auvik

The 7 Components of a Profitable Managed Network Service

ABOUT AUVIK NETWORKS

With its cloud-based network operations system, Auvik helps MSPs deliver profitable network services. Auvik's software provides unprecedented insight into client networks and automates complex and time-consuming tasks so MSPs can scale their practices efficiently.

CONTENTS

Networks Are the Engine That Run Today's Businesses

The 7 Components of a Profitable Managed Network Service

- #1: Client Knowledge
- #2: Real-Time Awareness
- #3: Controlled Access
- #4: Network Continuity
- #5: Integrated Workflows
- #6: Reporting
- #7: Network Expertise

TL;DR Summary

NETWORKS ARE THE ENGINE THAT RUN TODAY'S BUSINESSES

Most business owners are familiar with the basics of running a successful business: Develop a valuable product or service. Market it effectively. Deliver amazing customer service. Reinvest profits to grow the business.

But there's another secret to operating a profitable business today that most MBA programs don't cover: *Having an efficient, reliable IT network*.

> *The network is the business,*
> *and the business is the network.*

After all, most businesses—regardless of size or industry—rely on networks to get things done. Nearly every app, system, and person in a company is connected.

- VoIP and instant messaging allow employees to share information rapidly and cost-effectively.
- Servers host vital company data.
- Cloud-based document services let workers store and edit information collaboratively.
- Customers expect 24/7 access to a company's website and email.
- Ecommerce platforms bring in revenue.
- Point of sale systems process transactions.

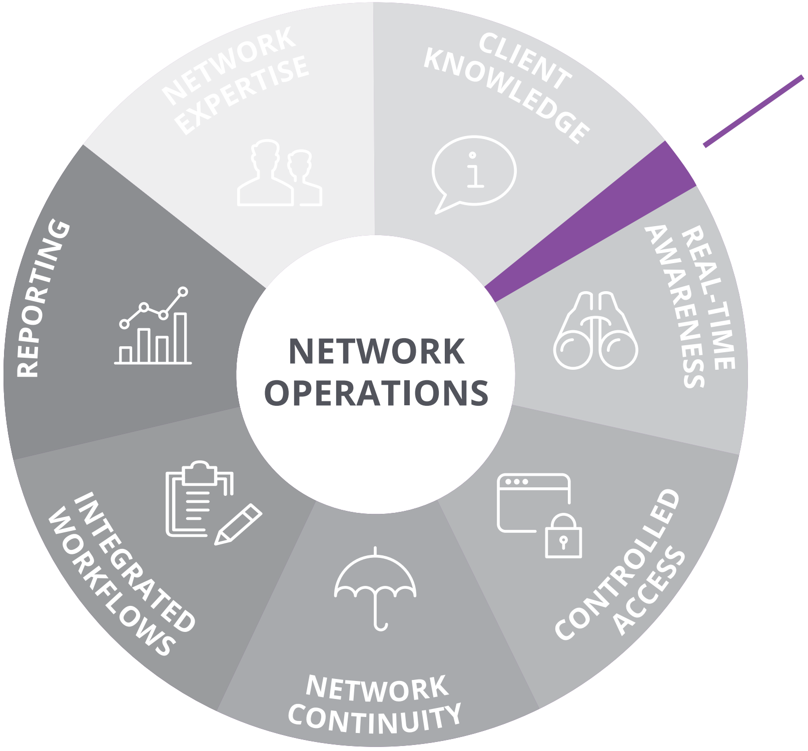
When your client's network goes down, their business stops. Productivity plummets and revenue is jeopardized. And suddenly, your relationship with that client is at risk too.

So their network needs to just work—all the time.

BUT THERE'S A HUGE PROBLEM IN NETWORK MANAGEMENT

Traditionally, "network management" hasn't lived up to its name.

It's been focused primarily on servers and desktops—which are only part of the network.



Traditional network management has focused on monitoring and little else.

And it's been focused on reactive monitoring—which is only a small slice of the network operations activity that needs to happen.

As the devil in that old Caramilk commercial used to say, "*Not enough*."

Occasionally pinging the network to see if it's up? Not enough. Getting an alert when some vital device like a router goes down? Not enough. Not anymore.

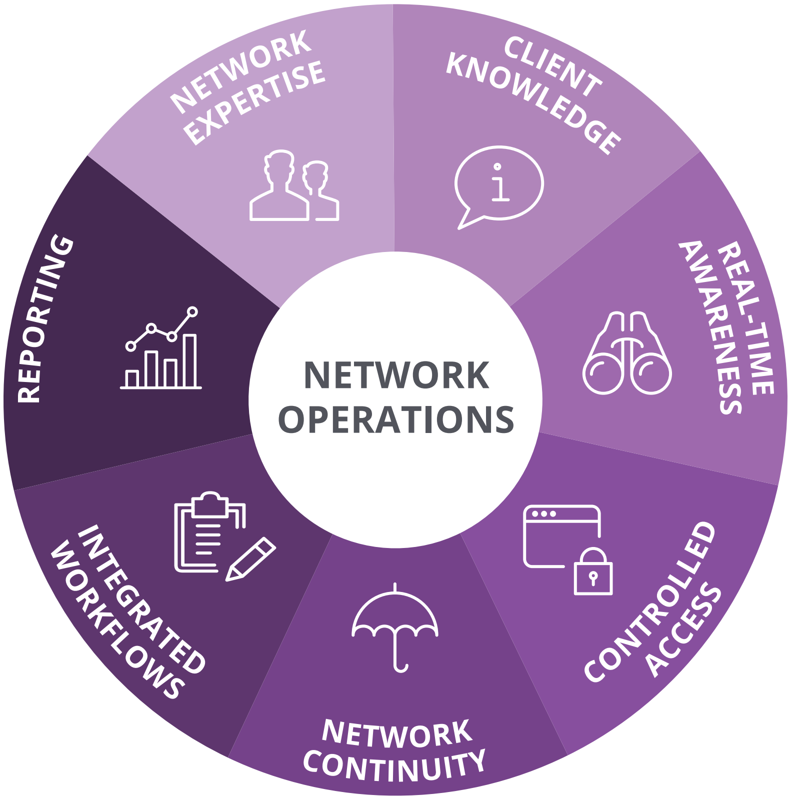
This problem in network management can be a hard truth for MSPs to face. But it's also an amazing opportunity.

By building out your network practice beyond monitoring servers and endpoints, you can:

- Enhance the network services you're already offering to existing clients
- Bring more devices under management for increased revenue
- Bring on new clients who are struggling with their networks
- Streamline and optimize your network processes
- Differentiate yourself in a crowded MSP market

This guide will outline the 7 components of a complete managed network service and how using them together as a discipline will help you scale your practice profitably.

THE 7 COMPONENTS OF A PROFITABLE MANAGED NETWORK SERVICE



TRUE NETWORK OPERATIONS IS A DISCIPLINE WITH 7 COMPONENTS

Client knowledge	So you know exactly what your client requires and expects
Real-time awareness	So you know exactly what's happening on your client networks at all times
Controlled access	So you can manage user access and network device credentials in one secure location
Network continuity	So you can get client networks back up and running quickly when disaster strikes
Integrated workflows	So your processes are as efficient as possible
Reporting	So you can demonstrate your value
Network expertise	So you can deliver top-notch service

> *"Services that enhance the daily work being done to achieve business objectives show that the MSP understands what organizations really need."*
>
> - **Julie Hunt**, PivotPoint

#1: CLIENT KNOWLEDGE

So you know exactly what your client requires and expects

Life would be pretty easy if all your clients had identical needs and identical networks. But they don't. Every business is different and comes with unique requirements.

And few businesses truly know what those requirements are when it comes to IT. They're relying on you—the IT experts—to translate their business needs into a network that supports those needs.

In order to do that, you must fully understand the business itself: the day-to-day workflows, the broader business goals and priorities, and the bottlenecks.

Then you can layer on an in-depth understanding of their current network and how it supports the business. What are they key systems and what are they used for? Where's the risk? How tolerant is the client to risk?

An Internet connection going down at a manufacturing plant, for example, is very different than a connection going down at a company that hosts their own servers. Each company requires different care—which you'll only know by digging and learning.

Consulting and interviewing are a key part of the initial onboarding process, of course. But you'll also need some smart tools to x-ray, inventory, and assess the network.

A good system will map and document the network for you, as well as provide some automated analysis based on best practices. (Tracing wires and mapping ports by hand? Fugeddabout it. That's a massive efficiency bottleneck.)

Once you have a clear picture of the network you're dealing with, the trick is to stay up to the minute with your knowledge. And that takes us into component #2 of a profitable managed network service.

> *"Real-time monitoring is useful for big problems like a system down event, but it's just as key for seemingly small issues. Proactively responding to little issues as they happen means IT might be able to prevent a bigger problem that impacts the business."*
>
> \- **Ethan Banks**, co-founder of Packet Pushers Interactive

#2: REAL-TIME AWARENESS

So you know exactly what's happening on your client networks at all times

Twenty years ago, you might have been handling networks with a fixed number of devices in relatively static positions. No more.

Today's networks are in constant flux as devices connect and go offline throughout the day. As well, traffic ebbs and flows at variable rates causing bandwidth usage to spike and fall. Documentation goes out of date the minute you complete it.

This is particularly true because of the proliferation of mobile devices that come online and go offline at unpredictable rates at many organizations, especially those that aim to be BYOD-friendly. Mobile devices also tend to switch between different types of connections, or join and leave VPNs, in ways that a one-time snapshot of a client's network can't reveal.

Real-time awareness helps you prevent issues before they happen, not least by allowing you to compare historical and current data to spot trends. If something in your network stats looks inconsistent with past data, you have an early warning about a potential problem.

So if your network monitoring isn't being done in real-time, you're either missing key information entirely or getting it too late to react effectively.

Static network maps that don't change as the network changes aren't helpful either. How can you troubleshoot a network if you're looking at an outdated view that's no longer relevant?

For that matter, how do you know what's in your inventory at a crucial moment if you're not monitoring in real time? When trouble strikes, you want to know how many devices are being affected at that instant, not an hour or a day ago.

By the way, real-time awareness entails ongoing monitoring of all of your devices, not just certain ones. "It's not enough only having visibility at the gateway and the endpoint," says Ryan Morris, senior director of operations at BAI Federal. "You need to show what's going on across the board."

> *“Customers trust MSPs with the lifeblood of their businesses. But just how well is this lifeblood protected? In the case of passwords, the answer is, ‘Maybe not so much.’”*
>
> - **Doug Barney**, MSP Today

#3: CONTROLLED ACCESS

So you can manage user access and network device credentials in one secure location

Eek! Many MSPs are putting their clients at risk with insecure credential management and user access practices.

In fact, a 2013 study by Passportal revealed that more than 80% of MSPs store client passwords on Excel spreadsheets, Word documents, homegrown database solutions, and unprotected fields in their CRM or PSA system.

Don’t be part of that crowd.

In other words, don’t be like the Reddit user who writes, “We currently track passwords to access our client machines via our Confluence wiki.”

Oof. Private or not, a wiki is not at all designed or suited to keeping information secure. It might be better than keeping passwords in a spreadsheet that you upload to a public folder on Dropbox, but not by much.

And security is only part of the user access problem for MSPs. As the Reddit writer also admits, storing access information on a wiki constitutes an “administrative nightmare” because password data has to be updated whenever an employee leaves the company.

Set yourself apart from other MSPs by taking advantage of controlled access solutions that allow you to manage user access and client device credentials in a secure and compliant way.

A good solution will encrypt and store access credentials securely, where login information has to be entered only once. It will also allow you to define, granularly, which of your employees has access to which clients' login information.

Last but not least, solid controlled access lets your clients see or manage devices, where appropriate. When you put this feature together with real-time awareness and alerting, you're able to track any changes your clients make.

So say goodbye to sharing passwords with your entire team and having to update access information each time an employee moves on. Say hello to segmenting workloads among your techs in a way that provides each team member with the information needed to get the job done—and nothing more.

> *"With clients, the demand used to be that [backups] would refer back to yesterday and they were fine with that, but now they want to be referred back to almost real time."*
>
> \- **Steve Rutkovitz**, CEO, Choice Technologies

#4: NETWORK CONTINUITY

So you can get client networks back up and running quickly when disaster strikes

One of the main reasons—perhaps the main reason—your clients hire you to manage their network is because they want to know the network will continue to support the business, whatever disasters might strike.

When IT infrastructure goes down, companies lose huge money. Depending on their size, downtime can cost from hundreds of dollars per hour to many thousands. And the people responsible for that infrastructure—that's you—are suddenly at risk of being fired. At the very least, it can dent an otherwise positive client relationship.

As we've said before, your clients expect the network to just work—all the time. If the network does go down, minutes matter. Speed in restoring service while losing as little client information as possible is critical.

To meet such expectations requires you to draw on a combination of other network operation components, including client knowledge and real-time awareness.

- **Detailed knowledge of the network's intent.** To effectively maintain network continuity, you need an intimate understanding of what the network is supposed to be doing and why.

- **Constant network monitoring.** We've already discussed the importance of real-time awareness to delivering proactive network service. It's essential for network continuity because constant monitoring ensures you always have the most up-to-date information about network configuration and status when something goes wrong.

- **Real-time alerting.** In addition to constant monitoring, an effective alert system lets you know about emerging problems before they bring the network down. Remember what Ben Franklin said about an ounce of prevention.

Client knowledge
+ real-time awareness
+ real-time backups

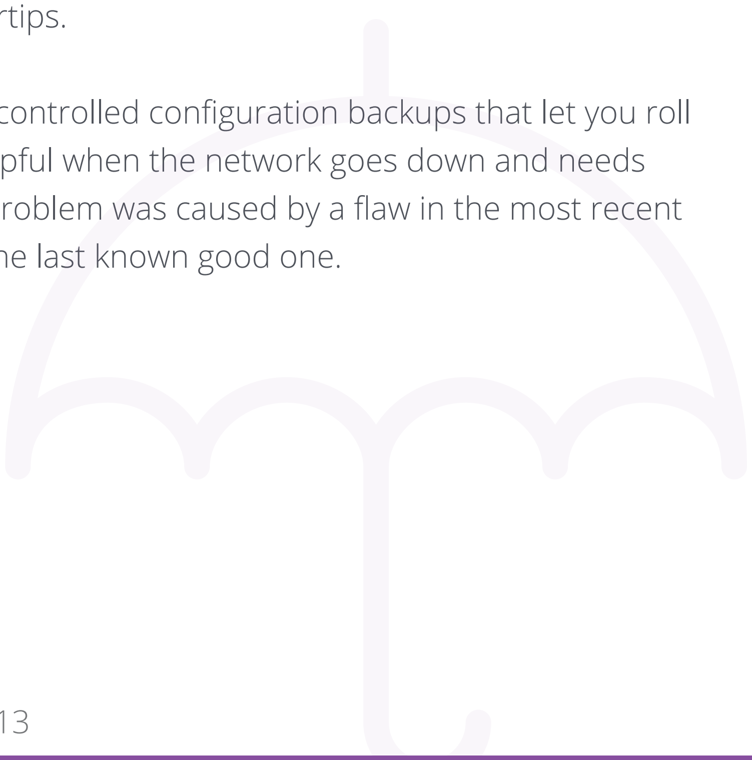
---

network continuity

- **Accurate, detailed, and up-to-date network documentation.** The last thing you want to be doing when disaster strikes a client's network is struggling to figure out how devices are supposed to operate.

- **Configuration back-ups.** Many MSPs are quick to think about backing up data but are less rigorous when it comes to backing up network devices. Device backups tend to be on a periodic schedule (say, once a month), and your technicians have to remember to do it and take the time to do it. There are lots of places where the process can fall down. Much better to use an automated system that continually does infrastructure backups for you, ensuring that if you need to bring devices back online quickly, you have exactly the information you require at your fingertips.

- **Configuration restore.** Having version-controlled configuration backups that let you roll back to an earlier config is immensely helpful when the network goes down and needs to be restored quickly—especially if the problem was caused by a flaw in the most recent configuration and you want to revert to the last known good one.



“If integration isn’t there, you lose speed and the ability to quickly respond to your customers’ needs.”

- **Randy Mott**, CIO, General Motors

#5: INTEGRATED WORKFLOWS

So your processes are as efficient as possible

Just as devices have proliferated within an office, so has software. There are literally hundreds, if not thousands, of tools and systems you, as an MSP, can choose from when deciding how you’ll run your business.

Realistically, you’ll use a dozen or more different ones to handle different tasks such as accounting, quoting, ticketing, messaging, desktop management, network operations, and more.

If those apps and systems are siloed, with no integration between them, you’ve got an efficiency problem on your hands.

It’s much smarter to choose products that have hooks into complementary products. Integration helps you avoid task duplication, and ensures workflows are as quick and smooth as possible.

Bottom line, it’s all about your bottom line. Process and workflow efficiencies help boost profitability; siloed systems eat away at profitability.

Here are some ways you can take advantage of platform integration:

- Sync your ticketing system with your network alerting and monitoring tools.
- Sync your messaging and pager apps with your network alerting system.
- Sync inventory and configuration details between your business platform and your network operations system.

- Sync your access control tools with your help desk software so you don’t have to store credentials in more than one place.
- Sync your reports on network performance with metrics from the rest of your business
- Adopt cloud-based tools that are platform-agnostic and work from whichever system a staff members chooses to run.

"Reporting is that tangible weekly or monthly reminder to the clients on why they are forking over that monthly fee."

- **Brian Dosal**, BrightGauge

#6: REPORTING

So you can demonstrate your value

The MSP market is a crowded one. There's no shortage of competition, as you're all too well aware. If you want to gain new customers and keep them, numbers-based visibility and accountability are essential.

"MSPs build trust with customers and prospects by providing transparency," writes Michael Brown of MSPmentor. "Merely claiming your services are secure and reliable isn't enough. Transparency gives customers information about not just what you can promise, but also how you're going to fulfill that promise."

Strong reporting tools are a must. Producing benchmarks and performance metrics about your services can quantify the value you're providing and how your value increases over time.

Device downtime decreased by 20%, resulting in 40% fewer tickets for downtime. Network availability increased by 8%, resulting in 18% fewer tickets for that.

That's the kind of data to share with your customers so they remain confident in their decision to keep working with you.

Reporting also delivers value by empowering you to make proactive recommendations, backed by hard data, about infrastructure and service upgrades. For example, a monthly report with minimum, maximum, and average figures on things like disk utilization, network bandwidth, and CPU time helps you point out where new hardware purchases and network upgrades will help the customer avoid performance issues down the line.

In turn, by ensuring customers know when to increase bandwidth capacity, links, disk space and other resources to prevent overload, your reports actually make your job easier, because the networks you're managing are healthier.

Effective reporting also entails communicating data to customers in clear, easy-to-read ways. As reporting firm M&E Studies notes, “If reports are reader-friendly, they are likely to be read, remembered, and acted upon.”

Since not all readers are the same, being reader-friendly requires the ability to tailor each report to the customer receiving it. Instead of taking a one-report-fits-all approach, be sure you can export report data into whichever format you require.

Make sure you can also customize the data you export when creating a report. You should have the freedom to pull information from any range of dates and any dashboard, then turn it into a report to share with clients.

> *"Staffing costs are usually an MSP's biggest expense. Having a good grasp of these costs can make the difference between your company turning a healthy profit or barely breaking even."*
>
> - **Scott Calonico**, MSP Business Management

#7: NETWORK EXPERTISE

So you can deliver top-notch service

The final component of a profitable managed network service, network expertise, is not only the hardest to acquire, but also the most costly.

Expertise is expensive because good technicians require high salaries. According to Taylor Business Group, technicians earn an average of $70,000 per year. With benefits and payroll taxes factored in, their total annual cost to the MSP reaches $88,000.

That's a lot of money. It's especially dear when you consider that the expected utilization for a service technician is 75 percent, meaning MSPs only make money off a technician's work 75 percent of the time.

Faced with the high cost of expertise, service providers who want to stay in business and grow need to find a way to keep staff costs under control.

Traditionally, network management has been very manual and very time-consuming. That doesn't scale. So how do you scale network operations cost-effectively? Automation. You must automate rather than growing your team.

Automation multiplies the impact of your staff. It lets a single tech manage many networks. Instead of tracing wires and mapping ports by hand, or logging into the CLI to hunt for a potential issue, technicians can quickly know what they're looking at and how to deal with it.

That's not all. Automation improves the efficiency of your workload allocation. It can help L1 and L2 technicians, who cost less, complete tasks that would otherwise have to be performed by higher-paid L3 techs or even senior management.

Meanwhile, with the right software resources on their side, your senior staff can spend their time on big-picture items, like planning network expansions and consulting with clients, instead of performing more mundane networking chores.

That’s better for everyone. You get more bang for the bucks you spend on salary. Your clients get better service. And your techs spend their time doing things that are best matched to their skills and seniority.

TL;DR SUMMARY

Businesses need efficient, reliable networks to make money. As a managed service provider, you deliver that vital resource to your clients.

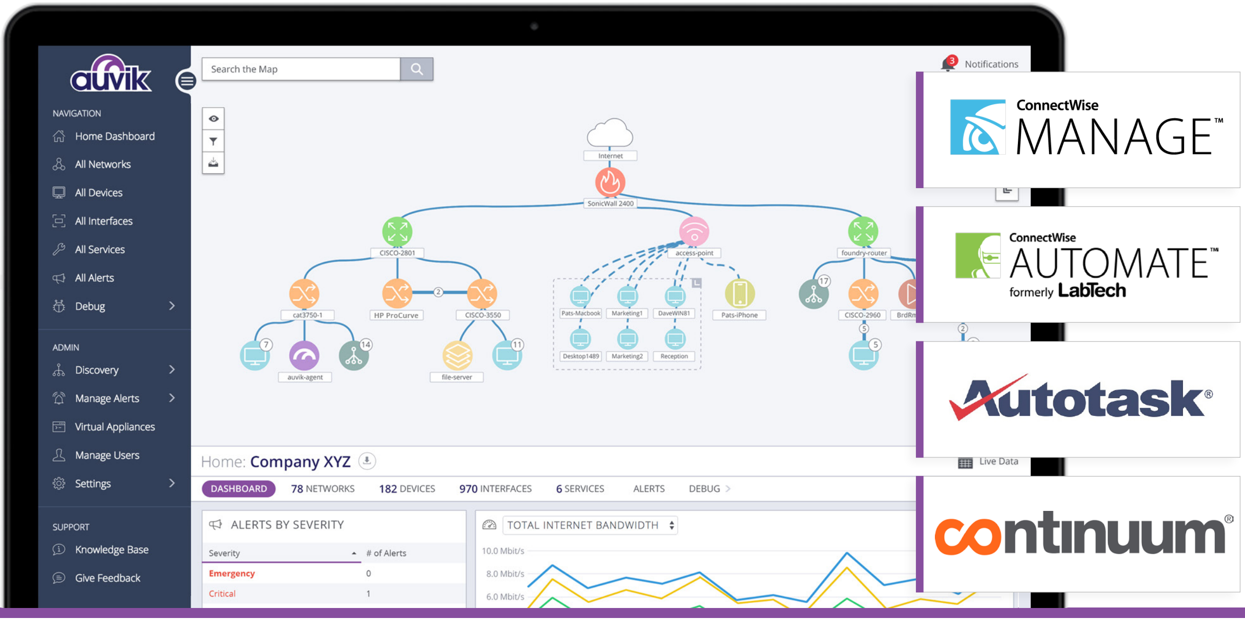
But traditional network management isn't enough. To deliver outstanding value, stand out in a crowded MSP market, bring in more revenue, and boost profitability, approach network operations as a discipline.

That means incorporating these seven components into your managed network service:

1. Know your clients' unique business and networking needs—even if they don't fully understand them themselves.
2. Provide real-time network awareness so you know what's happening on client networks at all times.
3. Manage user access and client device credentials in a way that's secure and compliant.
4. Deliver network continuity by heading problems off at the pass and restoring service quickly when disaster strikes. Pick up as close as possible to where things were when the network broke.
5. Integrate your systems so your employees can work as efficiently as possible.
6. Leverage reporting to demonstrate your value to clients, and assure visibility and accountability.
7. Hire or acquire the right staff so you've got the network expertise to get the job done. Support your staff with automation tools to get the most bang for your buck at each salary tier.

> *"Managed services is all about operating as efficiently as possible, controlling expenses while maximizing revenue. The end result can be fantastic profit margins."*
>
> \- **Mike Monocello**, Business Solutions magazine

See and manage the whole network, not just endpoints



Severity	# of Alerts
Emergency	0
Critical	1

USE AUVIK'S RMM FOR NETWORK INFRASTRUCTURE TO:

- ✓ Differentiate yourself in a crowded service provider market by actively managing network infrastructure, as well as servers and endpoints.
- ✓ Deliver fully on client expectations for network management and performance.
- ✓ See and know everything happening on a client network in real-time—including the gear clients don't tell you about.
- ✓ Save time and money with Auvik's automation of complex network monitoring and documentation tasks.
- ✓ Integrate smoothly with tools you already use, like ConnectWise, Autotask, and Freshdesk.

Take a video tour through Auvik's main features today: bit.ly/AuvikTour

www.auvik.com