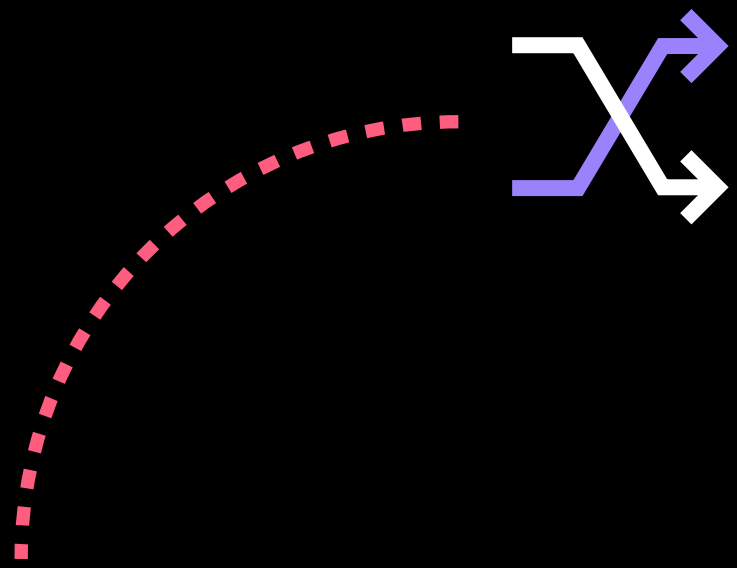
Auvik



Getting started with TrafficInsights

Whitepaper

Contents

03. What is TrafficInsights?

04. Setting up a new device for TrafficInsights

06. Managing devices enabled for TrafficInsights

06. The TrafficInsights dashboard

- **07.** · Filter bar
- **09.** · Time interval selector
- **09.** · Applications area
- **10.** · Protocols area
- **11.** · Top-N area
- **12.** · Geolocation area
- **13.** · Flows area

13. Have questions?

What is TrafficInsights?

TrafficInsights is a new set of features within Auvik that gives you deep visibility into the traffic flowing through your client networks.

With TrafficInsights, you can see all traffic flows across enabled network devices including traffic by application, protocol, IP address, and port; and visual representations of where traffic is going once it leaves the network.

For example, you'll quickly be able to see:

- Who's using banned applications such as BitTorrent.
- Who's hogging bandwidth and slowing down the network.
- Why your client's web server is receiving so many connections from China.
- What a hacked server was connected to during an infection.

TrafficInsights can be used on any network device that supports NetFlow v5, NetFlow v9, IPFIX, J-Flow, and soon, sFlow.

How do I get started with TrafficInsights?

You don't need any extra devices or software to start using TrafficInsights. You simply set up your existing Auvik collector to ingest flow-based data.

The setup and configuration process is very simple and takes just a few minutes. This guide shows you exactly how to do it.

Let's go!

Setting up a new device for TrafficInsights

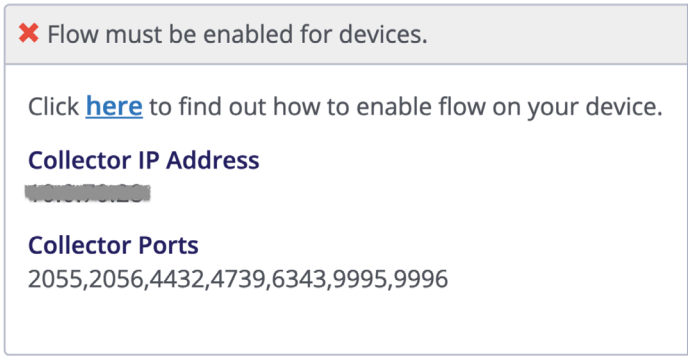
TrafficInsights needs to be set up on each device you'd like to monitor for traffic flows. For this reason, setup should be done at the client level, not at the MSP level.

Remember, for a device to be compatible with TrafficInsights, it needs to be capable of exporting NetFlow v5, NetFlow v9, IPFIX, or J-Flow. (Support for sFlow is coming soon.)

1. From the client dashboard, click on the device you want to set up for TrafficInsights.
2. From the device dashboard, click **TrafficInsights > Setup.**



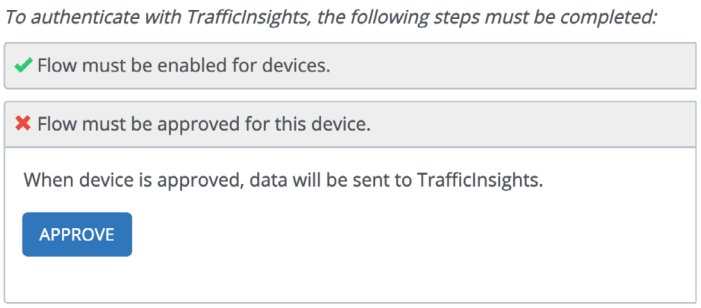
3. On the setup screen, you'll see details on how to configure your device to send flow data. These details will look something like this:
   a. Collector IP Address: Your Auvik collector IP.
   b. Collector Ports: Ports the Auvik collector is configured to receive flow data on. You only need to select one of the ports. If you're not sure which one to pick, use 2055.



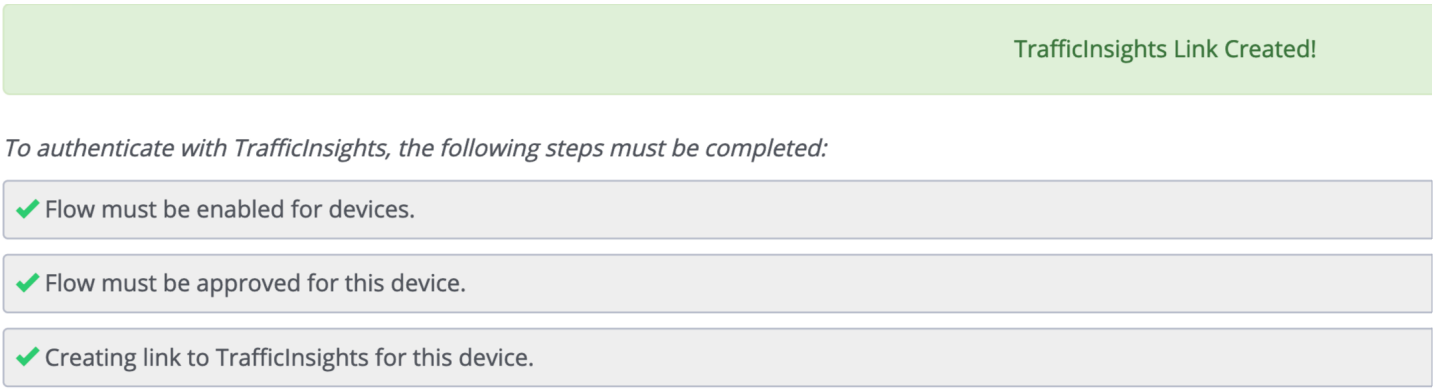
4. Now you need to connect to your device to configure a flow protocol using the information from Step 3. The configuration for each device will be a little different but these are the recommended parameters:
   a. Active timeout: 1 minute
   b. (optional) Report on connection open: False
   c. (optional) Report on connection close: True
   d. Default options for the rest of parameters

5. Once Auvik detects flow data from the device, the device dashboard changes. You'll see a green checkmark. It normally takes just a few seconds for data to start flowing, so if you've followed the manufacturer's recommended steps and you don't see the Approve button within 5 minutes, reach out to **support@auvik.com.**

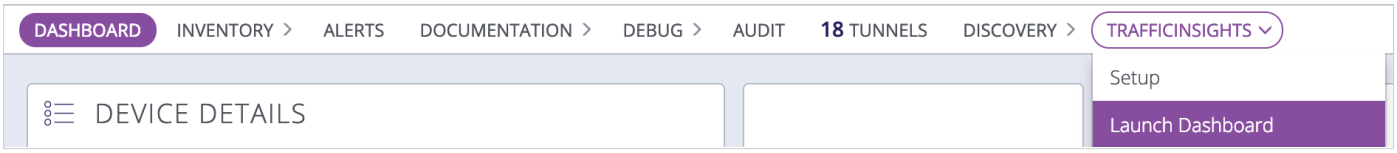
   To enable your TrafficInsights dashboard, click the blue **Approve** button.



6. To access TrafficInsights and review the device's data, click **View device in TrafficInsights.**

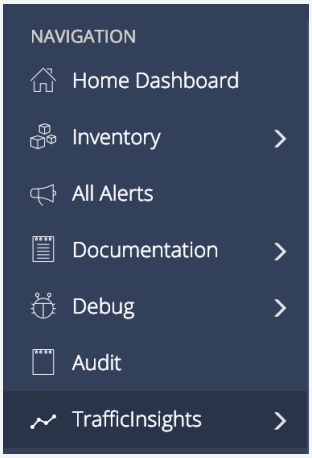


Going forward, you can access the TrafficInsights dashboard by clicking **TrafficInsights > Launch Dashboard** from the device dashboard. The TrafficInsights dashboard opens as a new tab.

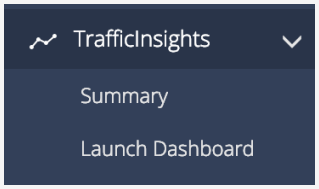


Managing devices enabled for TrafficInsights

In Auvik's side navigation bar, there's a new **TrafficInsights** section.



From here, you can manage all the devices you've configured to send flow data.



Summary shows you the complete list of devices sending flow data, including their status. From the MSP level, you can also see a column with the name of the client the device belongs to.

Launch Dashboard launches your TrafficInsights dashboard. The default view is All, showing you all flows across all TrafficInsights-enabled devices.

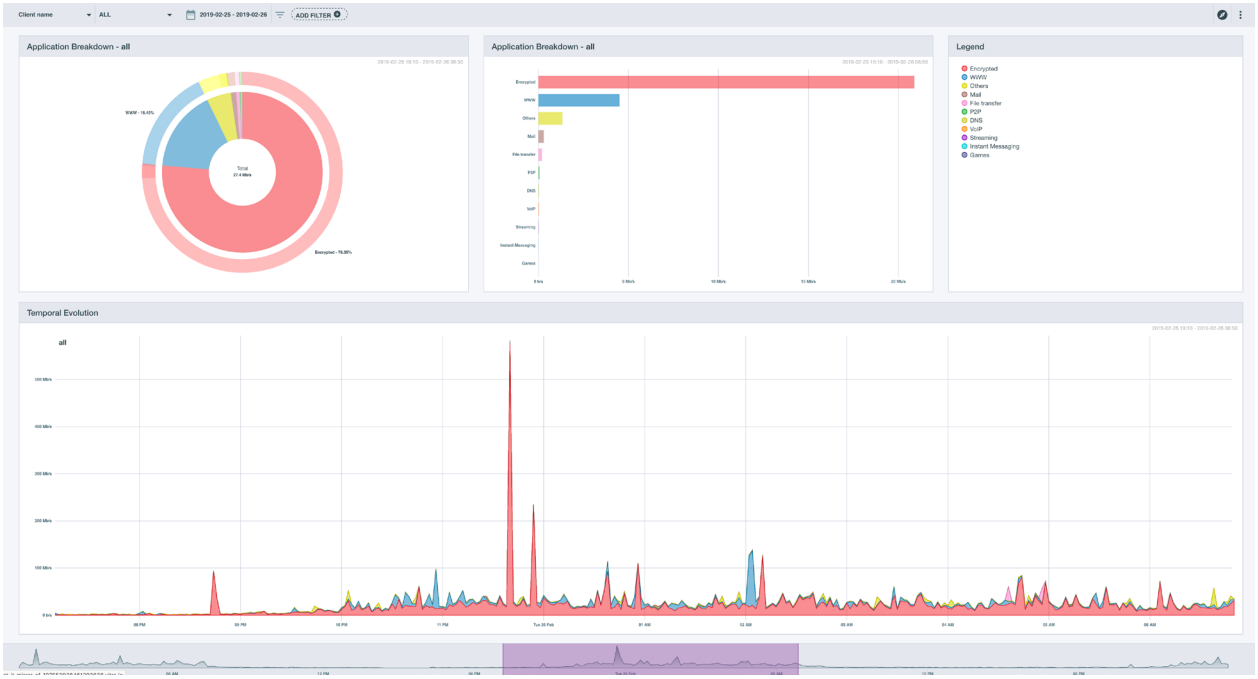
The TrafficInsights dashboard

The TrafficInsights dashboard features a number of different areas, as well as elements that are common to all areas. You can navigate to different areas using the side navigation bar.

At the top of the screen is the entity navigation bar, which here we call the filter bar. The filter bar allows you to select a subset of traffic, a calendar period, and a metric for the data being displayed.

At the bottom of the screen is the time interval selection bar, which can be used to refine the calendar period selection made in the filter bar.

The network traffic data is shown in the center of the screen.



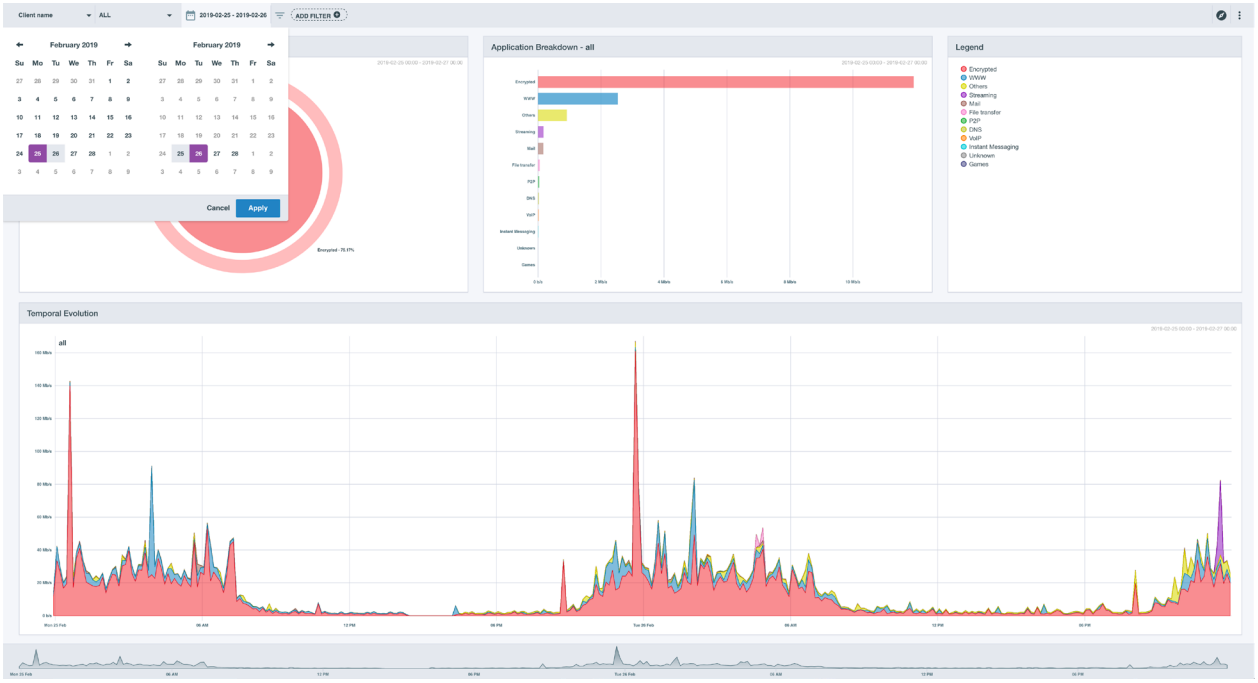
Filter bar

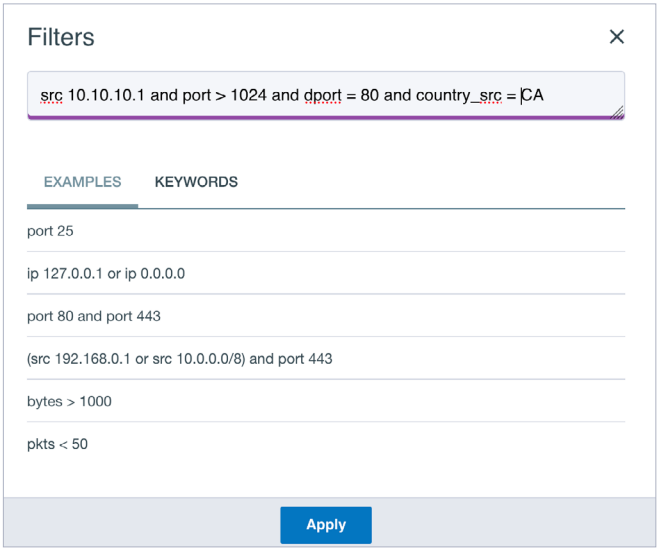
The filter bar lets you configure general elements that are common to all areas. The filter bar remains static as you switch areas so you can quickly analyze traffic from several points of view.

From left to right, the first element is the **Client name.**

Next in the filter bar comes **ALL,** a drop-down list where you can select any device for the chosen client that has been activated to export flow data. You can also choose to leave the list set to All, which shows all the traffic from all the devices together. The data displayed on the screen is defined by the client and device that have been chosen.

The third element of the filter bar is the **Calendar,** which you can use to select a time period for the data. You can refine the time period using the time interval selector (see page 10 for more information).

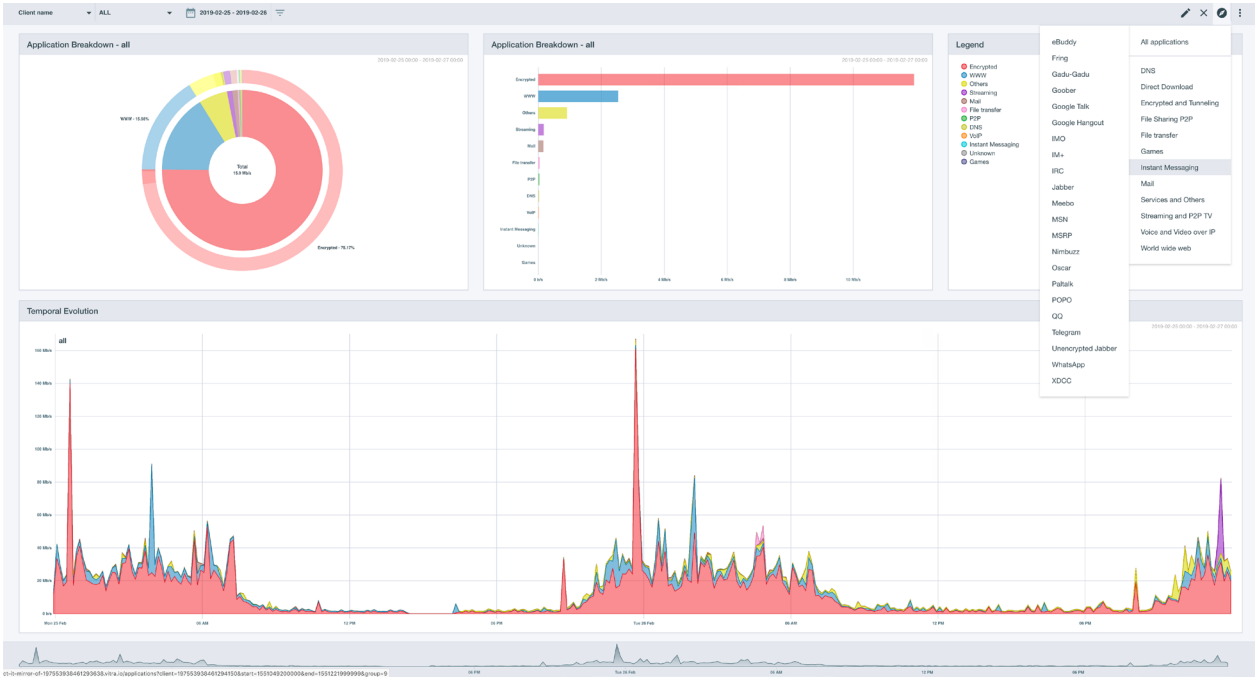




The **Add Filter** button opens the advanced filtering feature. With advanced filtering, you can get granular in tracking network usage by looking at a particular subnet, IP address, or country, for example.

All traffic reports in TrafficInsights are broken down by application group and application.

The **Application** button (the compass point icon in the top right corner of the dashboard) lets you choose the different groups of applications or specific applications you want to see.



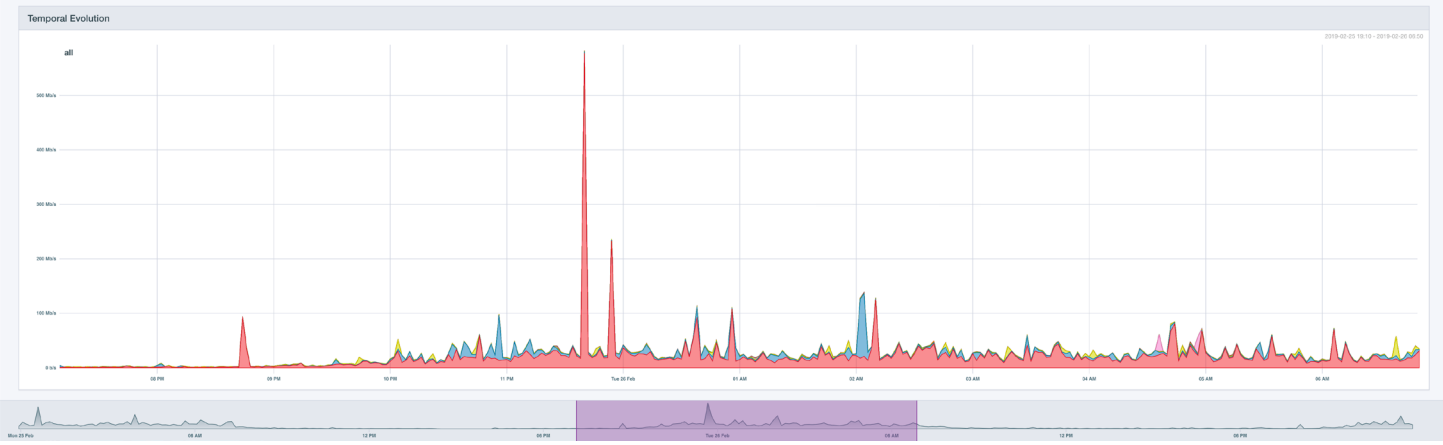
The Settings button (the three stacked dots in the top right corner of the dashboard) lets you choose which metric to use when presenting the data.

There are two main groups—absolute and average values—computed by bits, bytes, packets, and flows. The Settings options also allow you to switch the dashboard to dark mode.



Time interval selector

The time interval selector at the bottom of the screen lets you choose a specific timeframe within your selected calendar period. Your timeframe selection is maintained as you switch areas.

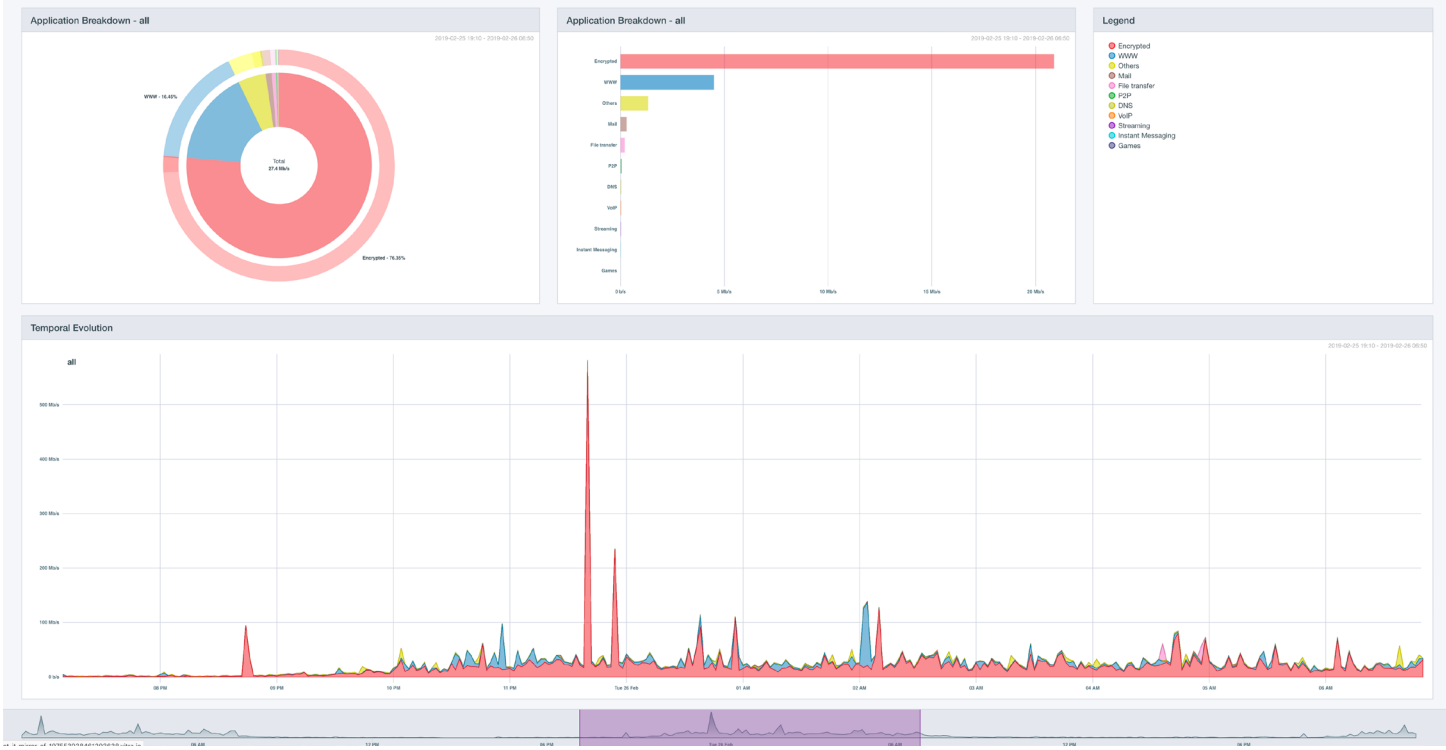


Applications area

TrafficInsights defaults to showing the Applications area. The Applications area shows bandwidth usage broken down by application group.

At the top of the screen, traffic for the selected views is presented in pie and bar charts. Below the charts, a timeline plots how bandwidth usage has evolved over the specified period.

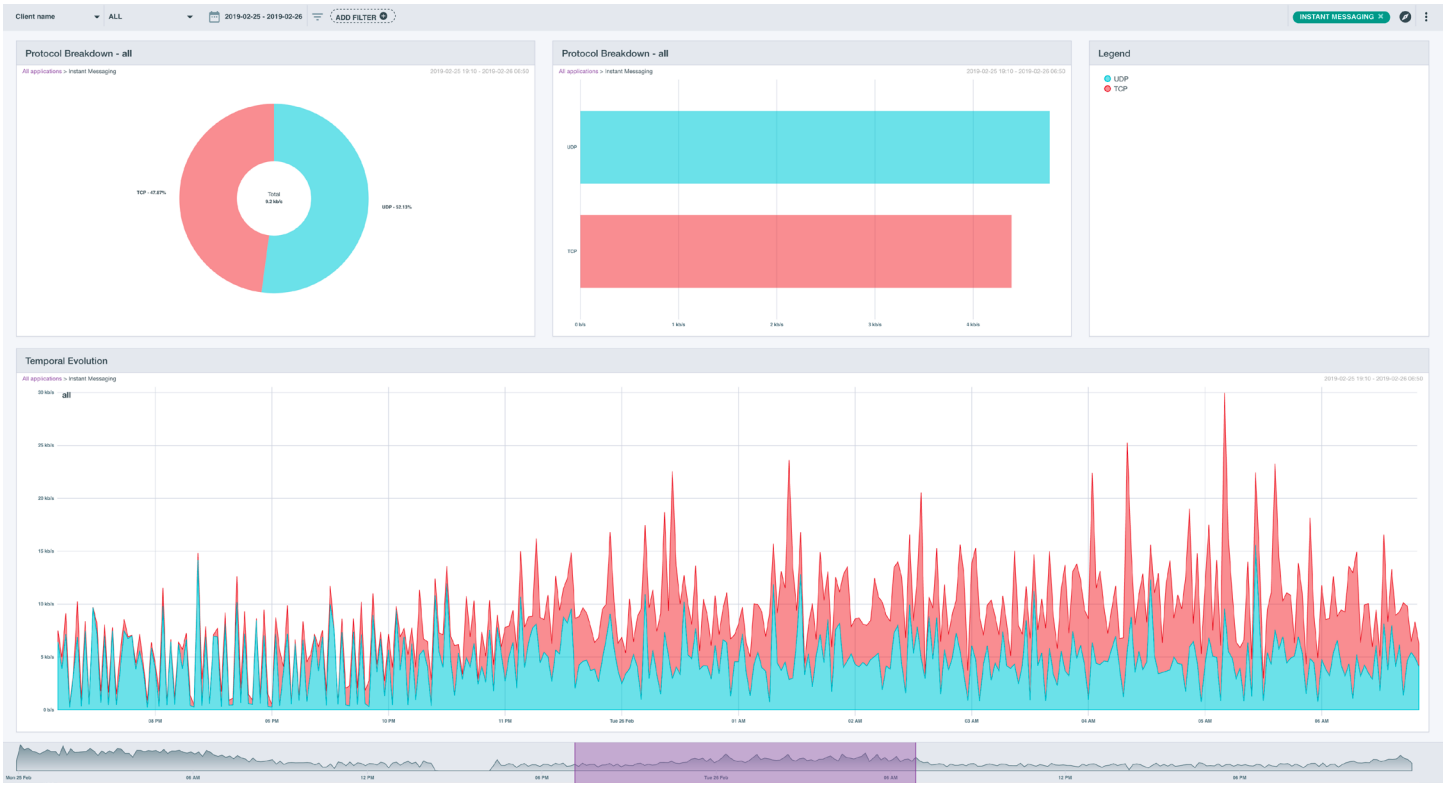
To focus on specific application groups or applications, use the application selector in the filter bar or click any of the charts.



Protocols area

The Protocols area presents bandwidth usage broken down by protocol rather than application. Like the Applications area, the Protocols area shows the distribution of traffic as pie and bar charts and plots the traffic on a timeline.

In the Protocols area, as in every area, you can break down the data by application or other parameters such as country or IP address using the filter bar. This helps you identify what protocols a specific application is using.



Top-N area

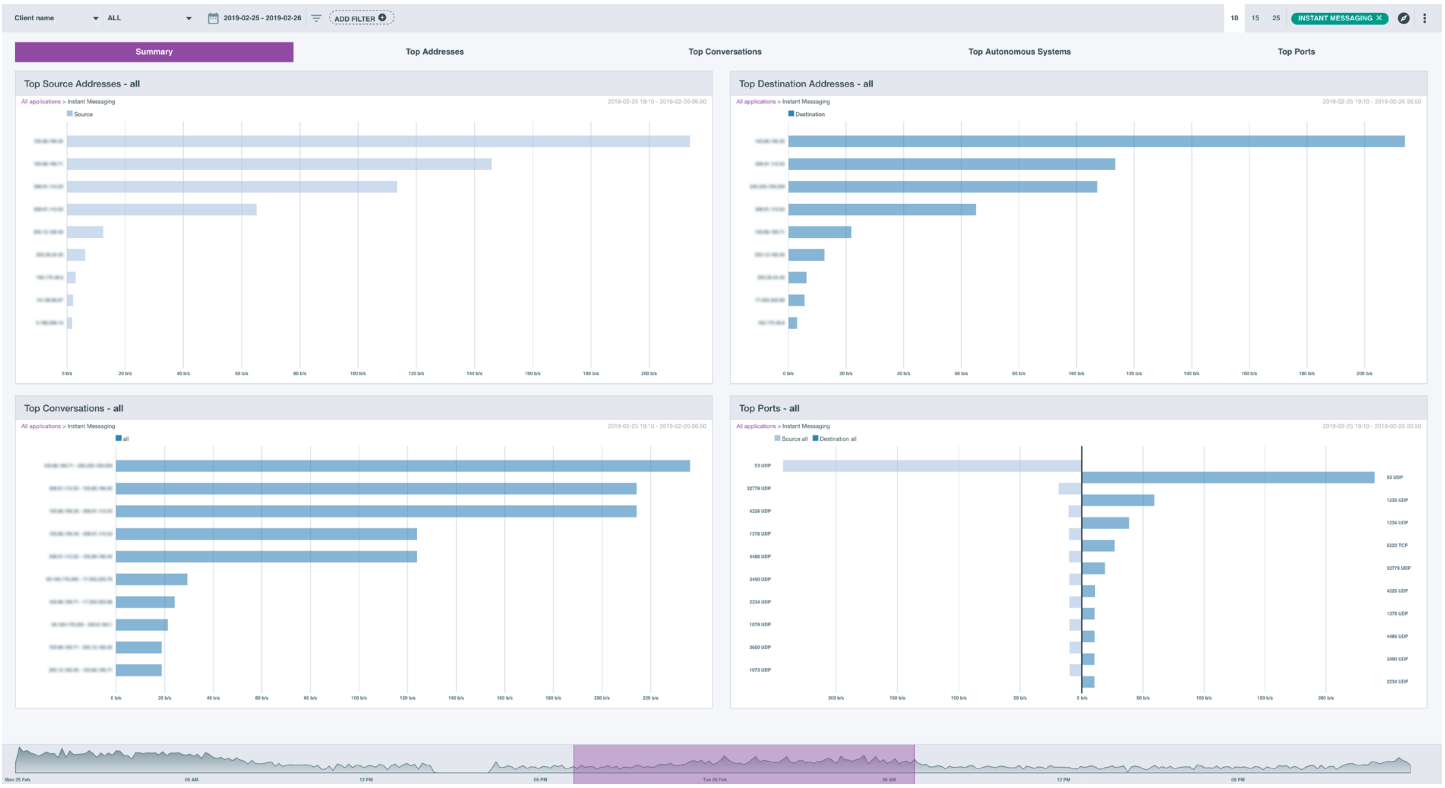
The Top-N area helps you identify the behavior of individual entities on the network. The Top-N area has five sub-areas: Summary, Top Addresses, Top Conversations, Top Autonomous Systems, and Top Ports.

The view defaults to the Summary sub-area, which gives you an overview of the information on the rest of the sub-areas.

The Conversations sub-area shows you the IP address pairs that are exchanging the highest volumes of traffic. These are shown because watching individual IP addresses in Top Addresses can be misleading. For example, you can't always assume that the top source IP address is talking to the top destination IP address.

The rest of the sub-areas should be self-explanatory.

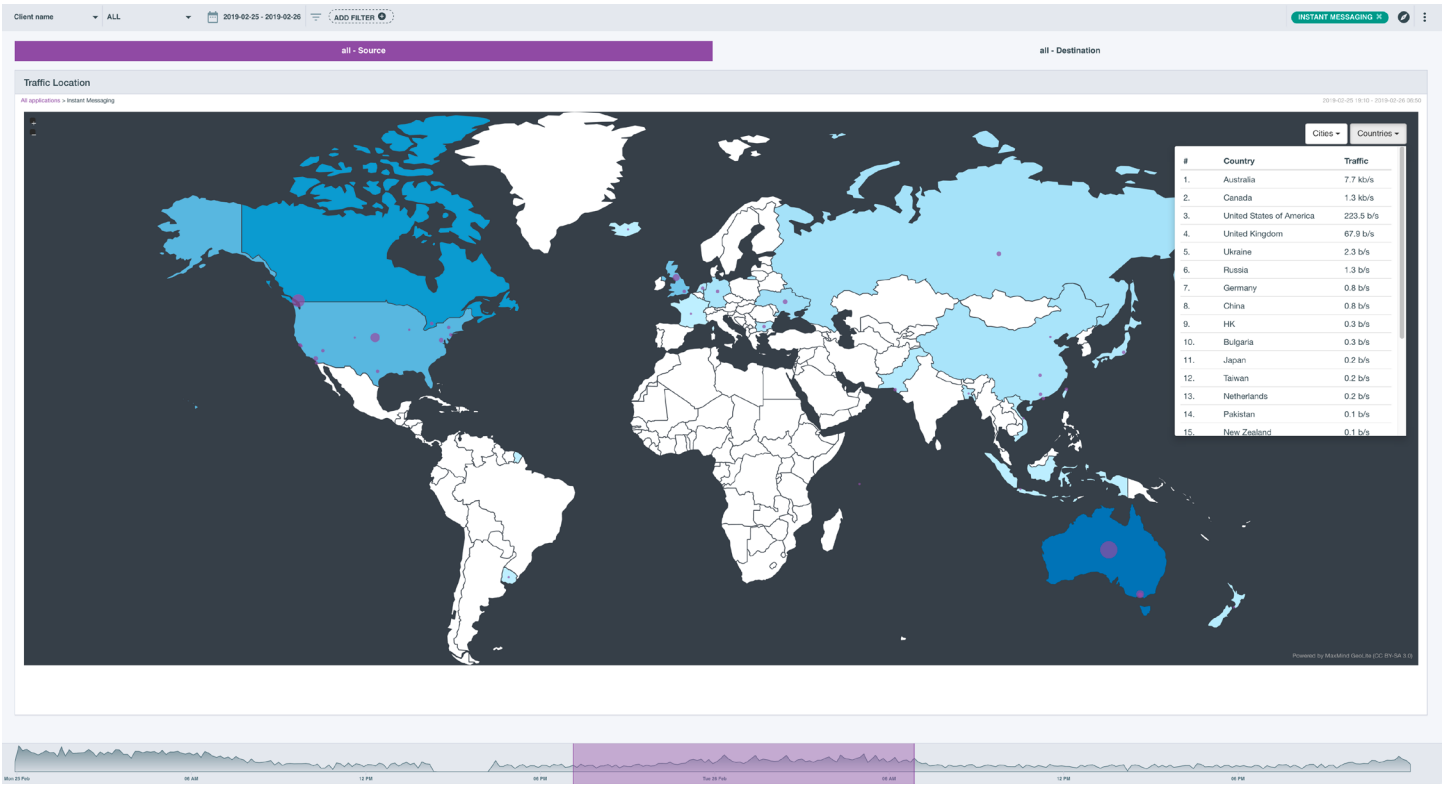
As with all the areas, you can break down the data by application using the filter bar. This can help you identify the ports used by a given application, an IP address causing a sudden traffic spike, or which internal computers are engaging in peer-to-peer conversations.



Geolocation area

The Geolocation area shows you the distribution of traffic by geographic location. The data is shown by source and destination IP addresses.

The geolocation area can show you where network users that are consuming or uploading content are located.



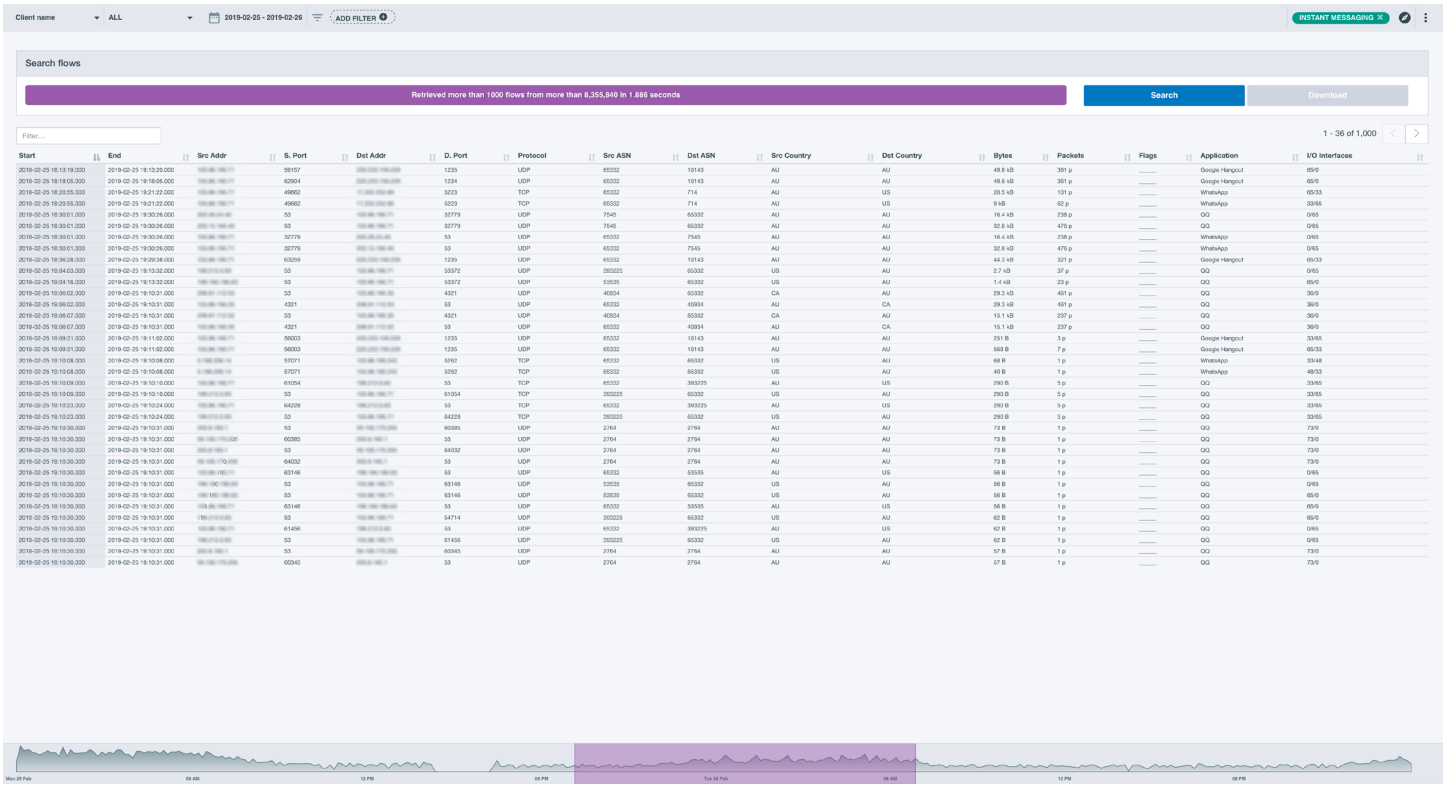
Flows area

The Flows area lets you directly query the raw traffic data that TrafficInsights is processing.

The Flows area provides the deepest insights and is usually used to study and analyze the characteristics of a specific anomaly.

A simple form helps you set your search parameters. For example, you can search by IP addresses, ports, protocols, or autonomous systems.

Searches are limited to 1,000 flows to avoid overloading the browser.



Once you submit your search, you'll see a list of flow statistics. You can export this data to a CSV file, then import it into virtually any spreadsheet program.

You can also process the data using scripts to extract specific information you might be interested in.

Have questions?

The Auvik support team is always available to provide technical guidance and to answer your questions. To reach us:

- Use the chat box in the bottom right corner of the Auvik window.
- To create a ticket, email **support@auvik.com**. Someone from the support team will get back to you shortly.

© Copyright 2013-2024 Auvik Networks Inc. All rights reserved. Auvik, the logo, and other identifiers of Auvik goods or services are trademarks of Auvik Networks Inc and may not be used without express written permission. All other trademarks, service marks, trade dress, and logos are the property of their respective owners. Reference to them does not imply sponsorship, affiliation, or endorsement.

auvik.com/try-now