



Up or Down? Considerations for Scaling IT Monitoring

1.888.624.4671 (US)
+1.651.204.9102 (INTL)
www.nagios.com

MAXIMIZING FLEXIBILITY AND PRODUCTIVITY WITH IT INFRASTRUCTURE MONITORING SOLUTIONS

As companies respond to their customers and the industry environment, IT departments must scale up or down appropriately.

There may be new devices and platforms to be monitored, sudden regulatory challenges and new vulnerabilities may require a different approach to monitoring. Read on to learn how to prepare your company to scale its IT monitoring, as well as key factors to consider.

Preparing to scale IT monitoring

Effectively scaling IT monitoring requires an IT monitoring solution that simplifies monitoring and accommodates increased or decreased bandwidth, depending on your needs.

In addition, IT leaders need to ensure the choices they make now prepare them for industry demands in the future. [Gartner predicts](#) that by 2025, "80 percent of enterprises will migrate entirely away from on-premise data centers" to "colocation, hosting, and the cloud."

When scaling IT monitoring, the key factors companies should consider are:

- Adding new devices
- Productivity
- Vulnerability and cybersecurity
- Reporting

When preparing to scale IT monitoring, consider solutions that automate manual processes (e.g., cloning and replication of templates) and come with advanced dashboards and reports for forecasting, planning, and executive consumption. The IT infrastructure monitoring solution should require less time from IT teams on manual tasks, speed up the adoption of the tool through an easy-to-use interface, and make it simple to add or remove items in the IT monitoring environment.

Adding new devices

As roles and departments change, new devices and apps are often required or acquired. For the IT department, this means new things to track and monitor. Since it can be challenging to know what devices your company will need in the future, IT monitoring solutions should be flexible enough to check the health of a wide variety of devices and platforms. If IT teams need to dedicate time to learning a new environment and figuring out the best way to start monitoring the new devices, they should work fast in order to keep on top of issues proactively. The team needs to collect data as soon as possible to predict trends, like resource overutilization. Effectively monitoring these devices can be the difference between proactive and reactive IT management.

When a solution can receive data from many device types, companies can centrally forecast what tools they will need in the future and add these new devices for monitoring when needed. In comparison, when you have an inflexible monitoring solution, companies face restrictions on which devices they can add. They also don't have the information necessary to forecast which tools they'll need. Sophisticated monitoring solutions allow companies to monitor any SNMP-enabled device. In these cases, the solution can both actively poll SNMP OIDs and act as an SNMP trap receiver.



Quickly add new devices with monitoring wizards

IT infrastructure monitoring tools should also make it easy to start monitoring new device types. Tools that use point-and-click wizards to set up new devices save IT teams valuable time not only because the set-up of these devices is quick and easy, but because they can [delegate the task to non-technical users](#).

Configuration wizards that bypass the need for users to understand complex configuration files **enable systems administrators to spend time working on things that require their advanced expertise**. Systems administrators, some of the most expensive resources at any organization, can pass simple tasks to less technical users and spend more time on enhancing their company's IT infrastructure. With point-and-click set up of new devices, companies get more value out of their systems administrators.

Consider the cost of new devices

Finding a solution that **does not have license-imposed limitations on services monitored** is a crucial factor when choosing a solution that can scale up or down with a company. Some solutions charge companies based on the number of services checked (e.g., CPU usage, port bandwidth, URL response code) while others charge on the number of hosts. When being charged based on services, companies often find themselves restricted in their monitoring because with each new service monitored, the cost increases. **IT monitoring solutions that charge based on the host give companies the flexibility to explore** what elements are essential for the company's successful monitoring.

Companies should also consider the technical limits of the IT monitoring solutions they consider implementing. Not all solutions are equal in this sense. Some solutions can't monitor all things at once, which restricts the scaling of IT monitoring. More powerful solutions without these limits don't restrict the number of items tracked, enabling flexible scaling that accommodates the monitoring of any new devices.

Related Reading: [When Free Infrastructure Monitoring Costs More than the Enterprise Version](#)

Productivity

IT teams are always striving for better productivity so they can increase the time spent on research and development to improve the company's IT infrastructure and decrease the time needed to respond to and correct issues or outages.

This balance becomes even more critical as companies grow and add new devices. IT infrastructure monitoring solutions should have features (like the point-and-click wizards mentioned before) built-in that not only increase productivity but enable your team to identify issues proactively instead of always reactively fixing issues.

Infrastructure monitoring should also enable users to use templates to indicate how frequently checks run on a device, how often re-checks run, and which users or groups need to be alerted of issues. [Automatic monitoring and alerting](#) identify problems before it's too late and notify the right people quickly. As the number of devices increase, so does the need for efficient and effective monitoring.



Increase productivity with automated monitoring & alerting

IT teams can **spend less time putting out fires and more time proactively working to prevent issues from arising when** using an IT infrastructure monitoring solution. These solutions enable users to set up reports that provide a view of historical device performance, trends, and real-time performance.

IT teams can quickly check these reports to see what isn't performing as it should be, rather than waiting for something to break or spending hours analyzing the raw data to assess performance. These performance reports help users quickly prioritize where they need to focus their work to prevent future outages.

If a team member can spot a trend that signals a future issue, they can spend a few minutes fixing the problem, instead of waiting for the device to fail. This proactive work saves valuable time that might otherwise require a visit to the server's site to repair the device. With an IT infrastructure monitoring solution, IT teams can access easy-to-read reports, spend more time improving the engineering of their IT environments, and less time responding to emergencies.

Quickly pinpoint issues when they arise

When failures do happen, some IT infrastructure monitoring solutions have features that allow administrators to [pinpoint the exact problem](#) and its location easily. These features save IT teams time that they would have had to spend sifting through complex command line configurations to figure out what's happening, where, and determining the best way to fix it — all while the device, server, or network is down.

As companies grow, their physical footprint often does too. An increased geographical footprint makes it necessary for growing companies to use an IT monitoring solution that quickly identifies issues and where they're happening. Productivity increases when IT teams have an infrastructure monitoring tool that reduces the time needed to troubleshoot.

Get Started with Nagios XI

BEGIN YOUR FREE TRIAL NOW

Vulnerability and cybersecurity

Cybersecurity has never been as critical as it is today. In fact, according to [McKinsey Digital](#), nearly 80 percent of technology executives say they can't keep up with attackers' increasing sophistication. Company changes only increase an organization's IT vulnerabilities and further necessitates [strong cybersecurity practices](#).

The more people involved in managing the IT infrastructure, the more critical it is to control what employees can access and do. As companies scale, they may add more networks, devices, and platforms. The more data and information the company has, the higher the potential is for vulnerabilities.

IT infrastructure monitoring should uncover areas of vulnerability to help IT teams prevent incidents. Reports should allow the monitoring of the IT environment for unusual activity and send alerts that enable the IT team to respond proactively.

Leverage granular user permissions and audit trails

Strong cybersecurity begins with strong user management. IT infrastructure monitoring solutions must allow IT teams to proactively manage security by assigning the right permissions to the right users. **Controlled user permissions enable teams to shut down or control logins, assign specific users the ability to access data based on their individual or group properties, and define read/write abilities.**

Without granular user permissions, users often end up receiving administrator access they don't need. Giving admin access to users who don't need it makes them a liability. These lax security practices expose the company to unnecessary security risks that increase exponentially as the company grows.

IT infrastructure monitoring solutions should make it easy to assign the right permissions with the ability to clone and apply existing user settings to a new user. Simple user management makes the onboarding process for new employees efficient. It also makes it easier to deactivate terminated users.

In addition to user-by-user permission settings, an IT monitoring solution should create logs of activity that serve as audit trails if anything goes awry. These activity logs give granular insight into user logins and configuration changes. If the company encounters a cybersecurity issue, audit trails can help identify if the vulnerability was internal.

Monitor and alert for security threats and vulnerability

IT infrastructure monitoring tools should make it easy to monitor and alert on security breaches and malicious attacks. Monitoring solutions that have easy-to-use, standardized security templates simplify security monitoring.

These solutions prioritize security and vulnerability monitoring by allowing IT teams to use templates to set criteria that checks for abnormal behavior that could signal a hacking attempt. Abnormal behavior checks compare recent performance with historical behavior to identify deviations.

When the tool spots abnormal behavior, customized alerting is key to efficient issue resolution. The solution should allow IT teams to alert specific users based on the severity, time, or location of the incident. **By defining alerting criteria, companies can ensure that they only inform those who need to know and only escalate issues when necessary.** Customized alerting prevents unnecessary distractions that could delay issue resolution.

IT monitoring solutions give IT teams the tools needed to shift their companies from reactive security and vulnerability practices to proactive strategies that defend the company against attacks. As companies scale, vulnerabilities change. Choosing an IT infrastructure monitoring solution that provides robust cybersecurity capabilities sets companies up for success as they adapt to changing market demands.

Related Reading: [Choosing a Custom Monitoring Solution for IT Infrastructure Success](#)

Reporting

Executives increasingly expect IT teams to use IT performance data to make a case for IT investments. [Scaling IT monitoring effectively](#) requires sophisticated reporting that uncovers insights to fuel these business decisions. IT infrastructure monitoring solutions should give companies the ability to consume data quickly in a way that works best for business planning. Reports help IT teams pinpoint the information needed, saving time, ensuring critical information isn't missed, and helping them make critical business decisions.

Reporting functionality should give companies access to real-time and historical data. When combined into capacity planning reports, these two data sources help IT teams predict when devices will reach their operating capacity. **These reports are valuable when IT teams need to make a case for investments in new IT equipment and hardware.** Reports that predict when devices will reach capacity is essential for companies preparing for change.

IT teams can align executives on the performance of the IT environment and make a case for necessary investments in IT infrastructure when using a solution that includes intuitive dashboards and reports.



Future-proof scaling IT monitoring

Company changes can be challenging for IT teams, but IT infrastructure monitoring can alleviate many common pains around scaling. IT teams should look for a flexible solution that doesn't force the company to predict the requirements their future environment will need. Solutions that make it easy to add new devices, servers, and networks without technical limitations allow companies to scale without worrying whether the solution will soon be obsolete.

When choosing the best solution for the business, companies should ask questions about ongoing product development and maintenance, and learn what customer support options are available to support the company through roadblocks. Both factors indicate whether the IT infrastructure monitoring solution is receiving investments needed to power growing companies into the future.

With sophisticated, easy-to-use features, IT infrastructure monitoring can increase an IT team's productivity, help the company adopt advanced cybersecurity practices, and deliver executive-level reports that aid in planning. Companies that choose a tool with these considerations in mind will successfully scale their IT infrastructure monitoring to match company flexibility.

Get Started with Nagios XI

BEGIN YOUR FREE TRIAL NOW