, a capacity issue with the user's mailbox, or even a problem in dropped packets over the wire. By analyzing the flow records, network admins can see if there are any packet drops or response time issues causing emails or any application access to be slow. This helps with determining if the network was the cause of application performance slowdown.

## Security Awareness

Network security is another key benefit of NetFlow. By monitoring NetFlow data, it's simple to understand where the most network resources are being used. Most security attacks consume resources, so if any spikes occur in a particular time or location, security teams can detect these changes in network behavior and identify and investigate for a security breach. The data is also a valuable forensic tool to replay the history of security incidents so security teams can learn from them.

For an example of the type of information that can be gathered and presented from a NetFlow collector application, see the Appendix that follows.

## Final Thoughts

NetFlow was developed in 1996 to reduce the amount of information collected from a network communication by aggregating packets with the same IP addresses, transport ports, and protocol into a compact record. NetFlow is even more relevant today, when the prevailing wisdom is that more data is always better. With no end in sight to the number of devices connecting to the Internet, networks are growing larger and faster than ever before, and NetFlow will continue to play a vital role in the future of network security and analysis.

## Additional Resources

Read the **NetVizion Product Sheet**

Visit the **Website**

Request a **Live Demo**

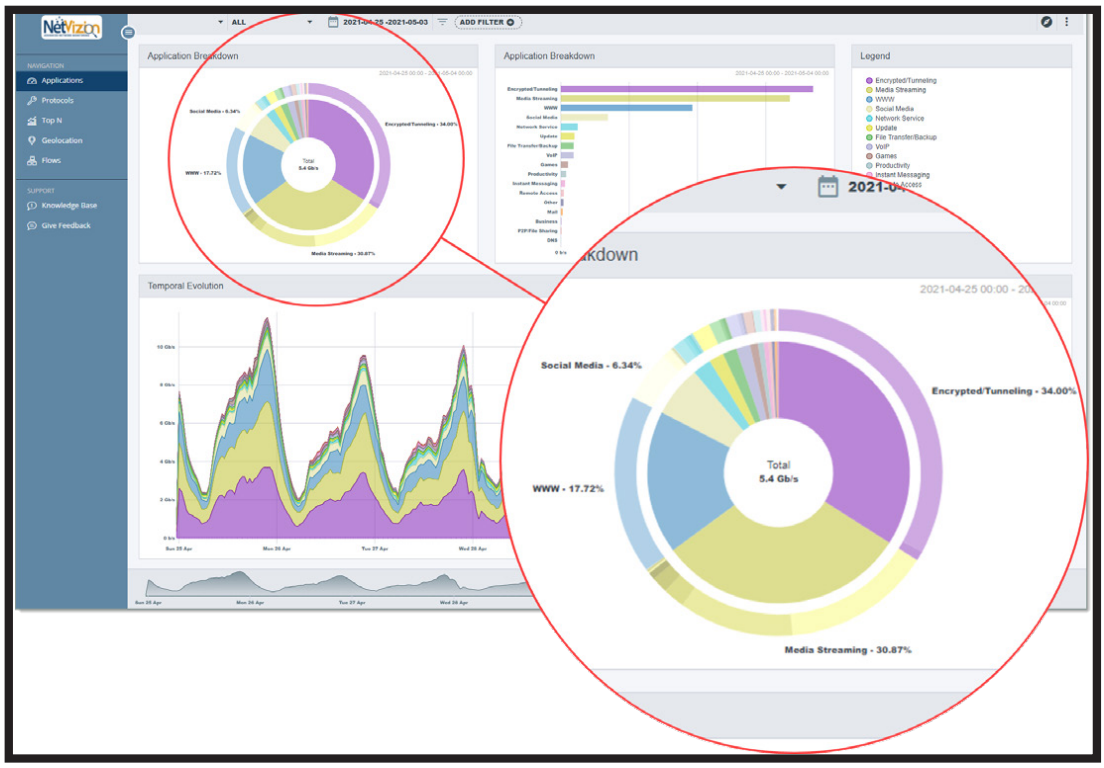
ZCorum™

NetVizion

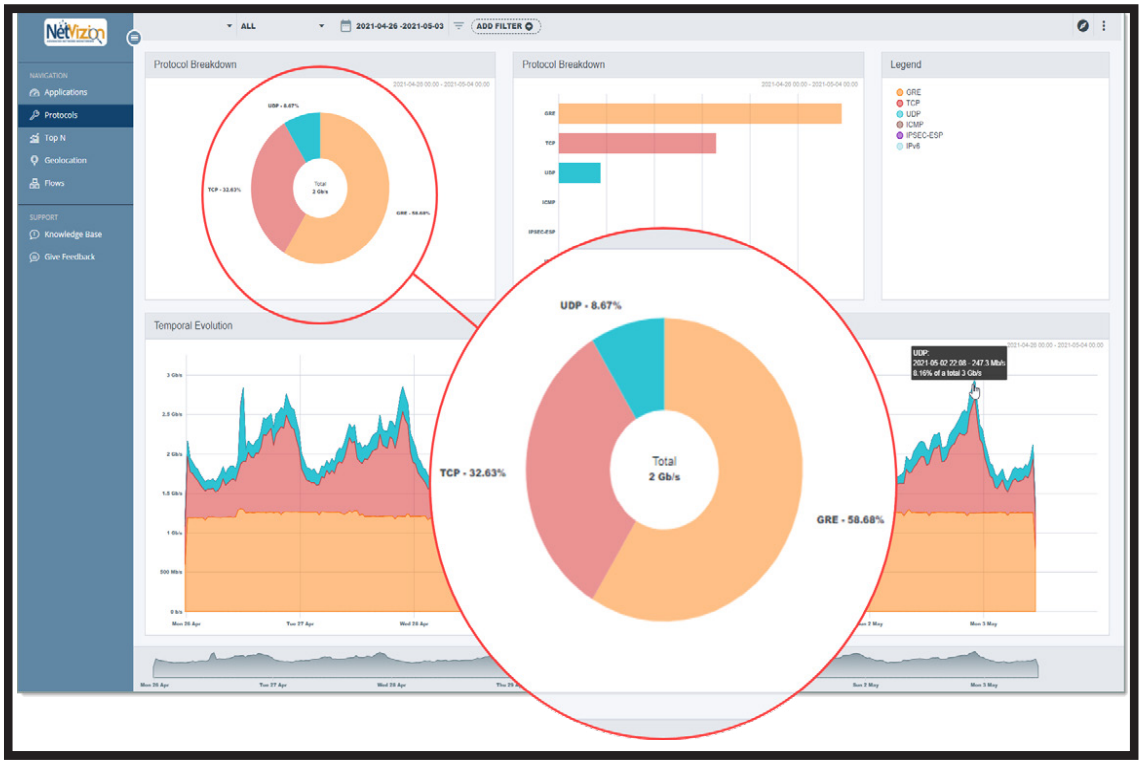
ZCorum provides a suite of products and services that help broadband operators increase operational efficiency and reduce costs, while improving subscriber experience. This is achieved through ZCorum's diagnostics solutions for DOCSIS and Fiber networks, plus managed services that include data and VoIP provisioning, residential and commercial VoIP service, IPTV service with programming included, branded email and Web hosting, along with 24x7 support for end-users. ZCorum is headquartered in Alpharetta, GA. For more information, please visit ZCorum.com. please visit **ZCorum.com.**

# Appendix

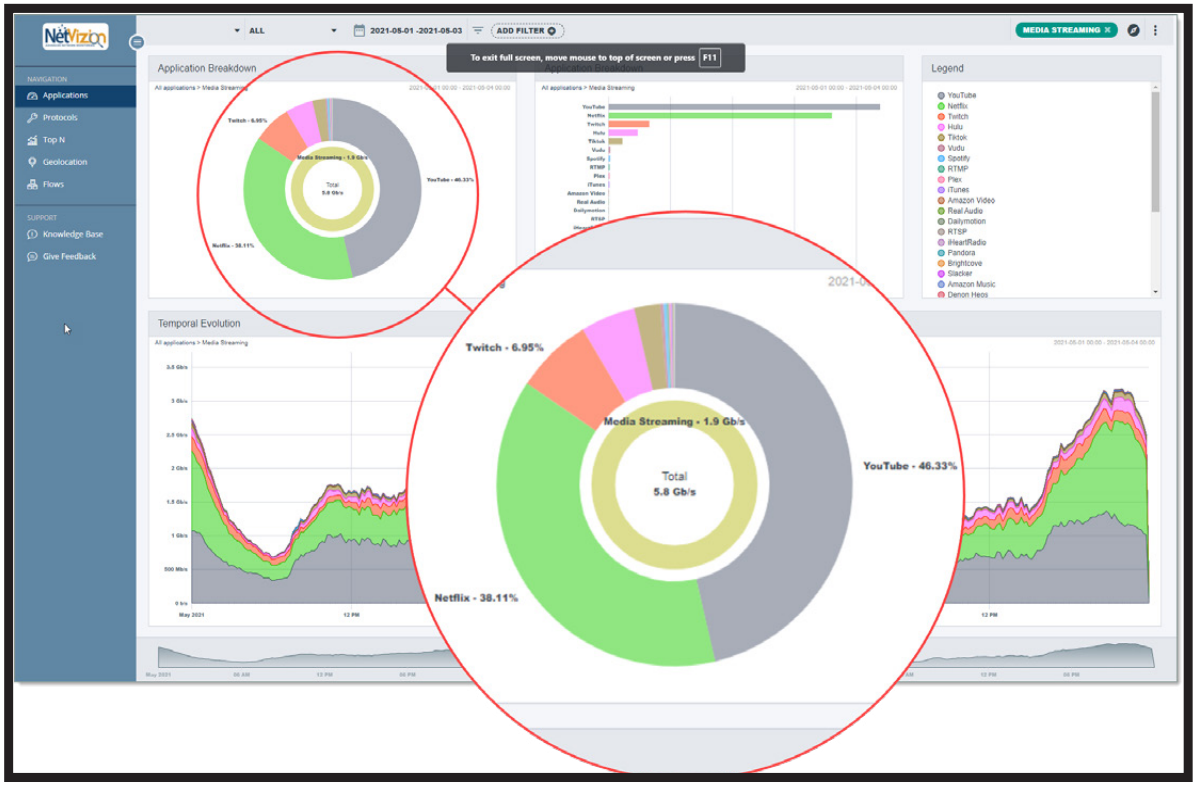
## Netflow Screens from ZCorum's NetVizion network monitoring application



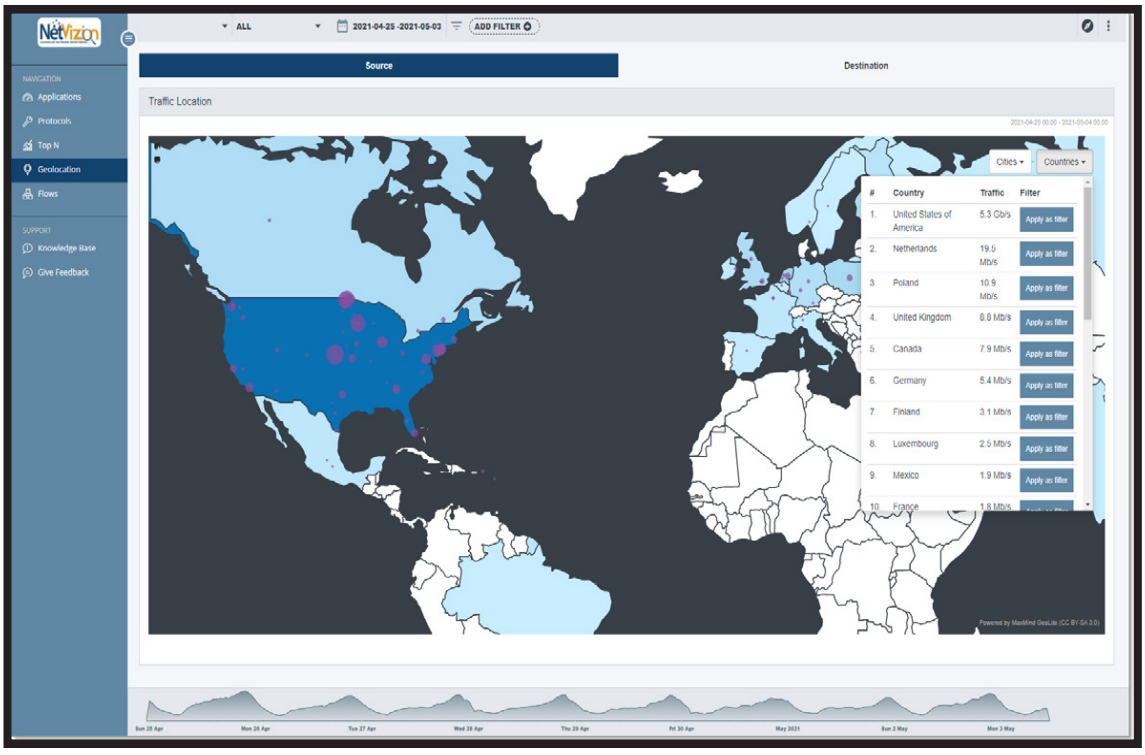

**Traffic Flow by Application**



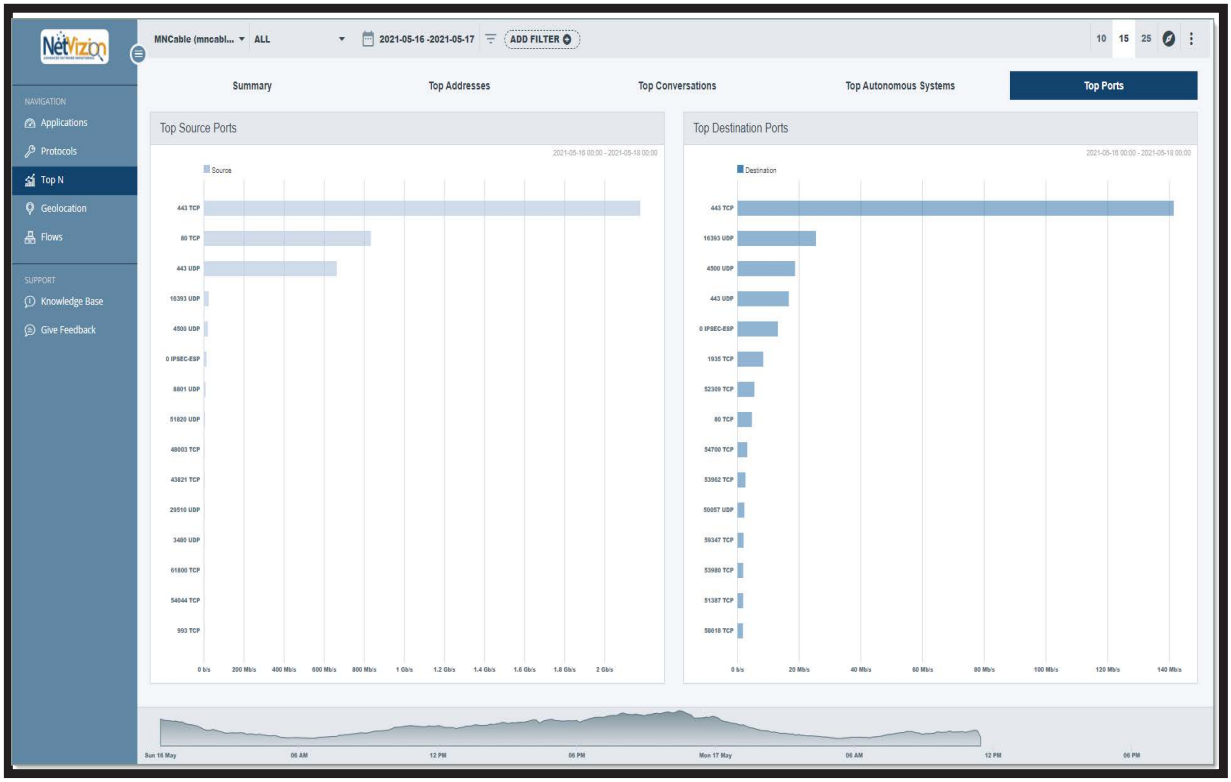

**Traffic Flow by Streaming Apps**



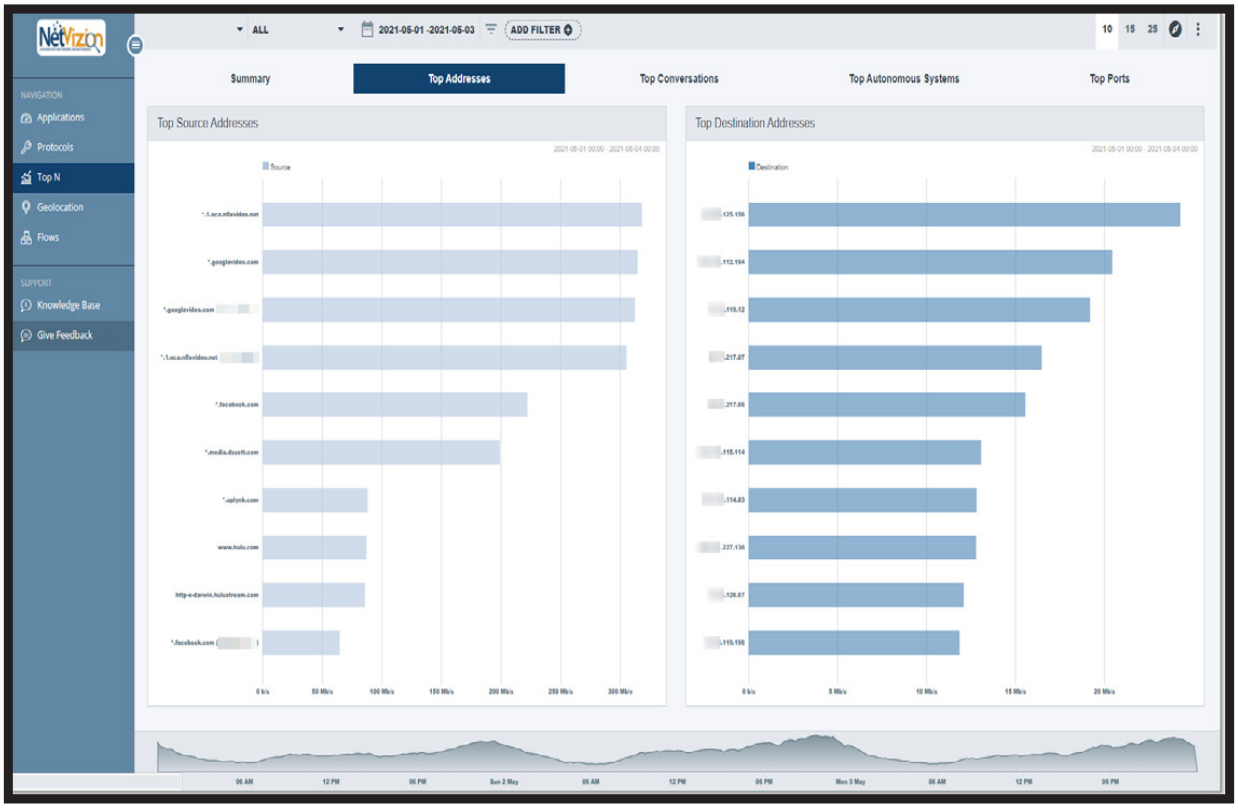

**Traffic Flow by Protocol**




**Traffic Flow by Geographic Location**




## Traffic Flow with Top Talkers




## Traffic Flow by Top Ports