helpsystems

ULTIMATE BUYER'S GUIDE

Network Monitoring Software in 2018

Table of Contents

GETTING STARTED

Using this Guide..... 3
Know the Trends..... 4
Understand the Benefits..... 6

DISCOVERING THE POSSIBILITIES

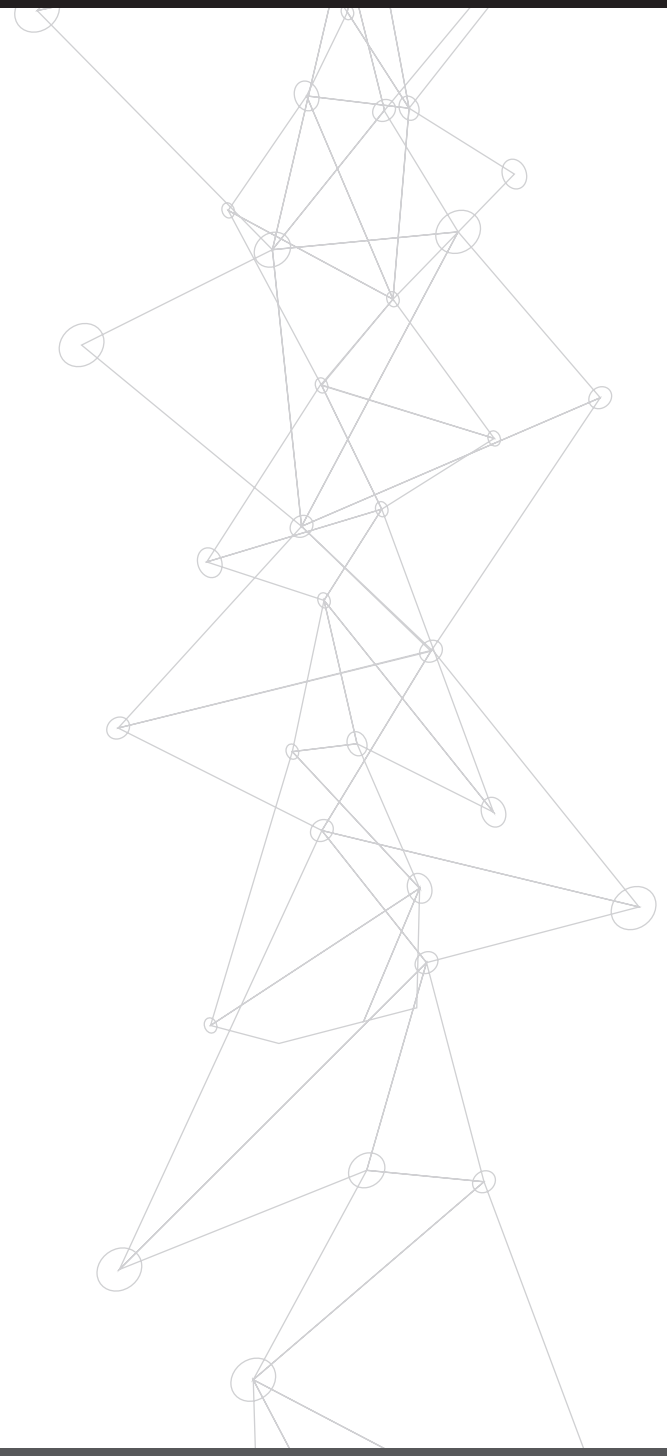
Consider Your Options..... 7
Identify Key Features..... 12

EVALUATING WHAT MATTERS

Create a Requirements List..... 13
Proving ROI..... 14
Determine Your Budget..... 17

RESEARCHING VENDORS

Find Trustworthy Reviews..... 18
Test Top Choices..... 19
Become a Partner..... 20



Using this Guide

Buying software can be a tedious process… **but it doesn't have to be.** An educated buyer can easily narrow the playing field with the right information.

Whatever your main responsibilities, whether that's systems or network administration, security, or general IT operations, this buyer's guide will help you determine **what criteria are most important** to your organization so you can knowledgeably navigate network monitoring solutions. In this guide, you'll find a **helpful summary of network monitoring trends, features, pricing models, and more.**

Take 15 minutes to review the valuable information in this guide. At the end, you'll be better equipped to choose the right tool—one that will help you **stay ahead of network issues and reduce the risk of downtime.** Got questions? I'm here to help. Please feel free to email me at kevin.jackson@helpsystems.com

Know the Trends

Whether you manage a small server room or a giant enterprise data center, modern networks are growing faster than ever. Choosing software solutions that can support your changing network is key.

Keep these trends in mind as you begin evaluating network monitoring software options.

THE ANALYST'S VIEW

[Network performance monitoring and diagnostics] solutions are key in helping I&O leaders support more complex technologies and services with network visibility, performance issue detection and root cause analysis. Vendors are innovating with cloud monitoring, support for software-defined environments and more flexible deployment models.

Summary of Gartner Magic Quadrant for Network Performance Monitoring and Diagnostics Report

Automation

As enterprises wake up to the benefits of automation, the number of IT and business processes they conduct manually is shrinking. Today, robotic process automation and centralized job scheduling help enterprises move faster than ever. Everything from network device discovery to remediation can be easily automated with software. Automation allows IT to spend more time on strategic projects, improves the availability of systems and networks, helps eliminate downtime, and reduces delays that inhibit efficiency.

SO WHAT?

Network monitoring is only half the solution. If your team can't automatically remediate problems, you risk costly downtime and unhappy customers the longer it takes your team to manually fix the issue. Look for network automation software that can detect outages and fix them immediately, without having to get any IT team members involved. When you know your software will not only alert you if technology fails, but automatically restart it, you can stay productive and sleep more soundly at night.

Cloud and Hybrid IT

The cloud is no longer just for startups. Hybrid IT environments (in which some resources are managed in-house while others are shifted to the cloud) are the new normal. As businesses adopt software-as-a-service and depend on the Internet more for daily operations, securing, monitoring, and managing cloud technologies will be essential.

SO WHAT?

Whether your routers, switches, and servers are mostly on-premises, or you're also running applications in Amazon Web Services (AWS) Microsoft Azure, Salesforce, or another cloud platform, you need visibility into your entire distributed IT infrastructure. Make sure you can map all your technology, monitor its availability, and automatically fix any failures.

As organizations consider public, private, and hybrid clouds for more cost-effective file storage, web hosting, backups, and other common IT initiatives, consider investing in a monitoring solution that gives you visibility no matter where your critical technology is hosted.

Server Virtualization

Server virtualization is the process of hiding physical server resources from users and dividing servers into multiple isolated virtual environments. Partitioning servers allows them to run their own operating systems. The many benefits of virtualization include the ability to save space, increase server efficiency, and cut costs by requiring less hardware.

SO WHAT?

Even if you don't have virtual servers today, it's very likely you will someday. Find a flexible network monitoring solution with the ability to map and monitor any kind of network technology, including both physical and virtual servers.

Know the Trends

Software-Defined Networking

For the past few years, software-defined networking—which allows IT to make changes to the network without changing the network's physical infrastructure—has been a hot topic. As organizations seek greater efficiency, flexibility, and cost savings, SDN offered a way to separate hardware from software and create more agile networks.

But while interest in SDN has grown, actual adoption by enterprises really hasn't, according to Gartner analysts. And while 20% of IT professionals say they are investigating SDN, only 11% noted it as a top priority this year, in a recent 2018 State of Infrastructure Survey.

SO WHAT?

All this talk around SDN has shifted the industry's focus from hardware to software. Even though SDN may not be the top trend to consider as you shop for software, I'd echo some advice Gartner analysts gave: instead of trying to find SDN-specific solutions, look for tools that give you greater automation, lower costs, and more network agility.

The Internet of Things

The world is shifting toward complete connectivity. Giving more devices IP access lets businesses gather real-time data in order to make smarter business decisions. It connects users with information they need. It also means IT has a larger inventory of devices to manage and monitor. According to an estimate by IHS, the IoT market will reach 75 billion devices by 2025.

SO WHAT?

As the number of devices with an IP address in your network increases, make sure your software can scale to monitor all of them.

Mobile Connectivity

It's no surprise that mobile connectivity is a ubiquitous workplace requirement. Bring your-own-device (BYOD) environments and remote working help employees stay connected and productive wherever they are. Increasing bandwidth will be a focus for many IT leaders in 2018, according to the 2018 State of Infrastructure study.

SO WHAT?

As time goes on, IT teams will only see mobility's importance grow. Providing ample bandwidth and smooth performance for every device that connects to the network is key. Network monitoring systems should allow you to monitor connected mobile devices and plan for future bandwidth needs.

Understand the Benefits

If you have a network, you need network monitoring. It's as simple as that. Otherwise, when network performance falters, you'll have no idea what's happening or how to fix it.

Long-term, lack of network visibility can lead to slow device performance, crashes, and costly outages—all of which negatively impact business productivity and the availability of your products and services.

Network monitoring software gives you the ability to:

Monitor your entire network

Auto-discover anything with an IP address, including physical and virtual equipment, so you have total visibility into the technology your organization relies on every day.

Enforce SLAs

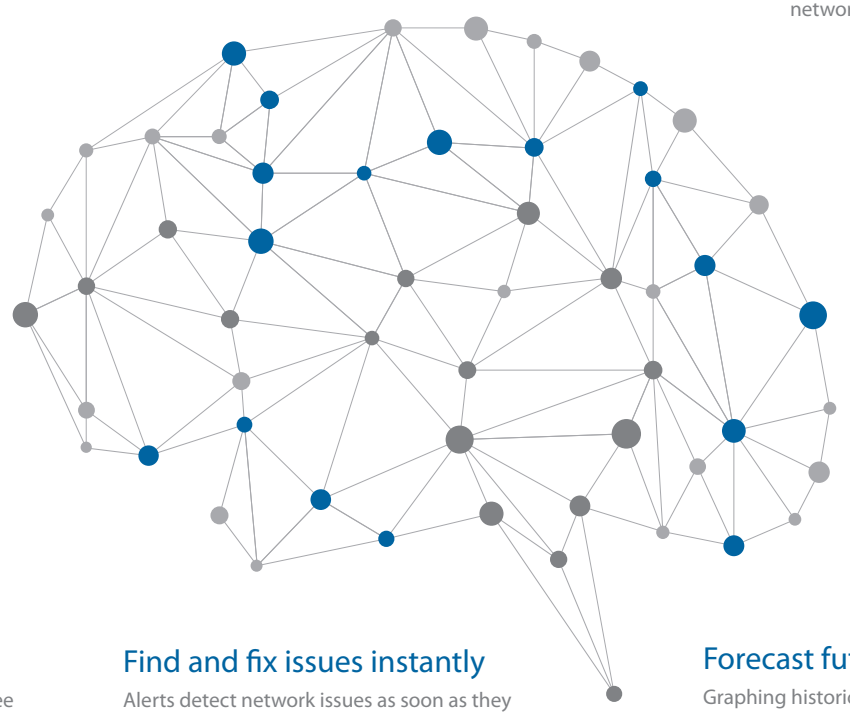
Keep customers happy and meet their service-level agreements (SLAs) with the help of real-time mapping, monitoring, and alerting.

Map your network

See devices on a floor plan or against a geographic map. Flexible mapping allows you to capture the network you see in your head and create it on the screen, choosing the layout, icons, and colors that make sense to you.

See how traffic is flowing across your network

Many network monitoring solutions offer bandwidth analysis capabilities to help you understand who and what is causing network spikes, for faster problem resolution.



Find and fix issues instantly

Alerts detect network issues as soon as they occur, and automation can fix them instantly without having to get employees involved.

Diagnose network health at a glance

With data on device statuses and traffic levels at your fingertips, you can rely on your software to show you how the network's performing now.

Know what "normal" looks like

Increased network visibility provides a baseline of day-to-day network performance, so that abnormal dips and spikes stand out.

Save time and money

Prevent costly outages and help IT work more efficiently, rather than manually monitoring and remediating network issues.

Forecast future network needs

Graphing historic traffic levels helps you accurately forecast future needs, like additional bandwidth or a hardware upgrade.

Consider Your Options

On-premise or cloud-based software? Free or paid? There are pros and cons to every option. Here's my take:

Management vs. monitoring

You will find network monitoring capabilities as part of both larger network management solutions as well as niche mapping and monitoring tools. What you choose will primarily depend on the features you need, your installation timeframe, and your budget.

Network management solutions go beyond simple monitoring capabilities to include additional features, from configuration, application, and server management to in-depth dashboards and reporting. Modules and add-ons expand the functionality of the product for an additional price. These solutions are feature-rich but tend to be expensive and present a steeper learning curve to users.

Network mapping and monitoring solution tend to be easier to deploy and manage. They offer tighter feature sets but richer core functionality. Because of their targeted focus, these solutions are usually less expensive.

TAKEAWAYS:

Large enterprises often prefer network management solutions for their expanded functionality, although specialized network mapping and monitoring tools can certainly be used to augment the features of a broader solution.

For organizations looking for a solution they can learn quickly and manage easily, a focused mapping/monitoring tool is a smart choice.

Consider Your Options

On premise vs. cloud-based

Do you want to install and manage your software on-site? Or would you rather host it in the cloud? With cloud-based technology becoming more common, you'll want to consider how much control you want (and need) over your network monitoring activities, and how comfortable you are with hosting data externally.

The biggest benefit to an on-premise solution is the control and customization it offers. Installing software on-site means you can configure it to meet your exact requirements and monitor data at the intervals you prefer. Cloud-based solutions don't offer the same level of control.

Because a managed service provider will take care of setup and configuration, cloud-based monitoring software is easier to start using—you just have to provide access to your network devices. It's also convenient, as you can log in from anywhere and on any device.

There are always security concerns when data is hosted in the cloud, as any breach to your hosting provider's system will expose your data. Additionally, you'll want to consider reliability and whether or not you're comfortable being at the mercy of a service provider if services become unavailable.

TAKEAWAYS:

While an investment in SaaS may appear lower than commercial software initially, after about three years the total cost of ownership for SaaS solutions, including migration costs, implementation costs, and costs for specialized enhancements or integrations, will often be higher than the cost of perpetual software licenses.

If easy access is what you need, many commercial solutions do offer web-based or mobile applications to provide anytime, anywhere software access. For IT teams who want to lower their TCO, maintain control over their solution, and keep data on site, an on-premise solution may be the better option. At the end of the day, it's about choosing the solution that best fits your organization's needs, today and in the future.

Consider Your Options

Open source vs. commercial

Free open source tools allow IT administrators with coding skills the ability to custom-configure software to do what they need it to.

The hidden risk of an open source tool is this: it will still cost you. Open source software can be time-intensive to set up and is not always user friendly.

Commercial tools will ultimately deliver more for your investment. Essential features are built right into the solution. They're typically user-friendly enough for a Level 1 technician to set up. Many offer free versions, with additional tiers available to provide high-quality support and regular software upgrades. If you're working with a limited budget but want the benefits of a commercial tool, consider trying a free commercial tool that offer additional value down the line.

TAKEAWAYS:

Open source tools are best for IT teams who can devote time and resources to customizing them.

If you need a tool that's quick and easy to set up, with a full feature set, scalability, and frequent product updates, a commercial tool will be the better choice.

And if you want support to help you fully utilize the tool and receive assistance when you need it, a commercial tool with world-class support is the way to go.

Consider Your Options

Agent vs. agentless

Every network monitoring tool uses either agents or protocols to monitor your IT infrastructure. Agent-based tools require an agent to be installed on every item you want to monitor. This gives the software the ability to collect data from those devices (endpoints). Agent-based software allows you to monitor any device on which you install an agent, providing comprehensive monitoring capabilities for virtual and cloud environments. Just be aware: agents must be upgraded simultaneously with devices, so they require more maintenance. Agents also have slightly more impact to network performance than probes.

Agentless tools use various protocols, such as SNMP, WMI, NetFlow, sFlow, etc. to gather traffic data. Agentless solutions offer an advantage in that they can communicate with non-standard or non-agent devices within your network. This allows for a more targeted monitoring approach, because you can access information that agents cannot. Since agentless software doesn't require extra installation or maintenance, the overhead and maintenance is generally low.

TAKEAWAYS:

For diverse, distributed IT environments where there isn't much co-dependency on the network, an agent-based solution may be most beneficial. For more homogenous, localized IT networks, an agentless solution may be a better fit.

Consider Your Options

Licensing models

Comparing software licensing models can be tricky. But understanding how licensing works is vital in order to accurately compare the value and cost of software options.

The three most common licensing models for network monitoring tools are by:

Number of devices.
This is the simplest licensing plan. No matter how many ports, interfaces, or monitors each device contains, your license will depend on the amount of devices (physical or virtual) you want to monitor. This model makes it easy to predict the implications of network growth on your budget.

Number of interfaces/ports.
When your devices have multiple interfaces/ports, you pay for a license on each interface in this model. The downside here is that it is harder to predict how many licenses you'll need as your network grows in size, and the costs can grow exponentially.

Active measurements/tests/sensors.
This model means that licensing is based on the number of active sensors you have. A sensor is any device component that you are monitoring, including one port, CPU load, network connection, etc. While this model offers a high degree of granularity, it can be complicated to measure, and harder to maintain and predict future costs.

TAKEAWAYS:

Per-device licensing is typically the most cost-effective and requires the least amount of work maintaining and updating licenses.

Typically, per-interface and per-measurement licensing are more expensive and more difficult to maintain for networks with a high degree of flux.

Identify Key Features

If you know what you need—and what you don't need—half the work of choosing the right tool is done. This core list includes the top functionalities most IT teams want in an effective and reliable network monitoring tool. Add any additional in the spaces provided.

- ☐ **Multi-vendor support**
  Since most IT environments aren't homogenous, it's important to have software that can support a variety of vendors, including Cisco, HP, Dell, and others.

- ☐ **Auto-discovery**
  The software should automatically poll your network and bring back a live inventory of your whole IT infrastructure, including physical and virtual devices.

- ☐ **Autotmation**
  Beyond basic monitoring, find software that can automate your network activities, such as detecting problems and automatically fixing them without getting a person involved.

- ☐ **Layer 2 and 3 visibility**
  Show interconnections between devices in order to troubleshoot the extent of network problems.

- ☐ **Customizable network map**
  The ability to change icons, move things around, and customize colors and backgrounds can make monitoring more intuitive for IT administrators.

- ☐ **Real-time monitoring**
  Your software should analyze common metrics like response time, uptime, availability, and CPU in real time.

- ☐ **NetFlow monitoring**
  Monitoring traffic bandwidth information provides a better understanding of who, what, and how traffic is flowing across the network for more effective troubleshooting.

- ☐ **Simple interface**
  User-friendliness is huge for time-strapped IT teams. Make sure the interface is easy to navigate and use.

- ☐ **Exception-based alerting**
  Alerts should notify you immediately when network issues occur and offer customization to eliminate false-positives. The ability to escalate messages and notify the team when problems are resolved or acknowledged is also helpful.

- ☐ **Reporting and dashboards**
  Having basic data analysis and reporting functionality is helpful for understanding network trends and capacity planning.

- ☐ **Easy deployment**
  Network monitoring software that is easy to configure and quick to get up and running yields ROI faster.

- ☐ **Remote monitoring**
  For IT teams who want to keep an eye on the network from home or work distributed across office locations, remote access functionality allows for anytime, anywhere monitoring.

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

In addition, make sure you have access to:

- ☐ Product manuals and documentation
- ☐ Expert technical support staff
- ☐ An engaged, active user community

Create a Requirements List

Your organization will have unique software requirements based on your IT environment, staff, and business priorities. Mark whether each item is "Required," "Optional," or "Not Needed." Add notes and additional requirements in the spaces marked "Other."

The ideal network monitoring software for our organization would:

Required	Optional	Not Needed	Feature
○	○	○	Monitor _____ routers
○	○	○	Monitor _____ servers
○	○	○	Monitor _____ firewalls
○	○	○	Monitor _____ workstations
○	○	○	Monitor _____ virtualized elements
○	○	○	Monitor _____ cloud applications
○	○	○	Monitor [other]: _____
○	○	○	Run on Windows
○	○	○	Run on Linux
○	○	○	Run on Mac/OS
○	○	○	Run on [other]: _____
○	○	○	Dynamically map the network
○	○	○	Provide end-to-end network discovery
○	○	○	Provide real-time responsiveness
○	○	○	Offer continuous, 24/7 monitoring
○	○	○	Provide useful notifications
○	○	○	Automatic network remediation
○	○	○	Remote monitoring and management
○	○	○	Be scalable for future network growth
○	○	○	Deploy at will
○	○	○	Be easy to use and maintain
○	○	○	Fit within my overall budget of $_____
○	○	○	Integrate with these network tools: _____
○	○	○	[Other:] _____
○	○	○	[Other:] _____
○	○	○	[Other:] _____
○	○	○	[Other:] _____

Proving ROI

Conducting day-to-day business without some kind of network monitoring system in place is incredibly risky. Very few businesses can operate without network availability. But realizing return on investment can take time. Part of the dilemma of quickly identifying cost savings relating to network monitoring is the nature of network monitoring itself. By detecting and resolving IT issues before they grow worse, it's tricky to estimate hard savings from disaster situations that never actually happened.

Because downtime has tangible and intangible effects, ROI is even more challenging to estimate. When a well-known brand's network fails, their market reputation, customer satisfaction, and employee morale will all be affected. Losses in these areas may be hard to put a dollar value to, but they can be costly nonetheless.

Ways to Save with Network Monitoring

Over the course of days, months, or years, network monitoring helps decrease:

- The amount of maintenance work your network requires
- The number of support calls you receive
- Time required to troubleshoot and monitor the network

By maximizing network availability over time, network monitoring helps increase:

- Revenue generation
- User productivity
- Customer and user satisfaction
- Employee morale

The Cost of Downtime

As businesses rely more and more on technology for daily business operations, avoiding downtime becomes more crucial. For organizations of any size, a loss in the availability of technology could result in high costs. One report estimated that the average hourly cost of an infrastructure failure is $100,000 per hour—but for critical applications, the potential hourly costs skyrocket to anywhere from $500,000 to $1 million.

A simple calculation to estimate the impact of downtime on your business is as follows:

Loss of revenue = (GR/TH) x I x H

In this calculation, each variable represents:

GR = ***gross yearly revenue***

TH = ***total yearly business hours***

I = ***percentage of impact***

H = ***number of hours of outages***

While the numbers will vary widely by industry and type of business, this simple calculation is a helpful place to start. If you can know the price of downtime, it's much easier to see the ROI of investing in preventative software solutions.

Example: Network Monitoring ROI for An Ecommerce Organization

Let's say you're a small ecommerce business making a gross yearly revenue of five million dollars. During the holiday season (November and December), you typically bring in 30% of your total yearly revenue. Considering that your website is available 24 hours a day online, you'd have potentially 1,464 available shopping hours over these two months.

How much could a 24-hour outage cost your business?

Loss of revenue = ($1,500,000 dollars/1,464 hours) x 1.6 x 24 hours = $39,344.26

Using the calculation above, a 24-hour outage could cost your business over $39,000 in revenue.

Now let's estimate the total cost of ownership for a network monitoring solution.

Say your business has a small network of 25 devices. You have two full-time IT employees. With a small IT team, you select a network monitoring solution that is intuitive and user-friendly, so it doesn't require another full-time employee to run it. To get up and running faster, you also purchase a small block of installation services.

Total costs:

Initial purchase: $550
First-year maintenance: $215
Installation/implementation services: $200
Training services: 0
Salaries of employees who will manage the solution: 0

Purchasing a network monitoring solution will result in a total cost of ownership of $965.

Further ROI could be achieved by:

- Re-allocating employees from manual monitoring to more strategic IT projects
- Higher morale and satisfaction from employees who no longer spend their day on manual activities
- Customers and employees reporting less network incidents
- Higher customer satisfaction with orders, shipping, and customer service
- IT spending less time troubleshooting network incidents
- Reduced downtime throughout the entire year
- Better network health and performance over time

While putting numbers to these factors requires a bit of imagination, spending less than $1,000 to potentially save thousands of dollars (plus all of the intangible benefits above) turns out to be a wise investment.

Determine Your Budget

Network monitoring software comes at all price points, from free software to a $50,000 or more commercial installation for unlimited enterprise monitoring.

How many devices do you have?

While some network monitoring software solutions are licensed based on the number of interfaces or sensors you want to monitor, most are licensed per device or node. Get a general ballpark of the total cost you should plan to pay based on number of devices in your network.

25-50 devices	$750 - $1,800
50-100 devices	$1,300 - $3,500
100-500 devices	$2,000 - $10,000
Unlimited devices	$5,000 - $60,000

Inquire about special discounts

Some vendors offer discounted software pricing for certain industries or business types, such as educators, non-profits, or government institutions. When requesting quotes, make sure to ask about any special discounts that may apply to you.

Other things to consider

As you're forming your budget, make sure to ask about:

Additional costs

Beyond the initial software licenses, find out what else is included in your investment, including:

- Software maintenance and support
- Installation/implementation services
- Training services
- Any necessary associated hardware or software upgrades

Subscription pricing

Some vendors offer software subscription packages, in which you only pay for what you want to monitor and renew annually. Subscription licensing provides faster time-to-value, which can be an attractive benefit to many.

Special discounts

Some vendors offer discounted software pricing for certain industries or business types, such as educators, non-profits, or government institutions. When requesting quotes, make sure to ask about any special discounts that may apply to you.

Find Trustworthy Reviews

Authentic software reviews help prove a vendor's credibility and allow you to compare your business needs and profile with those of real users.

Find honest user feedback at these software review sites:

G2 Crowd: Network Management Software
Capterra: Network Monitoring Software
IT Central Station: Network Monitoring Software
TrustRadius: Network Management & Monitoring Tools

Browse these discussions for more valuable insights from like-minded IT professionals:

Sysadmin or Networking subreddits
Server Fault
Spiceworks Community

Test Top Choices

One of the best ways to evaluate software options is to take advantage of free trials. Many vendors allow you to download the software and use its full functionality for a certain timeframe. Trying before buying helps you make sure that the software will meet your goals and determine what kind of learning curve is required to get started.

Here are seven tips to get the most out of your trial experience.

1. **Attend an expert feature demonstration** so you can ask questions about your own installation needs and make sure you're aware of all the features available to try out.

2. **Map your network.** Network mapping is a unique and intuitive way to see network performance in a glimpse. Knowing exactly what's on your network and how devices are connected is essential information for IT administrators. Keep in mind that mapping is an afterthought for some vendors, so make sure you test out the mapping functionality to ensure it has the sophistication you need.

3. **Have fun with customization,** including icons, backgrounds, and map and sub-map creation, to make the software work for you.

4. **Analyze your traffic flow** by setting up flows exporters to give you a closer look at how traffic is behaving across the network.

5. **Grow your expertise with complimentary educational resources.** Many vendors will share tips, invite you to webinars, and send guides and other best practice documentation. Take the opportunity to deepen your knowledge of network monitoring.

6. **Learn about add-on solutions that might expand your capabilities.** If you feel like key functionality is missing, ask—you may even be able to try out add-on products free as part of your trial.

7. **Call technical support at least once.** If you have access to support staff during your trial, get their help. If you're not having issues, contact them anyway. Support is a critical piece of the whole software experience. If you have a poor experience as a trial user, it doesn't bode well for your experience as a customer. On the flip side, attentive support during a trial is a positive sign for the type of relationship you're sure to have with the vendor as a customer.

Become a Partner

If you're a managed service provider, consultant, systems integrator, or software reseller, consider partnering with a network monitoring software vendor. As you evaluate solutions to enhance your portfolio, ask vendors these questions:

1. **Why should I partner with you?** Research the vendor to ensure their mission and business strategy align with your own. Finally, determine if the partner benefits you'll receive are competitive and the program is structured in a way that provides multiple ways to generate new business.

2. **What kind of discounts do you offer partners?** Find a network monitoring vendor who will give you a competitive discount on their product, provide additional discounts for new logo business, and offer greater benefits when you exceed a sales threshold.

3. **What will you do to get me sales-ready?** Whether that's providing technical expertise or thorough product training, make sure your vendor equips you to succeed. Also get an understanding of how long the typical partner onboarding process takes and what types of resources are available on their partner portal.

4. **What kind of marketing support do you provide?** Many vendors will work with you to define your go-to-market strategy and provide the tools you need to introduce the product to your customer install base. Pre-packaged marketing campaigns, for example, make it easy to generate demand for the solution even with minimal in-house marketing resources.

5. **What other solutions do you offer?** Your customers' requirements are constantly changing. Partnering with a vendor who offers a diverse, integrated profile gives you more opportunity to earn your customers' business over time.

Kevin Jackson

With over 16 years of expertise in IT infrastructure, consulting, and support, Kevin works with organizations to understand their technical and business needs in order to help them find solutions that can solve their problems. He is currently a technical solutions consultant at HelpSystems.

Previously, Kevin worked with IT firm Richard Fleishman & Associates as an IT technology design engineer and business analyst.

Email: kevin.jackson@helpsystems.com
Phone: +1 952-486-6847