Auvik

Building a modern educational IT network

Ebook

Introduction

Education and IT leaders are united in a call to action: it's time to modernize educational institutions to meet today's digital pressures head on. It's a great rallying cry, but what does it really mean to prepare IT organizations for a future wrought with hybrid approaches to digital transformation?

Education leaders are responding to these shifts with flexible networks, modernizing their infrastructure and reimagining what it means to design, build, and maintain their networks— the backbone of today's learning environment.

This guide is meant to help IT leaders, network engineers, and teams discover how to take advantage of best practices, automation, and modern management tools to simplify the job and transform the networks powering today's educational institutions to meet today's digital demands.

Table of contents

Meeting today's challenges

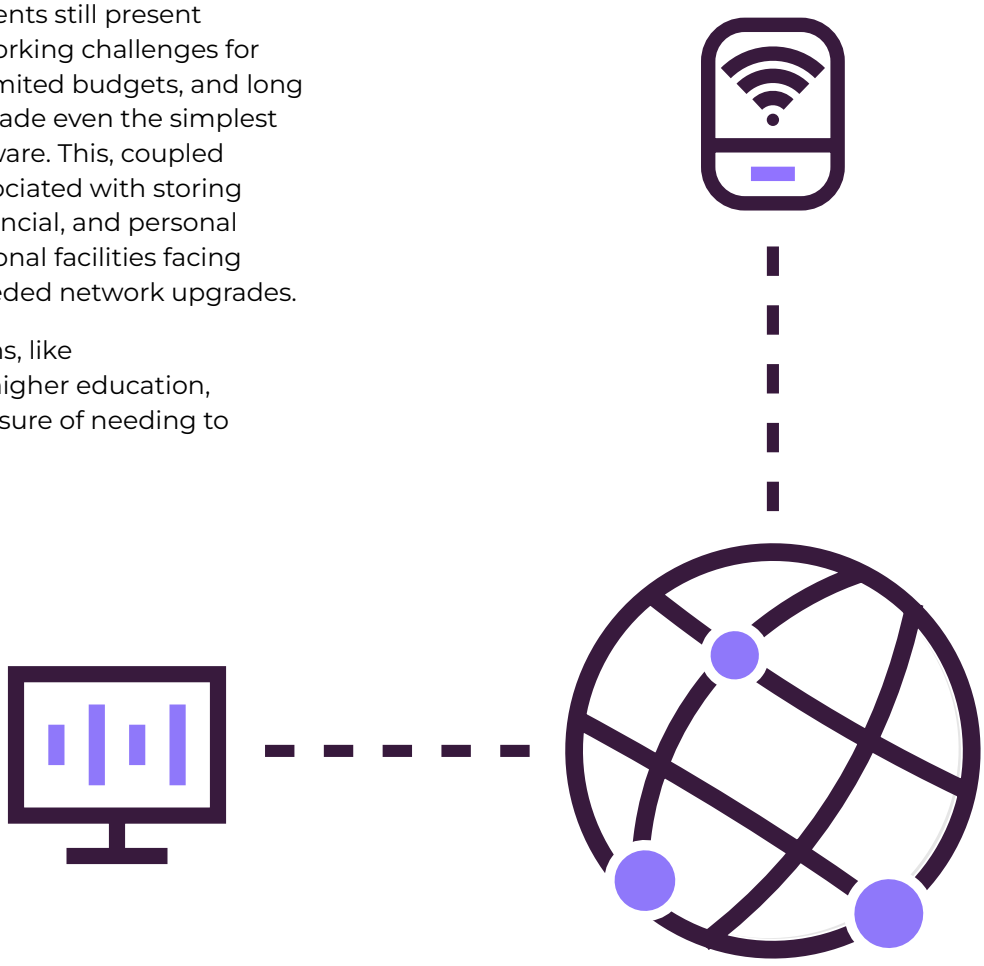
Technology lies at the heart of the modern education sector. It's breaking down traditional barriers, providing staff and students the ability to access learning from almost anywhere. Online services from digital textbooks, courses, and other transformational tools have become the standard.

The recent shift to remote teaching during the COVID-19 pandemic has forced education facilities to rapidly adjust and invest heavily in technology to enable necessary digital operations. The pandemic has also forced organizations to reassess their approach to managing the network. Network analytics, automation, and security all became heightened priorities. Knowing the detailed status of network conditions and components in real-time has become a vital requirement.

That being said, these shifts are far from complete. Today's education environments still present significant and unique networking challenges for the IT team. Those include limited budgets, and long evaluation processes to upgrade even the simplest pieces of equipment or software. This, coupled with the increasing risks associated with storing and managing sensitive, financial, and personal information, has left educational facilities facing difficult barriers to sorely needed network upgrades.

Some educational institutions, like private/charter schools and higher education, also have the additional pressure of needing to remain competitive in order to attract enrollment. If they don't provide a solid infrastructure, at a high performing level, they may lose potential students, funding dollars, or even face reputational risks.

Poorly managed networks lead to reduced or lost access to educational service delivery, which given the reliance on digital learning tools, leaves both teachers and students behind. Given the unprecedented digital shifts caused by the COVID-19 pandemic, connectivity within the education sector has emerged as critical components to online learning. Simply put, teaching and learning is directly affected by the quality and availability of your connection to the network.



What does a perfect network look like?

Industry analysts believe the primary focus for education leaders moving forward should be on streamlining operations, understanding organizational performance, and encouraging communication and engagement between students, faculty, and staff within digital environments.

To govern those expectations, network considerations should include:

Deployment and procurement

What does it mean to grow the network, build better infrastructure to meet demands, and manage it all within the confines of a limited budget?

Device onboarding (think mobility)

The sheer number and variety of Wi-Fi devices students bring to a university or college campus continues to grow exponentially. Smartphones, tablets, laptops, gaming devices, and streaming media players—all demanding flawless connectivity. In addition, IT teams are deploying wireless IP phones for better communications, IP video cameras to enhance physical security, and sensors for a more efficient environment.

Network performance and campus coverage

How do you establish a baseline and work towards a better future state? You must have clear visibility of your current network capacities before you can begin mapping out where you need to be, and the stepping stones necessary to get there.

Proactive management and analytics

What does it mean to support the entire organization? Plan, build, secure, monitor, remediate, and grow towards the future. Grasping deeper knowledge of all areas of the business helps from a reporting and transparency standpoint. Analytics can help initiatives where KPIs and measurements are necessary to present value for future budgetary requests.

IT operational simplicity

Tools and resources that offer visibility and proactive monitoring and maintenance simplify the job of managing the network for school IT administrators. Being able to rely upon automation to conduct things like remediation when issues arise, automated backups, config management, baseline performance monitoring, etc., are the difference between a stressed out IT department and one that runs efficiently and effectively.

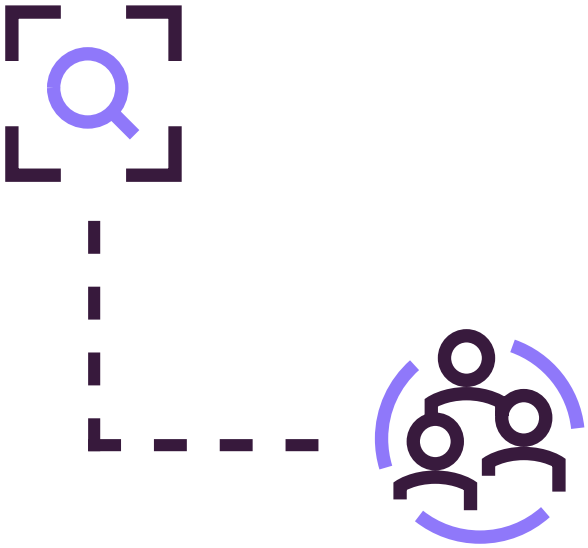
End-user training

Don't forget your users! These are students, staff, and enterprise level administration that will look to the IT department for education on the latest SaaS-based applications, troubleshoot Wi-Fi connectivity issues and keep all the organizational and student data secure.

Questions to consider during the discovery phase with your organization:

- What is your institution's vision for learning that technology needs to support?
- Are there digital learning content, tools, and resources that will need to be supported?
- What types of devices will be supported?
- What is your current state of your physical infrastructure and network capacity?
- Is Wi-Fi a priority across campus?
- Does your network need to be IoT friendly?
- Is there professional development or cybersecurity awareness that users will need in order to be proficient with any new digital learning enhancements?
- What resources are available to fund this transition?
- Will we outsource? If so, what areas of IT can be outsourced?

Feedback from all areas of the business will be crucial for planning for the future.



How do you get there from here?

Start with a network assessment

Be proactive! Write down your goals and define your targets. Discuss with leadership about where the network needs to be, and what business requirements it has to support. Address their questions and document known gaps. Create a vision board. Whatever helps you be creative and motivated. Understanding where your organization wants to go will assist in better planning. Remember, the campus network you're building is the foundation that will help the school meet current and future education requirements more easily.

Start your journey with an assessment. Assessments bring awareness of the existing infrastructure, and usually include a general understanding of the network topology by mapping the network infrastructure, documenting access needs for students, faculty, and the enterprise as a whole, recording where data is stored, reviewing disaster recovery and backup plans, and recording technical details to outline the existing environment.

Assessments also help to establish a performance and capacity baseline. For example, reassess existing WLAN infrastructure and conduct performance testing to ensure mobile devices and bandwidth hungry SaaS-based applications do not cause bottlenecks. Knowing where you are is a necessary starting point to getting to where you need to be. Understanding the limits of the existing network opens the door to better network management.

Work to document existing infrastructure and identify outdated hardware that may be holding you back. These are the planning processes that help admins and engineers deliver a high-performing network.

For schools, it's important for all the devices coming off and on the network receive their share of network resources. Software defined networking (SDN) is a network architecture approach that enables the network to be intelligently and centrally controlled, helping network administrators close gaps with connectivity and onboarding over wired and wireless networks.

The modern schools of today are increasing Wi-Fi infrastructures to increase capacity and efficiency of access for optimum speed and performance. It's what users have come to expect—connect anywhere and anytime.

To achieve these high standards for wireless connectivity, school network administrators should plot their Wi-Fi capacity and coverage, and align it with high-traffic access points. Using a Wi-Fi heat mapper to highlight areas for best frequency may help to benefit administrators looking to expand Wi-Fi coverage across the campus.

If your school's digital transformation includes smart buildings or other facilities and locations outfitted with sensors as part of the network, consider an IoT gateway. Like a router, IoT gateways allow users to manage the many IoT devices making their way onto a given network. They translate the myriad of sensor protocols and forward the data to the appropriate destination for processing. IoT gateways manage and support the advancing array of wireless protocols that new devices and applications require. Schools and universities can also use IoT gateways for additional real-time network security protection, as IoT devices are notoriously unsecure in their design.

TIP:
Education networks need major wireless capacity

Keep it simple to start

Mapping the network, maintaining an up-to-date device inventory, and maintaining a centralized config backup repository are all basic practices to help maintain an optimized network. Then, look to simplify operations through insight, automation, and unified monitoring. And don't forget to incorporate comprehensive security at every level of the network for users, devices, and their applications.

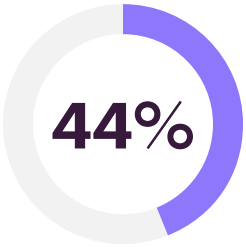
Look for tools to provide a single-pane-of-glass view into the entire to establish a holistic, full life cycle management solution for the network. With the right network monitoring and management system, you can bring together disparate networks and IT operations under one tool to easily stay ahead of common issues before they become critical emergencies.

Consider security, compliance, and data privacy

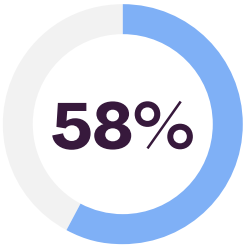
Security is, of course, a major concern among education administrators, and one of the biggest challenges facing schools today. Whether it's BYOD policies, remote access for off-site users, or reuse of passwords by students and staff, IT professionals in the education sector face down a huge number of vulnerabilities in order to maintain the integrity of the digital network. It should come as no surprise that securing students' data, and ensuring compliance with federal and state cybersecurity regulations, requires a complex approach.

If we think about it, an educational institution's technical resources are worthless without a secured infrastructure. Data security and user privacy is of utmost importance, and an organization's reputation is on the line where security breaches are concerned. Therefore, implementation of better security and disaster recovery practices should be embraced from the top down. This will ensure adoption is comprehensive across all areas of the school.

Key findings by Sophos State of Ransomware in Education 2021 report showed:



of organizations were hit by ransomware in the last year



of organizations hit by ransomware said the cybercriminals succeeded in encrypting their data

of those whose data was encrypted paid the ransom to get their data back

The average ransom payment was US $112,435

Those are startling statistics when you consider education budgets are already constrained. The report concludes, "The total bill for rectifying a ransomware attack in the education sector, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was, on average, US$2.73 million–the highest across all sectors surveyed."

Findings like the above are reasons enough that IT leaders are so concerned, and why security is always "top of mind". This puts additional strains on internal departments to react, often without the fiscal resources to overhaul existing systems and infrastructures to meet these ever-evolving threats.

A duty to disclose

Schools and districts have an obligation to communicate what kind of student data the school and/or third parties are collecting, and how that data is going to be used. The following are just a few examples of federal laws outlining requirements educational institutions must adhere to.

- **The Family Educational Rights and Privacy Act (FERPA)** is a federal law that affords parents the right to inspect and review their children's education records, the right to seek to have the education records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years of age or attends a postsecondary education institution at any age, thereby becoming an "eligible student," the parent's rights under FERPA transfer to the student.
- **The Protection of Pupil Rights Amendment (PPRA)** is a federal law that governs what information can be collected from students in certain surveys, analyses, and evaluations as part of programs administered by the U.S. Department of Education. For instance, students may not be required, as part of an applicable program and without prior written consent, to take any survey, analysis, or evaluation that reveals information concerning one or more of eight protected areas, including, but not limited to, behaviors and attitudes, and illegal, anti-social, self-incriminating, or demeaning behavior.
- **The Children's Online Privacy Protection Act (COPPA)** governs online collection of personal information from children under age 13. For example, before a developer can collect any information from a student under 13, verifiable parental consent is required. The FTC, which enforces COPPA, has said that school officials can act in the capacity of a parent to provide consent to sign students up for online educational programs at school for the use and benefit of the school, and for no other commercial purpose.

Hackers are increasingly targeting schools because those networks contain valuable data and may be relatively easy to access. With outdated infrastructure and so many points of ingress, these networks are often vulnerable to bad actors.

The following are three best practice approaches for which network leaders are changing the way they think about securing both student data and the network itself:

1. **Network segmentation**
   Give users access to only the areas of the network they need for their job. User access rights should be a requirement, and part of the discovery and network planning process. By segmenting your network, it makes it much more difficult for unauthorized users or bad actors to breach and gain access to the entire network.
2. **Enable filtering for IPs and monitor internet traffic**
   This is an additional security layer which helps to lock down traffic that has been authorized. This will require much effort up front and require tedious maintenance but is a sure indicator of a solid security plan. With security, it's best to layer it on and this is just added comfort.
3. **Develop and maintain policies for unsecured devices (BYOD) and terms of use for users**
   This should also include items like cybersecurity awareness and training for all users. Policies and training practices can help to protect the entity from means of which are often out of the IT department's control.

> "With free Wi-Fi in school buildings and a generation of students glued to their smartphones, there are thousands of opportunities for a hacker to gain access to a school network. Students downloading free apps on their phones or hopping from one school computer to the next can spread a computer virus faster than the flu during flu season."
>
> **–K-12 Education Networking Guide**

Building out your security plan

It's important to work with all areas of the company to develop a comprehensive security plan. This plan should take into consideration the management of security risk, incident response, and disaster recovery for people, process, and technology. An in-depth review of assets, and addressing environmental threats, will also help to enhance your comprehensive analysis. Ensure to a process that requires regular reviews and on a consistent basis. Just because you establish and formalize a security/disaster recovery plan doesn't mean the task is complete.

We recommend the following key processes to consider when building your security plan:

1. **Asset identification**
   This is essentially taking a basic inventory of all the school's assets. This first step can be daunting, as it may seem there is a lot to uncover— especially with multiple campuses, storage, and offsite locations. Start by grouping assets by category and threat potential. Ask yourself, "which assets of ours are the most valuable and probably of more interest to thieves?" Having visibility into your network infrastructure will be especially helpful in identifying data sources, clarifying user access, and updating policy. It will be crucial for education network administrators to review and provide a detailed technology assessment during this phase.

2. **Uncover vulnerabilities and existing gaps**
   Of the assets discovered in the first step, document all possible threats—including environmental (like natural disasters). Any possible downtime, whether it's on-prem, or associated with cloud-based applications, will be an important inclusion in this step. After all, downtime is a very real threat when we consider user access and reliance on cloud vendors to provide service.

3. **Determine "probability and priority"**
   Mapping the likelihood of threats to known assets will help prioritize proactive and reactive actions should that situation occur. Establish a scale (thinking DEFCON levels here) where threat stages equate to degrees of tolerance by the organization. This will also help to map appropriate responses based on each ranking. Address and retain. Work with the enterprise leaders to close discovered gaps. Record threat classifications and response, and finalize your security and disaster strategy. Document. Document. Document. Make prevention a priority. A systematic approach to establishing and implementing user training, access policy, and technology maintenance is critical in all modern work environments. These are the continued efforts required to prevent and maintain your organization's risk tolerance.

Ultimately, your security and disaster recovery plan should define your educational institution's tolerance for risk.It should outline efforts needed for best outcomes to mitigate, accept, and respond. Protecting your organization's gold, its information and access, is ultimately the goal of your security and disaster recovery process.

Level up your network plan

After your initial network assessment, and uncovering your security and data privacy needs, it's time to either initiate your network plan, or modernize your existing one. Outlining your needs and priorities in these areas will help guide you through the planning process.

To get started, consider how important the following components are to your goals of building a new network plan:

- Network management and monitoring systems
- User help desk and technical support
- Lifecycle support and upgrades to hardware (Insurance and licensing costs should be here as well)
- Budgets to support network capacity planning
- SaaS-based applications for digital learning content (don't forget licensing fees)
- SDN and future tech (analytics/automation)
- Security solutions for end points and firewall policy
- Network redundancy
- Back-up and disaster recovery plans
- Staff and user training
- Cybersecurity education
- Use of open standards to ensure interoperability with other learning networks
- Outsourcing opportunities

New technologies that are driving network design

Let's talk about a few key networking technology trends that are transforming the way administrators plan for, build and manage the digital networks of tomorrow.

Want to deliver high performance access and reliability while maintaining the school budget? Our **education sector hub** focuses on techniques network administrators in the industry can optimize the digital learning experience for students, without breaking the bank.

Pervasive connectivity. Pervasive computing combines existing network technologies with new, emerging ones like 5G, software-defined networking (SDN), network function virtualization (NFV), artificial intelligence (AI), and blockchain to empower connectivity that is unobtrusive and always available. These new advanced flexible networks offer trustworthy connectivity as the foundational component for an effective learning environment. Students and teachers cannot connect and engage globally, or leverage high-quality learning resources, without consistent and reliable access to the internet.

Video content and virtual classrooms. Harness network speed and implement control measures, like software defined networking, which intelligently directs traffic across the WAN and directly to trusted SaaS and IaaS providers.

Access to high-quality content. Students today need access to digital learning tools that give them the ability to curate and share learning materials. These new functions for learning and teaching applications will be an important component of a robust infrastructure for tomorrow.

Device policy and protection. If your organization provides devices directly to students, selecting appropriate devices depends largely on the age of the student, individual learning needs, and the types of learning activities. BYOD policies that allow the use of personal devices in the classroom should be thoroughly outlined and communicated through end-user training. It should be noted with BYOD, there are digital fairness considerations as well.

Responsible Use Policies (RUP), also known as Acceptable Use Policy, work to promote proper, responsible, and acceptable use of the school's internet connection. This "do no harm" policy helps unite users to protect the data privacy of the organization as a whole.

A RUP is a written agreement among parents, students, and school personnel that outlines the terms of responsible use and consequences for misuse. Best practice considerations for creating and establishing RUP in your educational organization are as follows:

- Discuss broadband access to the internet and adequate wireless connectivity, with a special focus on equality of access outside of the school environment. This highlights a previous suggestion for mention of BYOD policies.
- Discuss what it means to have a sustainable network infrastructure. Address concerns like upgrades of wired and wireless access as well as device refresh plans and sustainable funding sources while ensuring the safety and protection of student data.
- Map device connectivity and database alignment, highlight access types, and explain the use of openly-licensed resources. Transparency into end-user use is the goal.
- Include cybersafety and cybersecurity training for students, teachers and parents as part of district and school Internet use.

New measurements for success

How will you know when you are meeting the goals for the organization? With new trends in usage, design and overall network capacity, what are some modern metrics and KPIs to consider?

- **RTT.** Round Trip Time is an important metric to measure network performance, latency and packet loss. It can help to identify network performance issues across a number of vectors, including traffic bottlenecks, hardware issues, misconfigurations, and routing issues.
- **Uptime.** Availability and connectivity are key contributors to this metric. While you cannot guarantee 100% uptime, you can plan for a very close percentage to this by proactively selecting vendors, platforms, and tools that IT can monitor, measure, and quickly remediate should an outage occur.
- **Device health.** Measure the key indicators of the health of physical and virtual devices living on your network. Things like availability, CPU, memory and disk usage, and temperature can function as early warning signs of an overtaxed network . Coupled with asset documentation on things like maker, model, firmware versions, etc. you begin to shift network health towards a preventative process, instead of a reactive troubleshooting exercise.
- **Flow.** SNMP methods and polling can help administrators determine things like bandwidth capacity and utilization by analyzing throughput and network traffic flow.

There's a lot to unravel, but when IT teams put proactive plans in place for the networks, it helps the entire educational facility meet current and future requirements more easily.

How we can help

Auvik's network monitoring and management system is perfectly suited to solve the challenges faced by IT teams at educational institutions. Auvik provides you the tools to proactively monitor your network with insight and true visibility, no matter how it's designed.

See your network in real time, all the time

Know exactly what's on the network and how it's all connected in real-time. We do this by pulling from data from sources like CDP, LLDP, and forwarding tables to meticulously model the Layer 1 network diagram. Layers 2 and 3 are built from ARP tables, IP assignments, and VLAN associations. Whether it's a classroom lab, or an army of Wi-Fi devices, Auvik will show you exactly what's on the network, where it is, and how it's connected.

Track down where your capacity is going

Want an in-depth analysis of your users and where they are going when they are connected to your network? Auvik TrafficInsights provides transparency into the flow of network traffic and allows administrators to seamlessly understand the unique peak times of use faced by educational networks. This is highly helpful when you need to identify which applications are being used and if they're business-critical. Auvik's TrafficInsights tool leverages machine learning and traffic classifications to display which applications and protocols—like Dropbox, Netflix, or Facetime— are using up the bulk of the network's bandwidth. All this will help you confidently make the case for network upgrades, expansions, and traffic shaping. Be confident when management asks why you need additional budgetary resources.

Make your documentation audit-proof

Facilitate documentation needs to support the growth of the network as future technology is onboarded into classrooms by finding any device on the network in seconds. Auvik's powerful search feature lets you zero in on specific VLANs or devices present in your network maps. Search easily by typing in the device name, type, vendor, network, interface name, IP address, or MAC address. Don't remember the exact device name or IP? The intelligent search field can help you narrow it down.

Walk back changes and recover from disaster with ease

Not using automation to enable backups for syslog and device configurations? We've got you covered. When a network device dies, or fat fingers mistakenly change a device configuration, you won't have to figure out what went wrong while your users fume without service. Compare, and export your configurations with ease! You can also export configs and apply them to new devices, helping you onboard while standardizing.

All your networks in one place

Easily manage every site you're responsible for, whether it's across the city, country, or globe with distributed site management functionality. Auvik is built from the ground up to manage multiple sites easily. If your educational facility is highly distributed, you can use our network map to see all network locations you're responsible for managing, or split and group your networks to best fit your team's responsibilities. Combined with Auvik's alert notifications, you can quickly see which sites are experiencing issues.

Conclusion

In today's educational institutions, network administrators have the power to engage and increase collaborative digital learning experiences for all. The network must address the needs of the entire organization. Develop a strategy and pursue your digital learning goals starting today! Modern educational technology has made great strides in lowering the barriers to equity and accessibility in learning. So, whether you are trying to start from the ground up, tackle existing network infrastructure, automate more, streamline network operations, or manage risk more effectively, a best in class network monitoring and management system can make a big impact. Digitally empower all users across your campus with a potent network plan—with best in class access to resources, experiences, tools, and information, setting everyone on the path to the best educational experiences possible.

Ready to see what Auvik can do for your network? It's time for some higher learning.

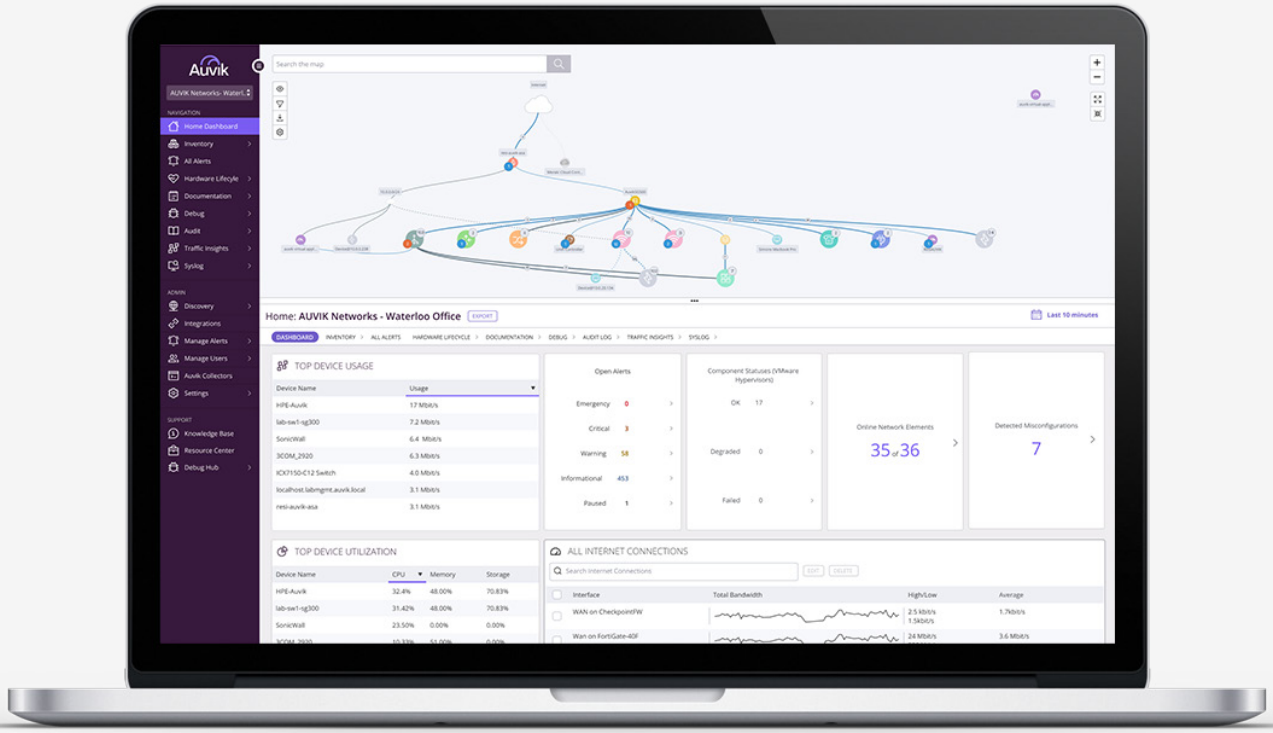
Sign up for your free trial today

1-866-59-AUVIK (28845) | North America

+44 800 368 7578 | UK & Europe

800 934 221 | Australia

800 854 898 | New Zealand



About Auvik

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.