# How to Solve the Top IT Issues at Remote Locations

Setting up a solid IT foundation at a remote office is essential. IT teams can run into many typical challenges when supporting remote office users, with the added challenge that they're not physically able to see the problem and might not have a colleague on site to help. Here are the top issues to watch for when you're in charge of offices, users and technology that you can't actually see.

It can be an exciting milestone for a business when a new office or location opens. But it's not necessarily an exciting day for everyone. Setting up a solid IT foundation at a remote office can bring issues to the surface or create new ones for IT teams and the users accessing services from that off-site location.

A remote office is only as technically sound as the main data center or cloud infrastructure supporting it. IT teams can run into many typical challenges when supporting remote office users, with the added challenge that they're not physically able to see the problem and might not have a colleague on site to help.

Of course, lots of technology advances, such as real-time collaboration tools, cloud computing and VPNs, have made distributed IT environments more connected. They've also added complexity.

Here are the top issues to watch for when you're in charge of offices, users and technology that you can't actually see.
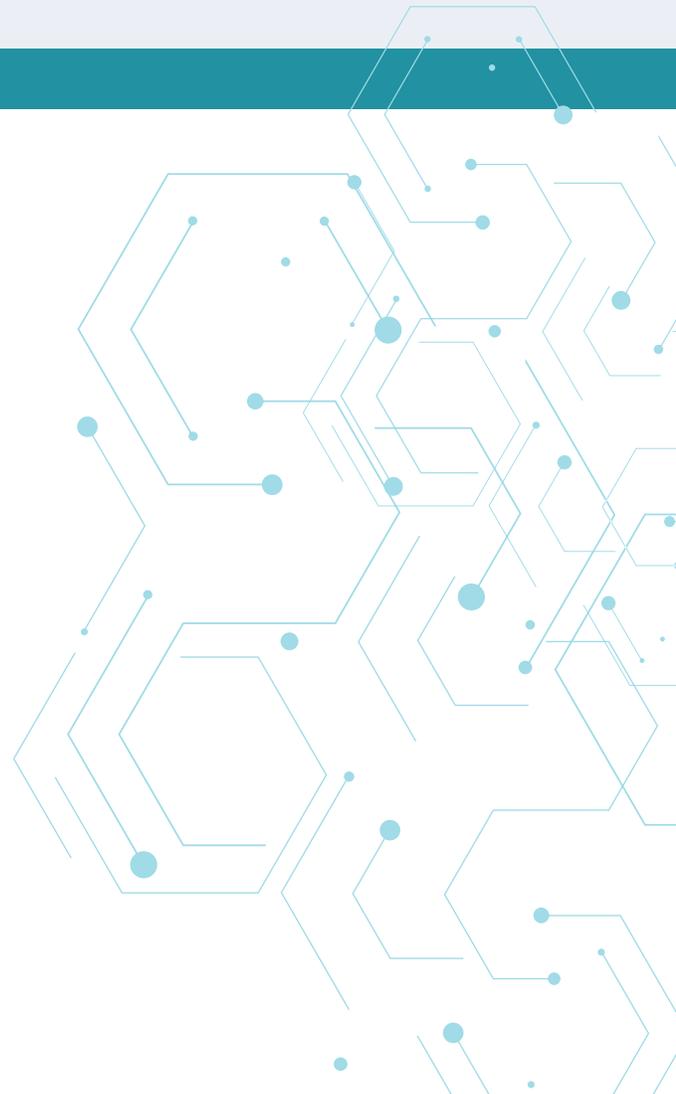
1. Integrations, especially with shadow IT

Integration issues often rear their ugly head when remote locations enter the picture. With the influx of cloud services and SaaS apps, the various parts of IT infrastructure are scattered. It's easy for a company to be using hundreds of different applications and for IT not to be aware of all of them. Integration and standardization are important for IT to be efficient, but they're hard to accomplish.

Integrating systems at a remote office is a big part of off-site efficiency. If functions are consolidated, it's harder for users to waste resources or make duplicate efforts. Fewer systems also means fewer patches or upgrades for IT. Cloud computing can help deliver services to remote offices from a central location, which helps with the problem of incompatible computer systems. If a company's data center infrastructure is well-integrated, remote offices have an advantage in getting technologies that have already been tested to work together.

By 2018, **65%** of companies' IT assets will be off-site in colocation, hosting and cloud data centers.
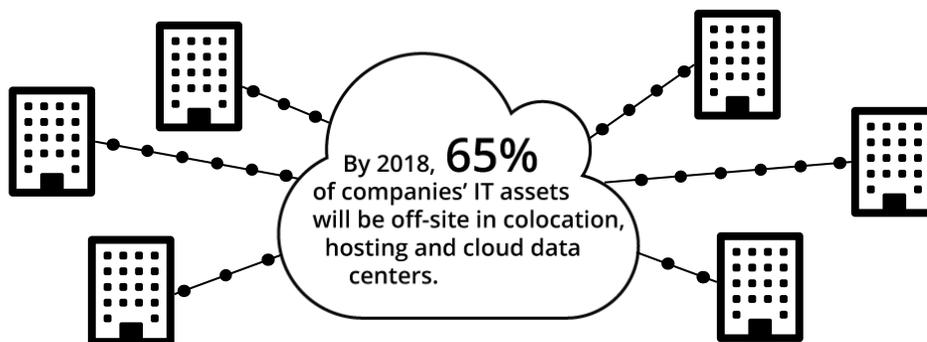
2. Scaling IT resources and budget

At a remote office, the efficiency and flexibility of technology is key to worker productivity. There's also usually not an unlimited fund for IT to set up a new location with every bell and whistle. IT professionals reported their top challenges in managing IT solutions as "lack of time and resources" (44%) and "insufficient budget" (40%). So IT managers likely need to choose carefully to right-size financial resources and tech resources like bandwidth at remote locations. They'll have to ensure good performance for users without exceeding those bandwidth and budget limits.

Application uptime helps workers be productive and keeps helpdesk tickets out of IT's queue. Ideally, IT will have a detailed understanding of application and network domains before launching a new location, or be able to map them out at an existing location. Understanding the interplay of apps and networks can lead to a real overall improvement in business performance.

3. Added network complexity

Networks haven't changed a ton over the years, but their uses have become more complex and varied. When a remote location opens, it may seem that no network has ever been as important as that connection over the WAN. It'll be a handy tool for users when it's working well, but for IT it's just one more piece of a bigger network puzzle to monitor and maintain. The WAN requires the same care, attention and monitoring as the onsite LAN, the internet and any cloud networks.

When remote locations are part of IT's domain, the old "Is it the application or is it the network?" question might emerge more often. If there's any lack of visibility into the WAN and its performance, it can complicate troubleshooting efforts of issues at the remote office. Remote workers need to access corporate applications and data as easily as they would at a central office, over high-bandwidth, low-latency networks. Modern applications depend on a strong network to avoid failures and productivity loss.

4. The resource gap

In a lot of industries, remote offices or branch locations don't have any IT staff or technical employees—think doctors' offices or banks. It's nearly inevitable that the gap in tech staff resources will lead to delays in services to those locations. The high costs of traveling to those locations or staffing them can be prohibitive for many businesses.

As the shift from physical to virtual infrastructure continues, the people involved also continue to adjust. Not so long ago, IT was always located in the same building as all the servers and tools they were managing and deploying. But with remote locations (as with cloud services) and virtualized infrastructure, IT employees just are not physically there. That can lead to confusion and a lack of communication around user issues. Help desk tickets might not reach IT's desk immediately, or a recurring problem can be ignored by remote location end users until it gets critically bad. These issues can lead to bigger problems and cause a lot of ongoing frustration for IT.

5. Ghost issues

"Ghost issues" are the bane of IT. They're issues that are often impossible to reproduce and usually take the most time to identify and fix. IT might hear from a user that a problem occurred, but not be able to figure out why. If IT doesn't have any staff at a remote site, troubleshooting involves a lot of guesswork—especially when the issue disappears.

A ghost issue in your on-premises data center is annoying enough, but what about one that's happening many miles of network cable, ISPs and hops away? They're difficult to troubleshoot without monitoring, so continuous monitoring and a path-centric, rather than device-centric, measurement can improve the remediation time for ghost issues. Without continuous monitoring, there's no historical data to pinpoint exactly when the problem happened and how it was resolved. Capturing the right metrics will be essential to preventing ghost issues—for example, being able to see the route history and perform remote packet captures.

If possible, set up processes as well as technology tools from the get-go. User communications will be essential, so make sure remote users are able to report problems and request services or tools easily. Supply users with monitoring reports or other feedback on recurring problems.

Monitor It Like You Own It—Because You Do

It's clear that not seeing what's happening at a remote location can be a hazard for IT teams. They need to understand what's happening with the network and applications at branch offices, without slowing them down. They're also still responsible for fixing issues fast, even when it's off-site or third-party infrastructure. Once they've got the needed visibility established, IT teams can fix any endemic problems to clear the way for better productivity.

Monitoring for remote locations requires always-on monitoring. It also requires reports that can be tailored for non-technical employees, so they can understand whether they should change any user behavior (YouTube streaming is out of control, perhaps?). Using continuous performance monitoring also allows IT to figure out whether it's the application or the network right away, speeding up the resolution process.

The right modern monitoring tool can also lead organizations to baseline performance when setting up a new location, then track ups and downs quickly to make adjustments and change configurations. With this kind of monitoring, IT can get performance data from the entire infrastructure, whether at remote sites, in the cloud or on-premises, and take action. Remote offices may be remote, but they don't have to be out of IT's control.