Auvik

Keeping network performance healthy & secure with intelligent network traffic analysis

Whitepaper

About Auvik Networks

Auvik is a cloud-based IT management platform that helps IT departments proactively manage their networks, endpoints and SaaS applications. The key is absolute simplicity: seamless deployment, an intuitive interface, and effortless automation. The result is less friction for IT departments, so that everyone can work however and wherever they want.

Nobody likes the feeling of not knowing.

As a trusted network advisor, “I don’t know” is a dangerous phrase you don’t want to say.

Just take a look at how it sounds:

“Who’s hogging bandwidth and slowing down the network?” I don’t know.

“Who’s using banned applications like BitTorrent? I don’t know.

“What was a hacked server connected to during an infection?” I don’t know.

If you say it often enough, it can completely break down the trust you’ve earned through effective network management. But when it comes to questions about network performance, you haven’t had much of a choice.

The issue is that many traditional NetFlow options don’t cut it. They’re incredibly expensive and tend to fall short when it comes to encrypted traffic. And since the vast majority of all network traffic is encrypted, that's a problem.

That’s why we created Auvik TrafficInsights.™ This network traffic analysis feature uses machine learning to complement device flow data with additional metadata—like source and destination geography—to give you granular insight into the applications and protocols being used so you can really understand the traffic.

Even if it’s encrypted.

TrafficInsights can collect and analyze flow data from any device supporting NetFlow v5 or v9, IPFIX, sFlow, or J-Flow. If any traffic flows through a TrafficInsights-enabled network device, then you can see who’s on the network, what they’re doing, and where their traffic is going.

Better yet, you can enable TrafficInsights on almost any device Auvik is already monitoring on your sites—including firewalls, routers, and some switches—since these devices can usually export flow data.

You’ll have deep visibility into all traffic that flows across the network. And you can stop saying “I don’t know.” Instead, you can confidently answer any question thrown your way.

Read on for 5 common cases where TrafficInsights can help.

What our customers say

> “One of our customers was experiencing network performance issues and TrafficInsights showed us exactly what was causing the issue. It turned out the firewall was being taxed by storage traffic. We moved this traffic off the device and instantly improved the client’s connectivity.”

Patrick Garman
WBM Technologies Inc.

Case #1

The surprise growth spurt

Before TrafficInsights, identifying the reason why the internet bandwidth was always maxed out was a guessing game.

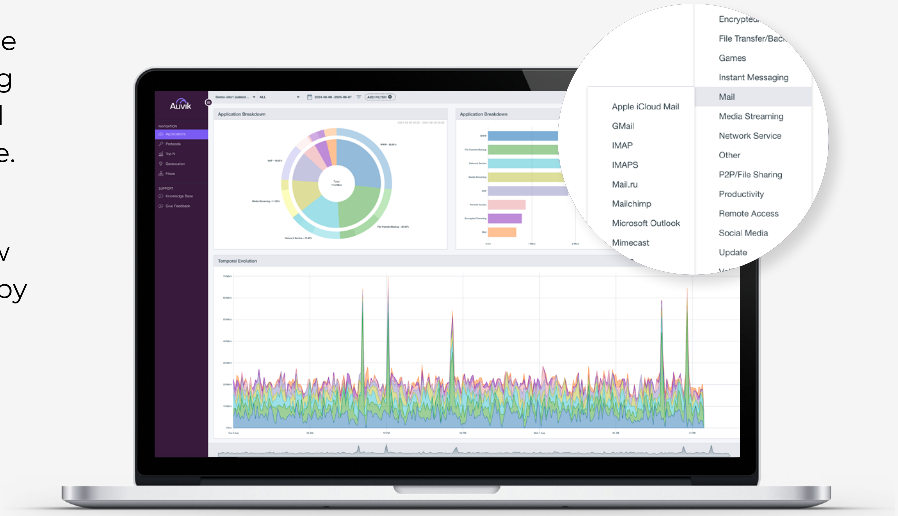
You knew *how much* bandwidth was being used, but you didn’t know what the traffic was or if it was legitimate—and unless you were walking around the affected site looking at monitors, you might not ever find out.

In TrafficInsights, all traffic reports are broken down by application group, application, and protocols. The Application view lets you choose the different groups of applications—including DNS, File Sharing P2P, Instant Messaging, and more—or specific applications you want to see.

In this view, you can determine the cause of the high bandwidth usage and, with just a few clicks, whether the high traffic load is caused by business-critical file transfer apps or personal peer-to-peer apps.

If bandwidth is being spent on a personal app, you can drop into the endpoint causing the spike and shut it down or work with the end user to stop it.

And if the network is reaching peak utilization because of legitimate business traffic, then you have the proof you need to make the case to invest in a better internet connection. It’s a capacity planning dream come true.



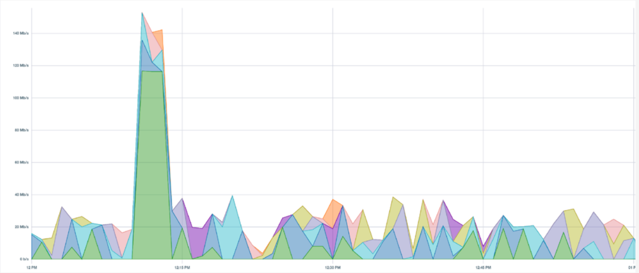
Case #2

The network pig

Network performance issues can arise at the most inconvenient times — like when you're sleeping at 2 a.m. or driving to pick up lunch at noon. Since most tools require you to catch the issue in real-time, that means you'd be working in your pajamas or skipping lunch… again.

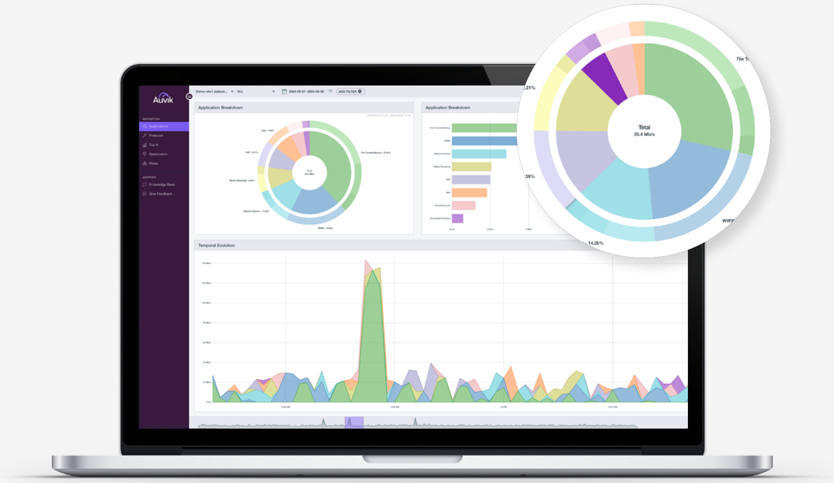
That's not the case with TrafficInsights. Since TrafficInsights stores flow data for 14 days, you can go back in time to investigate an issue.

Using the time interval selector at the bottom of the TrafficInsights dashboard, you can select a specific time frame within a specified date range — like Tuesday from noon to 1 p.m., for example.



Since your time frame selection is maintained as you switch dashboard panels, you're able to dive into IP details and application usage as part of your investigation.

Using the Top Talkers view, you can see exactly which device is using up all the bandwidth, and you can trace that information back to the specific user of the device.



Let's use a true story to show how this visibility can help you solve issues fast.

At noon every weekday, a network was slowing to a dead crawl. Before deploying Auvik, the troubleshooting process had been to get a technician on-site to run commands to try and find the device and port generating the traffic. That process required *a lot* of manual effort and still didn't uncover the issue.

But after putting Auvik on the network, the tech quickly identified the culprit: Automated backups had been mistakenly scheduled for noon instead of midnight. They rescheduled the backups with a few keystrokes—the problem was solved and the network users were happy.

To see why the user is taking up so much bandwidth, you can navigate to the Applications breakdown and determine if they're backing up files while away from their desk or if they're streaming Netflix while they eat their lunch.

Case #3

The banned (but used) application

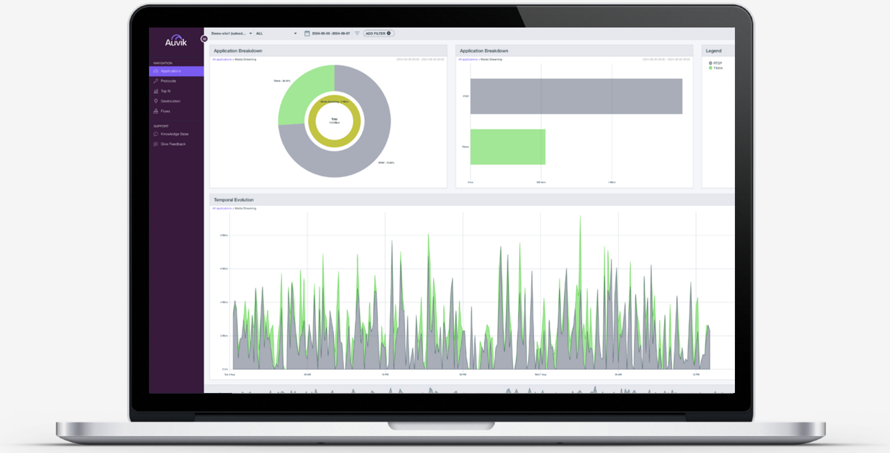
Some of your clients may have a list of banned applications their employees are not allowed to use. The problem is saying "You're not allowed to use this app" isn't going to stop some people.

If your clients suspect a banned application is being used, the Applications view in TrafficInsights should be the first stop in your investigation.

In the Applications view, you can quickly audit for banned applications —like instant messaging apps such as WhatsApp or peer-to-peer apps like BitTorrent—by selecting the application group they belong to.

If the application is in use (like WhatsApp is above in theInstant Messaging tab), you can quickly see how much traffic is being used and identify the user behind it. It doesn't matter if the traffic is encrypted.

With this information, you'll be able to help your clients enforce their application bans once and for all.



What our customers say

> “I was able to locate a device that was communicating with China for no reason. I was extremely impressed with how quickly I could find what I was looking for, and we resolved the issue by adding a geo-restriction rule to the firewall. Best NetFlow data interface I’ve used so far.”

Adam Peterson
Real IT Solution

Case #4

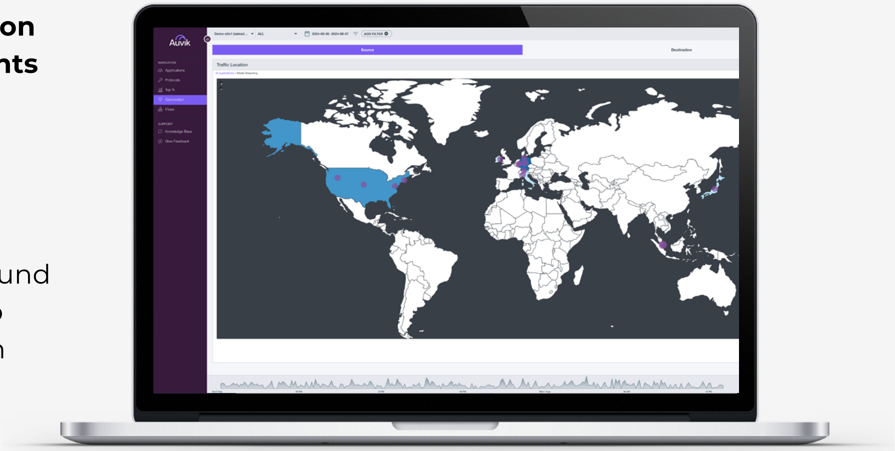
The globetrotting traffic

The networks you manage may be in highly regulated industries where they’re not allowed to communicate with certain countries, or worse, may have a data leak. But how are you supposed to know when data might be passing through a destination it’s not supposed to be in?

With TrafficInsights, it’s as easy as looking on a map. The Geolocation area in TrafficInsights shows you the distribution of traffic by geographic location.

In this view, you can see the source and destination IP addresses of all your network traffic. This allows you to easily spot traffic bound for sanctioned countries your network has no business communicating with, identify which device is sending the traffic, and isolate the device the traffic is coming from.

If you determine the traffic is illegitimate, potentially malicious, or headed to a sanctioned country, then you can take action and add restrictions to stop it in its tracks.



Case #5

The infected device

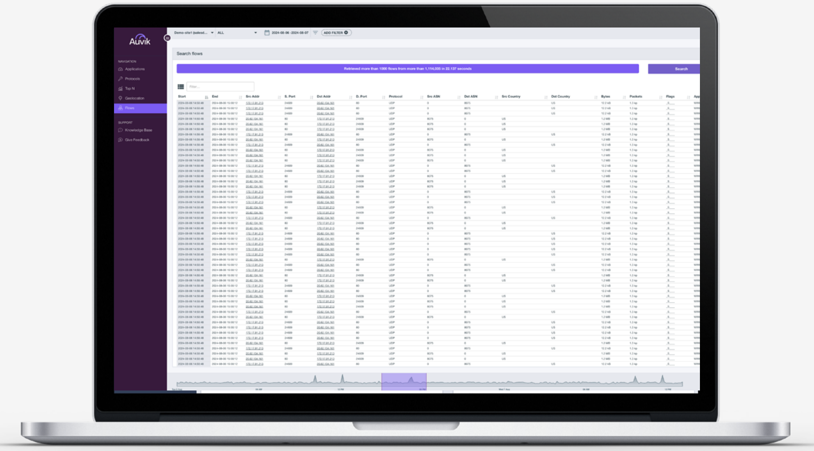
If an asset is compromised, it's important to understand everything the infected device talked to while it was infected — if anything is missed, the network is at risk.

The Flows area of TrafficInsights lets you directly query the raw traffic data that TrafficInsights is processing. It provides the deepest insights and can be used to analyze the characteristics of a specific anomaly.

In this area, you can investigate the infected device's flow records to assess the impact the malicious traffic has had on the network. Thanks to a simple form, you can set your search parameters—by IP addresses, ports, protocols, or autonomous systems—to pinpoint the source and destination of all traffic to or from the infected device.

This means you can see everything an infected device did and identify devices the malicious traffic touched on its way through the network. You can then resolve issues on each device that was hit by malicious traffic.

And thanks to an exportable CSV file of the flow records, you can update your team on your work and give assurance that you've got things under control.



Retrieved more than 1000 flows from more than 1,114,035 in 22.137 seconds

Start	End	Src Addr	S. Port	Dst Addr	D. Port	Protocol	Src ASN	Dst ASN	Src Country	Dst Country	Bytes	Packets	Flags	App

Auvik

NETWORK MANAGEMENT

Ready to see TrafficInsights for yourself?

Getting Started is Easy.

Try Auvik free for 14 days (no credit card required) to find and resolve problems faster than ever—from anywhere.

Or **book a demo** and we'll walk you through it and address any questions you may have.

Try Auvik Network Management yourself!

Start trial