ConnectWise®

Simplified Management for Complex Environments

ConnectWise eBook Series

Find IT Problems Before They Find You

Solve Users' Issues So Easily, They'll Never Know You Were There

Contents

Introduction

It's A Dangerous World Out There

With IT concerns on all sides—from visibility and availability, to security and compliance—you serve as the first and last line of defense for your users, who are looking to you to make sure everything is working simply and seamlessly. What's your secret weapon? Perfecting processes through monitoring.

With the wrong monitoring capabilities, your users are telling you about problems and you're scrambling to find solutions. With the right ones, you can proactively combat issues before users ever see them.

With the wrong monitoring solutions, your users systems are down for too long and they start questioning your value. With the right ones, downtime is kept to a minimum and you maintain confident systems control.

With the wrong monitoring tools, your staff and leadership team are held accountable to the fallout from hacked systems and a lack of compliant protocols. With the right ones, your users are kept safer and no one has to worry about fallout.

> *"Through 2015, 80% of outages impacting mission-critical services will be caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues."*
>
> —Ronni J, Colville, Gartner

Chapter 1: Systems Monitoring

Making the move from reactive to proactive service delivery starts with effective systems monitoring, which means you'll be able to sneak in under the cover of efficient monitoring and remediate issues before users know they exist.

Remote control is a great reactive service, but your team needs to be able to do more with less, without interrupting users. With the right systems monitoring in place, you can manage your entire supported environment from a single control center.

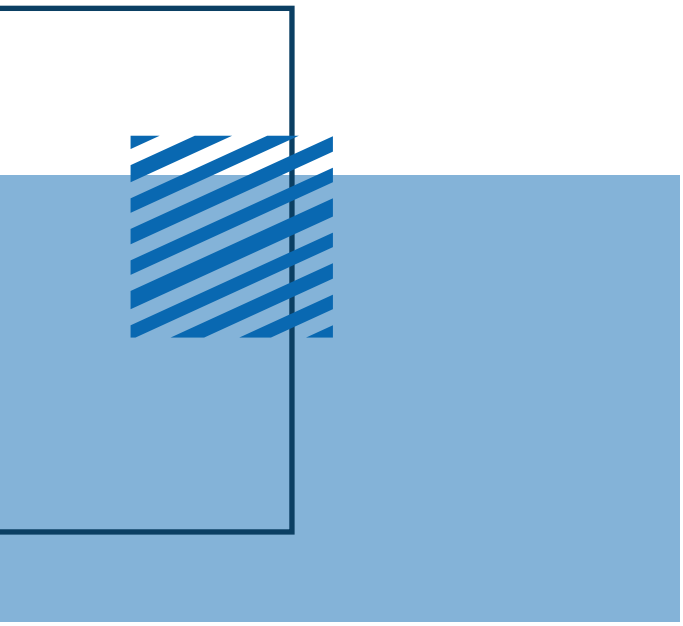
According to Gartner, **more than 95% of businesses know that reactive issue resolution isn't a scalable solution.** By implementing full systems monitoring, you can not only take steps toward proactive maintenance, but also simultaneously improve reactive response times thanks to increased visibility.

Chapter 2: Desktop and Server Monitoring

Desktops and servers are the tools that users rely on to get the job done. They're how your team produces solid results, and how you manage most of your work every day. When either one goes down, it could affect the productivity of a much larger team as work stoppages trickle down. **It's up to you to maintain a clear line of sight into everything that's happening, so you can react faster when issues arise.**

Make it work by starting with critical servers and focusing on the basics—up/down, disk space, and CPU. Then move on to more business specific items like services and event logs. Use scripting to combine and orchestrate multiple desktop and service management commands so that you can automate, save, and share the remediation of common issues.

Next, move your focus to security issues like failed login attempts and locked accounts, and get your desktop line of business applications covered, including services and event logs. Finally, adjust your monitoring thresholds for high-value desktops. If your customers are placing value on those users, it only makes sense to give them a little VIP treatment.



Chapter 3: Patch Monitoring

When securing your environment, the most basic proactive service you can offer is patch management to protect systems from known attack. Patches correct bugs and flaws, and provide enhancements which can prevent potential user impact, improve user experience, and save your technicians time researching and repairing issues that could have been resolved or prevented with an existing update.

Users generally understand that their systems need to be patched, but they might not have the expertise to comfortably approve and install patches without help.

But remember it's not enough to simply push patches, you need to validate they actually installed. This final step is the process if often forgotten, but is a necessary procedure to ensure that service levels are met. With the right solutions in place, you can automate this task to reliably monitor the patching of multiple systems at once, standardize policies, and manage by exception to efficiently secure more endpoints.

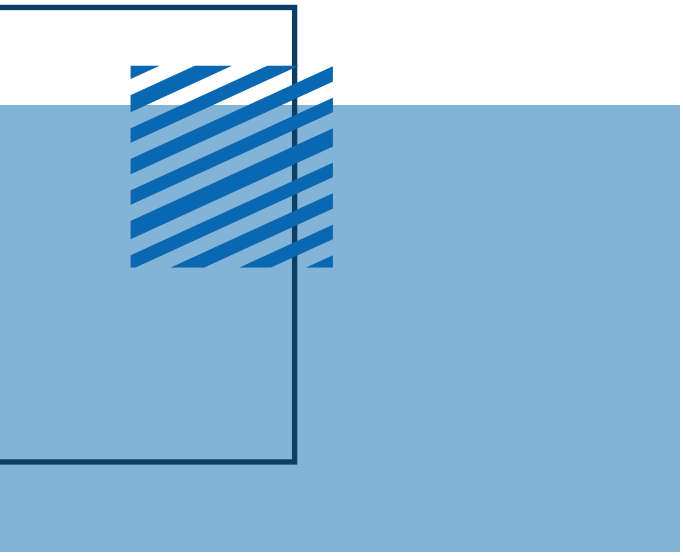
Developing best practices to manage the risks associated with the approval and deployment of patches is critical to your service offering.

Chapter 4: Infrastructure Monitoring

Many desktops and servers run on virtualized hardware like VMware or Hyper-V. While your most frequent problems will come from the virtualized OS or application layer, hardware problems in virtual environments are often missed during initial troubleshooting.

Most technicians assume the hardware health is fine. After all, if there were a hardware problem, you'd be seeing multiple systems with issues. Right? That may be true a lot of the time, but it can be a dangerous assumption. Issues, like memory ballooning, are a great example of problems that pop up in the virtualized OS, but have a root cause in the host.

The potential impact is huge when a larger scale issue occurs within a virtualized infrastructure. That's why **it's important to check the health of systems hardware. Missing that step can lead to hours of unnecessary troubleshooting.**

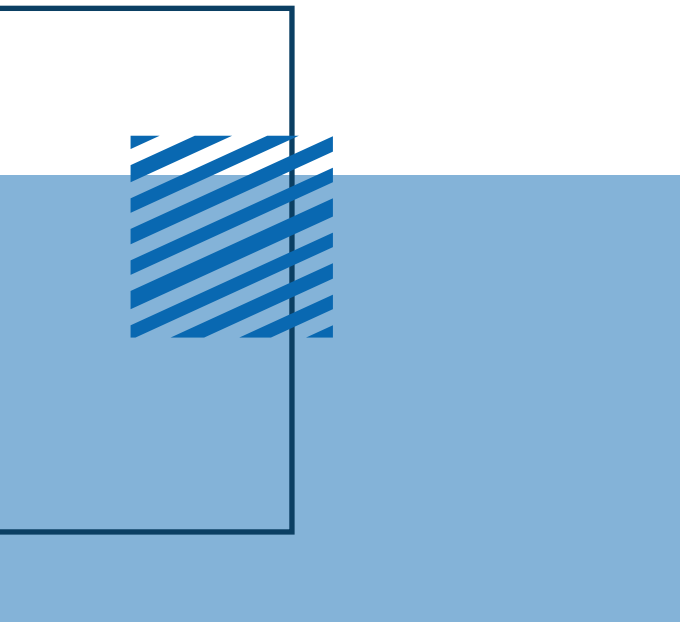


Chapter 5: Networking Monitoring

The final step in mastering monitoring is focusing on network monitoring. Printers are the first thing that springs to mind here, but they're easily addressed and aren't a high impact issue when they do have problems.

Networking devices, on the other hand, are at the center of how every one of your users connect to the systems they need to get their jobs done. The good news is that networking devices are extremely reliable, but when issues do happen...when a router crashes or a switch port dies, bandwidth plummets and the support calls start pouring in.

Just like desktop and server monitoring, start with the basics here. Once the lowest- hanging fruit is well handled, it's time to focus on the more complex issues to make sure your network devices experience minimal downtime.



Conclusion

At the end of the day, monitoring is all about finding problems before they cause issues for your users, and managing expectations when problems do crop up. Once critical and basic coverage is handled, start monitoring devices to keep everything tied together. If a switch, router, or hub goes down, or a printer starts having issues, you'll know before the complaints start rolling in.

When you automate recurring processes or tasks, your team can focus on delivering value instead of putting out fires.

That means increased user satisfaction and minimal downtime. Rely on silent IT to remotely troubleshoot issues without interrupting users, and see your efficiency skyrocket.

Do it all, simply and seamlessly, with help from ConnectWise Automate®. Our remote monitoring and management (RMM) solution is specifically designed to help you automate repetitive tasks, including necessary security measures like patch management, to help you keep systems secure and users satisfied.