CBTnuggets

How to Prepare Your Company to Go Remote:

29 Lessons from IT Professionals Who Rapidly Scaled their Remote Infrastructure

By Michael Hess

In response to local and state social distancing directives designed to limit the spread of COVID-19, many companies and organizations have asked employees to work remotely.

For the nearly third of Americans who already work from home — and the companies who already have the infrastructure to support them — these directives could immediately be carried out. For other organizations, sending everyone home presented challenges to the IT professionals tasked with preparing users, infrastructure, and hardware for the switch to a fully remote workforce.

The rapid shift to remote work for otherwise on-site employees brought with it both technological and social challenges. This paper compiles the experience of ten IT professionals as they scaled their infrastructure to accommodate remote work.

Methodology: We interviewed ten IT professionals from nine U.S. states and two countries who participated in rapidly deploying virtualization, cloud, and productivity software, as well as hardware to about 3,500 employees at ten companies. In some cases, they had 24 to 48 hours to prepare an entire workforce to work from home. Their experience covers roles in systems engineering, network engineering, virtualization, and desktop support.

Responses contributed by Seth Battles, Josh Burnett, Carlos Marquez, Nick Matveev, Graeme Messina, John Mintz, Erik Mikac, Jeff Richards, Steve Schwettman, and David Zomaya.

The Infrastructure of Remote Work

Most modern IT infrastructure is fundamentally designed to support remote work from both the user and administrator perspectives.

Microsoft has emerged as a cloud-first company, which means the ability to remotely manage thousands of Windows 10 instances from SCCM or Admin Center. Cisco has built its operating system, IOS, for software-defined networking, which means remote network management and monitoring. Desktop virtualization vendors Citrix and VMware have long played a role in untethering people from their desks in an office setting.

To successfully send everyone remote, you'll need at least these six core services:

VPN to Access Your Servers Securely

Virtual private networks (VPN) are a must for any company that allows employees to access their servers remotely. Without this, corporations must make at least portions of their server available to the entire internet so techs can access and log in. Think of a VPN as a secure, virtual ethernet cord that plugs a user's computer directly into the business network by using an encrypted tunnel. The signal is generally protected from prying eyes, and even if it is intercepted, only encrypted data is accessible.

There are three aspects to the system: the server, the VPN, and whatever device your techs are using to access the VPN. The VPN keeps the server secure by making it invisible to the internet at large, and since you've set everything up correctly, to begin with (of course!), your device is already mapped to the VPN. The only vulnerability at this point is the client device itself, so ensure that your antivirus is updated to prevent any malware from compromising the integrity of the physical laptop.

VDI to Decrease Complexity While Saving Money

Virtual Desktop Infrastructure (VDI) allows a desktop to be accessed from anywhere with an internet connection. This isn't limited to other desktops,

however, but can also be used with a variety of devices, including thin clients. Prior to VDI, the operating system was bound to hardware when it was installed—if the hardware failed, the OS also crashed, often causing someone to lose all their data.

VDI separates these two by using a software called a hypervisor. The hypervisor is installed on a server, allowing multiple operating systems to be installed and accessed remotely. Rather than having separate physical PCs, the hardware is divided into multiple virtual machines, each of which can have unique configurations, applications, and OS. This is taken a step further by the use of a High Availability (HA) function, extending VDI to multiple servers, so even a server hardware crash won't threaten data or accessibility.

This tech provides numerous advantages. The first, and most obvious, is accessibility. Particularly in today's environment of social distancing, being able to access your desktop from anywhere is invaluable. The second is security: physical devices can't be stolen, damaged, or lost. An additional benefit layer here can be found by considering what would happen if one of your mission essential IT techs lost a laptop and the inconvenience that would follow. You would have to procure a new device, set up the OS, reinstall all the necessary software, and restore licenses, all of which would require physical interaction to complete. With the number of devices heading out the door as many companies increase their remote workforce, this risk is almost entirely mitigated. Finally, the cost savings shouldn't be underestimated: the fewer devices that must be purchased, maintained, and tracked, the cheaper it is for a business.

Collaboration Software to Keep Everyone Connected

Staying connected to your employees and ensuring that they can have uninterrupted access to the rest of their team is critical in a remote environment. Numerous applications exist for virtually any business need. Here's a list of the most common applications and their uses:

- **Slack** is a team communication system that is reminiscent of the old instant messaging systems of the early 2000s. You can create individual or group channels, collaborating and sharing files in real-time.

- **Zoom** is widely recognized as one of, if not the, best video conferencing software systems available. The company has placed a high premium on security and is even HIPAA-approved.

- **Google Drive** is an excellent resource to store, share, and collectively create files within a team environment. It offers a number of tools comparable to the Microsoft Office Suite, and multiple individuals can work in a file simultaneously.

VoIP Solutions for Consistent Contact

VoIP stands for "Voice over Internet Protocol," giving you the capability to make phone calls over the internet rather than tying up an actual phone line. There are quite a few advantages to this for the remote worker and corporation. The first is cost savings: you don't have to pay for or subsidize someone's cell phone or landline when requiring them to be available for calls as they work off-site. As long as the data connection is strong, the sound tends to be clearer, faster, and more reliable than a normal phone connection. Depending on the area of the country or world, data lines can be far more stable than phone lines, adding an extra layer of insurance when considering your ability to make calls consistently. Last but not least, if you're working from home, there's no need to tie up a landline with business calls, ensuring uninterrupted business access.

There are three primary ways to access VoIP. The first is an analog telephone adaptor (ATA), a device that connects to the internet and that you can plug a regular phone into. Another way to use a dedicated device is by using an IP phone: this looks like a regular phone, but instead of having RF-11 phone connections, it comes equipped with an RJ-45 ethernet connector. Some IP phones are Wi-Fi enabled, foregoing the need for a physical connection.

The final access method is by using computers to make the call. Numerous software applications currently use this, including Cisco applications, Skype, and Zoom. These applications can be installed on virtually any device, from desktops to smartphones.

Configuration Management Tools to Automate Processes

When networked computing first began, sysadmins physically managed servers on an individual basis: configuring, installing software, and administering various services. As data centers began to exponentially increase in size, complexity, and number of applications, the limiting factor soon became a system administrator's ability to accomplish these tasks on an individual basis, ushering in the need for configuration management tools.

System Center Configuration Manager (SCCM) is a management technology that was first introduced in the mid-1990s. It was revolutionary for its time and still useful today in managing legacy applications but requires agents on each of the managed hosts, all of which must be installed, configured, and updated regularly.

Ansible is the newest solution and is an incredibly easy to use platform. It utilizes native management technologies, such as Powershell and WinRM on Windows machines, without requiring any additional software or third-party interactions. It's updated simply by keeping the OS patched. Ansible can create groups of machines and configure them en masse, as well as direct them to take actions collectively rather than individually. It's installed on the control machine (the central device from which all others are managed) and, other than when it's actually connected and interacting with a server, requires no CPU, memory, or software on the destination device. These tools are valuable for on-prem sysadmins but absolutely crucial in any kind of remote scenario.

Monitoring & Automation Software to Manage On-Prem Infrastructure

Infrastructure monitoring software automates physical, virtual, and cloud infrastructure oversight. Some of the major processes include error monitoring, log management, and application performance management. This level of insight into how resources are behaving allows businesses to identify and resolve problems before they happen, in many cases. The software is not only reactive, responding to issues the moment they become evident, but is also proactive, assisting sysadmins in planning for upgrades before outdated systems can fail.

The overall category of "infrastructure management" consists of storage management, network management, and systems management. These have traditionally existed on-premise, but are more and more commonly moving to the cloud. In rapid growth situations, infrastructure monitoring software is critical to ensure that configurations and installations occur as intended. In an increasingly common remote environment, sysadmins often aren't physically present to monitor, respond to, and resolve many issues, making automated monitoring software an absolute requirement to effectively manage on-prem infrastructure.

Build IT into Business Continuity

Tools to handle virtually every IT process outside of physical component handling already exist. Taking advantage of them will not only allow your company to maximize the advantages of remote access, but will also go a long way toward ensuring seamless business processes in times of either voluntary or forced (e.g., social distancing due to a pandemic) isolation. This is good for your employees, your company, and, most importantly, your customers.

Planning for Remote Work: 4 Essential Questions

IT teams can spend months planning and building VDI or RDS solutions. In the case of the COVID-19 response, IT professionals had at most a day to deploy virtual desktop infrastructure to support their teams. Still, planning was essential, even if it was compressed into a narrow window.

Here are the baseline questions that helped marshall the resources to get everyone remote:

How many people will be remote? This is the most basic information required for purchasing licenses. For small companies, this may be easy, but larger companies will need to develop a way to track and maintain who is remote. Work with HR, team leads, and leadership to get an accurate count of the remote workers.

Who will be remote? With a firm count of employees, you'll then need to know who will be going remote to set up licenses, assign privileges, and track equipment. This step is particularly important for organizations that will only send a portion of their workforce remote. When everyone goes remote, administrators can easily implement a sweeping remote solution for all employees. Determining who needs access and licensing for a partially remote workforce will require more communication with HR and department leaders.

How long will they be remote? The question of how long employees will be remote is the toughest to answer, but an essential one for licensing and logistical reasons. There may be potential cost savings by extending a licensing plan by three months versus one month.

What infrastructure resources do you need? With a headcount and historical data, you can extrapolate the resources you'll need. Is there enough compute, memory, storage, and networking capacity to handle the surge of users? Follow your vendor's best practices for capacity planning and the handful of golden rules such as a minimum n+1 for host failures and the 3-2-1 rule for backups.

Action without information and data could well be wasted. Knowing the baseline information is the most important thing when preparing to get everyone remote. Work with company leadership in HR and finance to marshall the resources you need to get everyone not only home, but working effectively.

29 Challenges Learned from COVID-19

Swiftly sending an entire workforce home presented a set of challenges to the ten IT professionals we interviewed.

Typically, remote work at scale would be planned out over months and enacted in phases. In preparation for the fundamental shift, companies would increase licenses to collaboration and VDI software, purchase laptops, configure group policies to allow access to internal resources, and test connections. However, many companies issued work-from-home directives and then relied on their IT departments to enact the necessary steps within hours or days.

For some companies, the mass exodus was as simple as telling everyone to grab their laptop and monitors on the way out the door. However, the reality is that many businesses were either ill-prepared or moderately prepared for their entire workforce to go remote.

From that experience, these 10 IT professionals encountered challenges and learned how to deal with them. Some challenges were esoteric and industry-specific. Others were common across companies and industries.

To help distribute the shared knowledge from this experience, we primarily compiled the widely applicable challenges and their solutions for this whitepaper.

4 Hardware Challenges: Planning to Go Remote

Most companies surveyed had viable software infrastructure to facilitate remote work — virtual desktop infrastructure, VPN, and collaboration and productivity software. With a couple of exceptions, software-based tools for remote work were implemented with relative ease.

Office equipment, however, posed logistical, technical, and social challenges for the companies as they prepared their workforce for remote work. To accommodate remote readiness, organizations need to put thought into their office hardware — particularly the individual workstations.

Challenge 1: Lack of Laptops

Two of the 10 companies surveyed didn't have enough laptops for every employee eligible to work remotely.

In the last decade, laptops have become a suitable alternative to the desktop for many enterprise environments. For most office tasks, laptops and desktops are virtually indistinguishable based on performance and utility. For the typical office worker, an off-the-shelf laptop has enough processing power to operate the standard productivity software and other enterprise software. For this reason, many companies have switched to laptops. However, there are reasons a company may still prefer desktop computers: industry standards, company policies, and cost savings.

Industry tools and software. For some industry professionals, desktop workstations are the standard due to system requirements for certain computer-assisted design (CAD), manufacturing, and graphic design software. High-end laptops may be able to run these types of processing-intensive software, but desktops often come out ahead in terms of cost to performance.

Organizational culture. Desktops are still popular in industries that haven't embraced remote work, like manufacturing, healthcare, and government. In these organizations, laptops are reserved for employees who require them. One respondent who works in the manufacturing industry wrote that laptops are issued or loaned only to "outside sales, employees who are traveling, executives, IT personnel catching up, and the occasional worker who may have an illness preventing them from working in the office."

Security and property management. Security is another reason companies enact policies that limit laptop use to those who regularly travel or work remotely. It's harder to lose valuable property if it never leaves the office. Similarly, it's more difficult to gain physical access to a computer if it's always in a secure building.

Cost savings. Quite simply, desktops are cheaper than laptops to purchase. They are also easier to maintain and configure, and more durable than laptops. There's also less chance a desktop will be accidentally damaged.

For these reasons, desktops make sense for many companies, which subsequently makes the switch to remote work more challenging for the IT teams charged with sending a workforce remote.

The IT professionals we interviewed found three solutions for quickly sending people home with a computer.

Solution 1: Hand out spare laptops

The first thing you should do is deplete the hardware you have on-hand — even if it's not perfect. Many IT shops have a stack of old or loaner laptops lying around. Deplete your cabinet of old hardware before moving to the labor-intensive second solution. The vast majority of office workers only really need a machine that can handle the Microsoft Office suite (Outlook, Word, and Excel) and a web browser.

Challenges: Loaning out old laptops is not the perfect solution — and it's a solution that crumbles at scale. Functionally, even if the laptops are updated, operational, and imaged properly, you're still giving someone hardware they're not familiar with. You're inevitably going to have to support that laptop and its user remotely.

Lesson: Know exactly what hardware employees need by job role to better prepare for the possibility of remote work.

> ***"IT personnel handed out all spare laptops immediately. The only other option was to send the user home with their desktop and monitors."***
>
> - John M., Jacksonville, Florida

Solution 2: Take desktops home

There are many good arguments for allowing employees to take their desktop towers home with them. The users are already familiar with the machine, which has all their applications and files. You can also be reasonably confident that the accessories they grabbed from the office will work with it. However, there are also challenges associated with sending hundreds or thousands of desktops — and their accessories — home with employees.

Challenges: Sending desktops home with newly-remote workers may seem like the easiest thing to do in the short-term. However, the IT administrators interviewed found that it posed a few challenges in practice:

Wired access only. Most enterprise PCs are built to sit on a desk and connected to ethernet, which means they may not have built-in wireless cards. One company's IT team solved this problem by purchasing USB wireless cards at local retail stores. Alternately, it may also be helpful to send everyone home with a length of ethernet cable as a backup. Take this into consideration before everyone heads out the door. Otherwise, be prepared to support both hardware and network connectivity issues remotely.

User support for a desktop setup. Some people will not know how to set up their desktop computers at home. In at least one case, "IT staff struggled to help a newly-remote employee over the phone to navigate all the cables and ports." Eventually, support techs resorted to FaceTime and other video call software to provide support.

Lesson: Prepare documentation for the most basic hardware tasks — and develop the documentation for someone with no experience with computer hardware. Even the most expeditious way to get people remote requires unique support challenges.

Solution 3: Buy new laptops

In the event that there isn't spare hardware and it's impossible for employees to take home desktops, then purchasing laptops may be the only solution to get a workforce remote. At least one company purchased "hundreds of laptops so that employees could take them". There are benefits to this solution. Supporting a homogenous device environment makes support easier. Additionally, with the purchase of new hardware, you'll be confident of the ability to send the workforce remote again. However, there are logistical challenges to this solution.

Challenges: Quickly purchasing and deploying hardware to a remote workforce is fraught with potential financial, logistical, and support challenges. The greatest challenge one IT team faced was a logistical one — unpacking, configuring, and distributing hundreds of laptops. In this particular case, the desktop computers the laptops replaced weren't functional with the company's VDI environment, which led to the decision to purchase the laptops. Ultimately, they were "stuck getting all users into the Active Directory group that allowed VPN access."

Lesson: Laptops with a dock are a versatile solution for an increasingly mobile workforce. Purchasing laptops may not be cheaper upfront, but it's cheaper

> ***"Rather than issuing multi-factor authentication (MFA) credentials on a case-by-case basis, employees should receive these when on-boarding — whether they need them or not — to avoid backlogs when they do."***
>
> - Seth B.,
> Chattanooga, Tennessee

and easier to set up everyone for remote work ahead of the immediate demand, rather than implement the infrastructure and hardware piecemeal — or rapidly.

Challenge 2: Using Office Equipment at Home

The typical office setup in the United States includes the basics: computer, monitor, keyboard, and mouse. While most people can make do with just a laptop or desktop and monitor, there are also additional accessories necessary for work, such as additional monitors, desk phones, and headsets that make work easier. Headsets, in particular, are necessary for remote work.

While many people can get along fine on a laptop screen and the trackpad, that's a big context shift (and potentially a productivity loss) for people who aren't used to it. The right accessories can make a big difference in productivity.

Among the IT professionals who helped get their employees remote, there were three elements that were most troublesome. Here are the essentials:

- **Mouse.** Having a mouse versus a trackpad can mean a world of difference. Similarly, shifting from one style of mouse to another can be particularly disorienting.
- **Monitor(s).** While laptop monitors may be sufficient for many tasks, multiple monitors have become a necessity for many people.
- **Keyboard.** A keyboard with a number pad versus one without can influence how fast math-heavy work gets done.
- **Headsets.** Headsets can impact the quality of remote meetings and calls. This is particularly important for employees who are working from home with family or roommates.
- **Printers.** Unfortunately, there's no good home alternative to the commercial print center. Users who regularly print or scan documents should move to PDFs or eSign capabilities while they are working remotely.

While individually issued company equipment can easily be packed up as employees head home, larger office equipment like printers, scanners, and other specialized equipment are no longer available in the remote work environment.

There's no one-size-fits-all answer to the accessories you'll need. Think about what you do in the office and try to replicate that at home. In some cases, you

may need a laptop dock or USB hub to support all the accessories, but it can be well worth the investment.

Solution 1: Take home your office equipment

Allowing employees to take their company-issued equipment home was the preferred option for most companies. While it may be cumbersome to haul a monitor, peripherals, and possibly even a full desktop tower home, it's still better than trying to work from personal equipment or a loaner laptop.

Challenges: Keeping track of inventory may be difficult. Support calls may increase. Additionally, some companies usually aren't too excited about letting that much equipment walk out the door, but that's the cost of remote work.

Lesson: Schedule regular hardware audits and maintain inventory as best as possible. When enacting company-wide remote work, build a form — even if it's as simple as a Google form — to track the equipment that employees take home. Knowing what equipment people have goes a long way for tracking and support.

> *The last thing you should be doing is packing up monitors, keyboards, and other peripherals just to move your office around. A docking station is a DR solution component that you really should consider if you are going to be moving between the office and your home during this lockdown period.*
>
> - Graeme M.,
> Durban, South Africa

Solution 2: Purchase accessories from online retailers

If an employee needs a USB hub, mouse batteries, or a new keyboard, it's probably relatively easy during normal operations. While everyone is remote, it may not be as easy as walking down the hall, but it should be as easy as submitting a ticket or a call to support.

Three companies either moved to online purchasing and shipping to alleviate the problems for remote workers or expanded existing programs to support remote workers.

Challenge: Depending on the number of people who are remote, purchasing more equipment poses both financial and logistical challenges. If purchasing is centralized, then it's likely you're tying up already burdened support staff to order supplies from an online retailer. In some cases, it may be easier to allow personal purchases for reimbursement.

Lesson: Build out a support system to deliver simple, but necessary office supplies from an approved list to remote employees. While everyone is remote, set up or build systems around online retailers. In some cases, it may be easier to manage supplies and track costs from a centralized location. Otherwise, allow employees to make purchases on their own and then reimburse them.

Solution 3: Bring your own device

In any office environment, employees go rogue and use their own equipment — whether they're using a vertical mouse, wave keyboard, or their own noise-canceling headphones. At home, it's tempting to move work over to a home office where they're comfortable.

Challenge: Company policies may govern what equipment can be used at work, but those policies are hard to enforce at home. In other cases, companies may necessitate using personal equipment while working at home. Neither situation is ideal, particularly for support.

Lesson: Be compassionate. Remote work isn't ideal for everyone. Anyone using their own equipment is using it to be as effective at home as they are at work.

Challenge 3: Making Calls from Home

Only one among the IT professionals surveyed even heard about difficulties with moving VoIP solutions into a remote environment — and it was a second-hand account. Thanks to softphones and mobile devices, support and sales teams are often perfectly situated to easily go remote. For job roles that regularly make outside calls, there are few options for making calls from home.

Solution 1: Bring your own device

Despite the challenges inherent to BYOD, you can actually maintain some control over the remote environment even when users bring their own devices. This can greatly improve security while reducing support headaches and ensuring compatibility among applications on different platforms.

You may already have Mobile Device Management features that you're not using. These have been integrated for some time into Exchange Server, Office 365, G Suite, and others. After getting this solution set up, it's worth taking a look at the MDM features available and implementing some policies.

Challenge: The challenge in this environment is to maintain adequate security over company systems and data, without implementing overly restrictive policies.

Lesson: Companies should have BYOD policies in place for business continuity and to address the certainty that employees bring their own devices into the office.

Solution 2: Take the VoIP hard phones home

Depending on the vendor, remote workers with VoIP hard phones can either opt to take their hard phones or use associated apps to make calls from home. With relative ease, Cisco phones can go home with employees. For easier calling from home, Cisco Webex Calling, Cisco Unified Communications Manager (UCM), and Cisco UCM Cloud solutions can route through a softphone application.

Challenge: Taking hard phones home requires some set up by the user, and considerable backend setup by collaboration engineers.

Lesson: Depending on company policies, your business continuity plan should include options for employees to make business calls on multiple devices or applications.

Solution 3: Use collaboration tools instead

For employees who aren't making outside calls often, they're probably relying on collaboration software like Teams, Skype, Zoom, Slack, GChat, or other services to make voice and video calls to colleagues.

Challenge: This solution only works for employees who primarily communicate with other employees. It's likely not a suitable solution for sales, support, call centers, or other functions that require regular phone contact with outside parties.

Lesson: Collaboration software is essential for internal teams to use to communicate with one another, but it shouldn't be relied upon as a replacement for phones.

Challenge 4: Monitoring and Automation On-Prem Hardware

The majority of the challenges noted in our interviews dealt with IT professionals serving their users directly. One administrator noted that he still needed to monitor infrastructure, which he accomplished with monitoring software. To this point, he brings up the need for both monitoring and automation.

At this point, monitoring and automation in IT should be complementary in any system — and having remote access to fix any additional issues should be the baseline. When monitoring software flags an error or failure, there should be an automated response. If it's a unique error, then technicians should get alerted

and they should be able to work remotely to fix the problem.

When sending home an entire workforce there are a lot of things that can go wrong, so it's more important than ever to quickly know when something has gone wrong — and that it's fixed promptly.

Solution 1: Automate as much as you can

Under normal operations, automation helps free up time while eliminating the possibility of human error. When everyone is working remote, automation is all the more important. While everyone is remote, endpoints can break, infrastructure resources are under uncommon loads, and in many companies systems have gone untested at scale.

With so many devices off-site remotely accessing resources, automation can help tame unwieldy desktops and integrate them successfully with BYOD, eliminating the need for frequent help desk tickets. You don't have to overhaul your entire automation and monitoring solutions. Get everyone remote and handle the issues as they occur.

Challenge: Unclogging these bottlenecks with automation does require expertise with diverse areas such as user profiles, policy management, VPNs, and remote desktop support. Without solid foundational knowledge of Ansible, PowerShell, or a scripting language, automating these processes may take more time.

Lesson: Even if you automate just one key process or section of your processes, you can make a major impact on the time it takes to deploy your remote workforce.

Solution 2: Use off-the-shelf tools

Modern infrastructure is built for automation, and there are tools that make monitoring and automation even easier. Ansible, Chef, and Puppet are three of the biggest configuration and system automation tools, but there are plenty of commercial products out there that offer monitoring components.

Challenge: Learning a new skill or software can be stressful, but automation is an absolutely essential skill to learn. That's particularly the case when executing on a tight deadline.

Lesson: Necessity often forces action. If you don't have remote monitoring and automation in place, then there's no better time than now to figure it out.

3 Things to Consider When Purchasing Software

Cloud-based software models make it increasingly simple to scale up or down licenses. That's particularly true for productivity suites, collaboration tools, and other seat-based licenses. For instance, Microsoft makes it relatively easy to add new Microsoft 365 seats to an existing plan. Similarly, Zoom, Slack, and other collaboration products offer tiered pricing. Upgrading enterprise software, however, may require a phone call or email to a representative to increase (even temporarily) essential software for VDI, RDS, and VPNs.

Most of the solutions employed during this difficult time will lean heavily on how you connect to your office or datacentre. Cloud services are amazing in this kind of scenario because all you need is an internet connection and you are good to go. However, there are many businesses that have lagged behind this trend and are not in a position to quickly and easily connect to their data.

Challenge 5: Not Enough Licenses

In almost every case, IT administrators had to purchase more VDI, VPN, softphone, and productivity and collaboration software licenses to accommodate their entire workforce going remote. In some cases, they simply purchased enough licenses for every single person in the company. In other cases, license purchases were done on an ad-hoc basis.

Planning is essential — particularly when attempting to quickly deploy a workforce remotely. To review from the section above, you'll need to be able to answer these three questions:

- How many people will be remote?
- Who will be remote?
- How long will they be remote?

Once you have the answers to these three questions, you'll be able to implement one of three solutions to ensure everyone has licenses to the tools they need to work at home.

Solution 1: Free up unused licenses

It may be possible to free up licenses for software by reassigning seats from on-site employees to remote employees or simply shuffling licenses around. Enterprise software often has a management and monitoring dashboard so that administrators can quickly see who is using their software seats and who is not. If not, then work with HR and department or team leads to determine what's absolutely necessary for employees' jobs. Similarly, remote services may temporarily replace on-site licenses. It may be possible to lower license counts for unused on-site services without penalty.

Challenge: Not every software has a robust administration dashboard, and it's possible that needs change when moving from on-site to remote work. For instance, someone may need the full version of Adobe Acrobat and eSign capabilities while at home because they used to scan and print documents at work.

Lesson: Usage data coupled with communication with HR, team leads, and company leadership are essential when dividing limited resources. Regular monitoring allows administrators to know who is using what license and can help you make decisions.

> ***I have colleagues who work at companies where remote work has been catered for, but not at scale. This means that basics like soft phone extensions and even VPN connection licenses are simply not enough to go around for everyone."***
>
> - Graeme M.,
> Durban, South Africa

Solution 2: Buy more licenses

It may seem simple to buy more licenses — and it may be for most software. But also take into consideration Microsoft has an entire certification exam dedicated in part to Microsoft 365 pricing and plans. Additionally, it's not as easy as adding licenses to a shopping cart for many vendors. You'll need to get on the phone and update your SLAs.

Challenge: Month-to-month licenses are often more expensive than annual subscriptions.

Lesson: Talk to your vendor sales representative about temporary licensing. In light of the COVID-19 crisis, many companies are banking on goodwill and may be able to cut deals not typically available during normal operations.

Try getting in touch with your vendors and see if you can get licenses and seats provisioned during this time. Also, it doesn't hurt to ask if you can temporarily purchase licenses. If you can be creative during this time then you might be able to get your team back online sooner rather than later. If this is not an option for you, then coordinating access with your colleagues could be the solution. Draft an access schedule and share the resources that you do have.

Challenge 6: Installing and Learning New Software

Almost all the IT professionals interviewed ended up installing new software that facilitated remote work, like new collaboration software to VPN clients.

One systems administrator noted that they would occasionally have someone work remotely while on a business trip or ill at home. However, the process was highly individualized and ad-hoc. Installing a VPN client, setting up MFA, adding the user to a Group Policy that allows remote access, and educating one user is relatively easy. Attempting to scale those processes necessitates a configuration manager like Microsoft SCCM — and good documentation.

Challenges: Installing and configuring software can be done relatively easily with the right tools. The greatest challenge is training users on how to use the new software effectively while remote. That's particularly the case when the user is remote.

Lesson: Develop documentation for the most common processes you expect your users to need on multiple operating systems, and host the documentation somewhere public like a SharePoint and Confluence site. Knowledge-base libraries also can easily be shared out in an email or referenced by support.

Challenge 7: Granting Permissions on Active Directory

Three of the 10 IT professionals interviewed found they had to adjust permissions to allow their users to work remotely, which is not surprising. Security-conscious administrators should limit remote access for anyone who doesn't need it.

Group policies are an essential timesaver when attempting to get everyone prepared to go remote. In this case, it's better to think ahead about the privileges to assign users rather than field support calls from the field.

Challenges: There are inherent security concerns with sending users to work outside the confines of a well-protected enterprise network. Make sure your users can access the resources they need to do their job, but also maintain a strong security posture with password requirements and multi-factor authentication.

Lesson: Think about the resources your users will need to access remotely — and develop an automated process to grant them least-privilege access by department or job role.

Remote desktop is already turned on by default for our computers in order to help us manage them. However, we typically did not add users to the "Remote Desktop Users" group because most users do not remote into their machine. Administrators do not need to be added to this group because they already have the permissions required for RDP access. We started by adding these one-by-one but that was a very slow tedious process. There is a better way through Group Policy.

4 Solutions to Help Users with Home Internet Connectivity

Internet connectivity is the bread and butter of any full-time teleworker. Nothing kills a day's productivity (and your patience) like a sluggish connection. With all employees tunneling through the VPN, it is no surprise that your throughput will be affected. However, there are steps you can take to maximize your internet bandwidth and ensure a productive work environment.

Challenge 8: Home Internet is Too Slow

Every IT professional surveyed cited issues with users' home internet as a source of support calls and troubleshooting.

In a business environment, you have full control over your network. Wireless access points are positioned and fine-tuned to kill dead spots and maximize bandwidth. All that goes out the window when everyone is working remote and connecting to the network with a VPN.

While home internet is typically not the responsibility of IT professionals, it's also not typical to suddenly hurry users to work remotely. To help their colleagues maintain internet connectivity in their homes, IT pros helped in the following ways.

Solution 1: Help troubleshoot wireless connections

The IT professionals surveyed experienced the full gamut of wireless issues from connectivity to bandwidth issues. Here are the most common recommendations in regard to wireless internet connectivity.

Check internet speed. Your first step should be to check internet speed. Luckily, that's easy enough. You can use a tool like Ookla Speedtest or Comparitech's speed test (which raises money for charity) to check your bandwidth if you're unsure.

Kill unneeded processes. One of the first things you can check is whether or not there are any applications eating up your bandwidth. Verify this by pressing CTRL+ALT+DEL and opening up your task manager. On the processes tab, look at the column titled "Network". If there is a large percentage of resources dedicated to that column, end the processes that are to blame, unless they are critical for your job.

Move close to the router. One of the best remedies for slow internet is simply moving closer to your router. Wireless can get finicky the further away you are from the access point. If you're set up in a back bedroom, garage, or basement, you may need to reposition yourself or your router for better access.

Limit bandwidth. If your spouse, children, or roommates are at home with you, ask them to refrain from streaming videos or music. These actions can hog significant amounts of bandwidth, and cause teleconference calls to drop. It's an escalated measure, but you can even get into your router and adjust the quality of service (QoS) settings to prioritize traffic from your work computer on the network. If all else fails, you can start blocking sites and applications.

Solution 2: Suggest a wired connection

If possible, send everyone home with a length of ethernet cable and make documentation available on how to select the ethernet rather than a wireless card. This is particularly useful for users who are sent home with their desktop computers.

Challenge: The primary challenges with supporting and troubleshooting home network connections are the variety of routers available — and the location of the router.

Lesson: A wired connection is preferable to a wireless one, but it may be difficult to achieve easily given router placement relative to the user's workstation at home.

Solution 3: Have them talk to their ISP

Encourage your users to contact their ISP for support. At the time of this writing, Comcast and T-Mobile were offering packages that either provide free internet access, increased bandwidth, or reduced prices for a period of time due to the COVID-19 epidemic.

Challenge: You don't want to pass the buck while trying to support your users, but there are some problems you simply can't solve. Like many other services, ISP support centers are working remotely, too, while trying to handle high volumes of calls.

Lesson: Confirm to the best of your abilities that the issue falls on the ISP.

Solution 4: Provide mobile hotspots

In the event that a user doesn't have internet at home or slow internet, mobile hotspots are a good solution. One IT professional's company distributed mobile hotspots to employees with no or slow internet.

Challenges: Mobile hotspots rely on cellular coverage, which is limited in some rural areas of the United States. Hotspots are also relatively expensive for the company, but the show of support it shows to users is priceless.

Lesson: Make every effort to provide users with the resources and training they need to work remotely — in all situations.

How to Prepare Your VDI Infrastructure

Virtual Desktop Infrastructure can best be described as “any device, anywhere, anytime”. This statement spells out with perfect clarity the promise that VDI represents. Remote users should be able to access local resources from any device, anywhere, anytime.

Both during normal operations and while remote, cost savings, security, and convenience are the primary benefits of VDI. It’s often the case that you have to sacrifice one for the others, but VDI allows all three.

Just 10 years ago businesses wouldn’t have had the capacity to allow hundreds of thousands of employees to work from home. Even now, it has been a struggle for some companies to get the infrastructure in place rapidly, but at least it’s now within grasp — and there are plenty of options.

Knowing Your VDI Options

Recent efforts in the end-user computing (EUC) space have lumped VDI into a group of solutions commonly packaged as a “workspace experience”. These technologies typically include the following:

- Desktop Virtualization Solution
- Application Virtualization Solution
- Endpoint Management Solution
- Gateway with Configurable Options for Accessing Other Internal Resources

Collectively, these fully encompass the workspace experience and it makes sense that vendors would package these as a one-stop-shop solution. Understanding the differentiators between these individual products and the options available empowers one to apply the right tool for the job.

Types of Desktop Virtualization

Desktop Virtualization includes a broad range of solutions — all with the end goal of providing a desktop experience to the end-user. Below, we'll outline their slight variations.

VDI. VDI refers to a platform whereby users access individual virtual machines that are hosted on virtualization servers and are presented with a familiar desktop operating experience. For most, this solution provides the best user-experience while being the most expensive.

Published desktops. Certainly, the most akin to VDIs, published desktops utilize the same virtualization servers while offering the same desktop experience. The differentiator here is that server OSes are used to allow a many-to-one ratio as they can be licensed for session sharing. This allows for greater user density and reduced costs. The downside is a potential risk to the user experience with user sessions potentially negatively impacting one another.

Remote PC access. Likely the simplest of all the solutions, remote PC access enables accessibility to physical endpoint PCs through the help of a software agent installed on the endpoint. This solution barely fits in the desktop virtualization platform, as it's more comparable to your typical RDP session with the added software enhancements of your chosen VDI solution's protocol. In a pinch though, this solution can be implemented swiftly and provide users with internal access without the overhead of building an entire infrastructure.

Local desktop virtualization. Local desktop virtualization uses the client's endpoint to run another desktop instance on the endpoint device. Eliminating the benefit of having the virtual resource alongside the internal data and applications, this solution normally only becomes viable for companies with little reliance on internal applications.

Desktop Virtualization vs. Application Virtualization

The argument for application virtualization over desktop virtualization is often approached with the question: "What do users care about once they log on to their desktops?"

The answer: Their applications. Application virtualization takes the idea of published desktops a step further by presenting only the application window for a designed application when a user launches a session. This approach can make sense for institutions with a limited number of applications and/or

little integration between applications. As you can imagine, though, for some applications where users need to interact with highly integrated applications the lack of a full-desktop experience can prove challenging for the end-users.

Fundamentally, application virtualization is a sound solution with years of proven viability. What's best for you will certainly depend on your particular use case.

Endpoint Management Solutions

Unifying the end-user experience is more easily handled when you have some level of control over the devices accessing your environment. This is where endpoint management comes into play. Going by several different names (unified endpoint management, mobile device management, etc.) endpoint management grants the ability to provide a consistent configuration and thereby some level of consistency for your end-users. In addition, endpoint management can enforce security controls around how your endpoints store and interact with enterprise data.

Gateway Options

Depending on your chosen VDI solution, the external gateway options available to you will vary. The standard options include:

- Access Gateway for Desktop/Application Virtualization – Provides external access to a VDI, Published Desktop, or Remote PC Access.
- VPN Tunnel – Provides end-to-end access from the user's endpoint to internal resources.
- Secure Web Proxy – Provides external access to internal web resources.

Additional options can include some variations allowing for an isolated VPN for single application traffic or external access to an internal file share. Collectively, the objective is to grant secure access to internal resources, but as you can tell there are many options.

Challenge 9: Planning for Infrastructure Resources

The number one thing an engineer will likely think about in preparation for a sudden surplus of users will likely be compute, memory, storage, and networking capacity. To prepare for rapid deployment of resources, it's important to have metrics and historical data to evaluate where you are and what you will need.

Challenge: Operationally, trying to look ahead at the resources you'll need is referred to as capacity planning. However, the unusual nature of the COVID-19 pandemic turns this into a business continuity planning (BCP) concern, which means figuring out how to keep the lights on rather than optimizing processes.

Lesson: Follow your vendor's best-practices for capacity planning and the handful of golden rules such as a minimum 'n+1' for host failures, and the 3-2-1 rule for backups.

Challenge 10: Ensure You Have Enough VDI Licenses

Different solutions handle licensing in different ways, but the overall objective here is to make sure you are properly licensed to handle the surge. In terms of license count, ideally, the VDI environment should use a least-privileged access model. Both licensing and least-privilege bring with it challenges.

Challenges: Every person who needs VDI access should have a license — and only be given access to what they need. If you're not using this model currently, pull from any historical metrics and data available to you to get an idea of currently unlicensed users and rectify the situation with the vendor. As you are getting these numbers together, make sure you understand your license model (concurrent vs. user/device vs. named user) and the consequences of breaching your allotted licenses.

Lesson: The last thing you want is user connections being denied and your team scrambling to identify the issue — only to find out you're out of licenses.

Challenge 11: Monitor Your VDI Solution

Monitoring your VDI solution during this period of remote work should provide you with the typical up-down statuses and glaring red-flags that require reactive

response. Beyond that, it's important to have actionable insights that will allow your team to respond efficiently and effectively. These typically come in the form of trend monitoring.

A great example of this would be Citrix's HDX Insight product that performs a deep analysis of the protocol allowing for end-to-end visibility that can quickly pinpoint issues down to the root cause.

Challenge: With everyone remote, trend monitoring will help you identify the escalation of potential issues and respond proactively, which is where you want to be in a crisis situation. However, there are plenty of factors over which you have no control — namely home internet connections. Monitoring will help you determine whether a problem is system-wide or unique to the user.

Lesson: When the workforce starts working remotely, the last place you want to be is pointing fingers on whether it's the internal infrastructure or a user's lousy internet connection.

Challenge 12: Any Device, Anywhere, Anytime

One of the main benefits of VDI is that it enables users to connect to an internal machine with any device. The promise of virtualization makes it possible to deploy hundreds or thousands of employees to work from home with relative ease. However, the "any device" part of the VDI promise comes with its inherent difficulties.

Challenge: The "any device, anywhere" model becomes problematic when it comes to supporting even a moderately sized workforce with many devices. Will they be provided a company device that is pre-configured for remote access? Or will they be using personal devices, which you'll have no control over? The answers to these questions will surely determine the level of challenge your users will face when connecting. Plan on supplying documentation for how to connect and how to configure personal devices should you have to rely on a BYOD strategy.

Lesson: Fumble on documentation and you can plan on your service desk being overwhelmed with calls for assistance in setting up endpoints.

The Many Issues with VPNs

For many companies, VPNs are an essential part of both security and the ability for users to access local resources remotely.

If you don't have VPN servers and clients installed, you have options in a pinch. Small businesses may be able to use a hosted VPN service such as Hamachi, but for larger businesses, a VPN should be built onsite at the router/firewall level. If you already have a firewall appliance in place, such as a Palo Alto Networks firewall or Check Point firewall, you probably already have a VPN. It just needs to be configured. For the rest of us, building a VPN is best accomplished using IPsec.

Modern VPNs are relatively easy to use and setup. However, VPNs still aren't always intuitive for unaccustomed users. For the IT professionals we interviewed, VPNs were the most problematic software to troubleshoot and train their users on.

Challenge 13: The Many VPN User Issues

Just about everyone we talked to experienced VPN issues — some technical, but mostly user-related. With their workforce remote, many companies have needed to securely extend their LAN for their custom applications to work properly, or for access to premise-based file shares.

There are the most common VPN issues that shared with us, and something to consider when sending your workforce remote:

The software requires a VPN to access resources. One of the issues that you may run into is that users will try to connect to a vendor application without completing a VPN connection. Say your proprietary software needs to access a SQL database that is running on one of your servers. Without accessing the network there is no way to communicate with it. Because the connection is always there at the office, it may not be immediately apparent to an everyday user that the server is not accessible from the outside.

Visually differentiate between remote and local sessions. Some users have a really hard time switching between their remote session and their home PC. If they are running the same operating system and have the same color scheme, it can get confusing quickly. Especially for someone who is not used to handling remote sessions. Thankfully, this is a simple problem to fix. Setting a desktop background and changing the style or the color scheme of the taskbar makes it easier to differentiate. Basically, anything visual that can clearly define which machine they are looking at.

Don't let users shut down their office desktop. Users have a daily routine. Quite often shutting down the machine at the end of the day is part of that routine. Ordinarily, that is fine. However, because every user is remoting into their machine, if their desktop gets shut down, someone will have to go to the office to turn it back on.

Create documentation for file management. Users may have a hard time getting a local file (on the computer they were using at home) to the remote machine (in the office). For example, if a user scans a document using their home scanner, they will need a way to get that file over to the new machine. This used to be quite a hassle requiring things like FTP servers or file shares. Make it simple for your user. You can copy and paste things from your PC directly into the remote session — the same way you would if you were just copying them between folders. This works with both Windows Remote Desktop and Teamviewer.

Challenge: The primary challenge here is the sheer quantity of unknowns introduced in a rapidly deployed remote environment — and the volume of support calls. During normal operations, you should know with relative certainty that everything was configured properly when you sent the remote employee out the door. You also have the luxury of time to troubleshoot a problem thoroughly.

Lesson: Rely on best practices. They'll get you through. Use monitoring, basic troubleshooting, and common sense to pinpoint a problem, then document it in case it comes up again.

Challenge 14: Slow or Lagging VPN Connections

A couple of IT professionals who were surveyed found that their users were experiencing significant lag on their VPN connection, which significantly slowed down work and frustrated the users. After attempting to troubleshoot the network, they built out several gateways at other locations and routed through existing MPLS connections to alleviate the issue.

Challenge: Troubleshooting is one of the most difficult things to do — even in a relatively stable enterprise environment. It's easy to blame the home network or attempt to find a hardware or resource solution for a speed issue.

Lesson: Know the options you have to allow users to securely access network resources while remote requires networking expertise.

Challenge 15: ISP Won't Allow VPN Connections

One IT professional found that the ISP used by several remote employees didn't allow VPN connections. While that may be common for university, work, or pay-per-day internet, most ISPs allow VPNs.

Challenge: Troubleshooting an ISP issue can be difficult "because everything appears fine, but it just will not work." Circumventing ISP restrictions on VPNs may sound like a fun exercise, but it's not something you want to embark on with your users. There's no other way to fix this than talking to the ISP or perhaps finding a different ISP.

Lesson: Don't start with the ISP, but don't rule it out. While troubleshooting, be thorough and use best practices as you trace issues.

4 Ways to Scale Support: Being Available

For small companies, support may be routed through a ticketing system. It may also be more ad hoc and personal. In either scenario, you'll likely be working with a lot of users who have never been remote, so make sure they know how to contact the help desk from home, access documentation, and don't feel stranded and frustrated.

All the documentation and planning in the world is all for naught if you don't effectively communicate to your end-users and support staff what is expected. Communication is likely the most important aspect of any emergency-planning scenario. Orchestrating resources and people toward a common goal is no easy task. But always consider the perspective of others, how you would like for them to respond, and how you can facilitate that response.

Challenge 16: Knowing How to Contact the Help Desk

Several of the IT professionals we interviewed noted that despite their best efforts users were still having trouble contacting IT for support.

You'll likely be working with a lot of users who have never been remote, so make sure they know how to contact the help desk from home, access documentation, and don't feel stranded and frustrated. When an entire office rushes into remote mode, it's a very simple thing to overlook. There will be users with network issues who may not know the help desk phone number or how to access documentation. If possible, host documentation publicly and communicate regularly with staff and leadership.

Challenge: Help desk contact information and essential documentation may be accessible from an internal knowledge base like SharePoint or Confluence. During normal operations that's fine. However, what if the documentation to access the VPN is only available by VPNing into an internal resource?

Lesson: Make sure your users know how to contact you.

Challenge 17: Troubleshooting a Problem Over the Phone

When you try to troubleshoot a problem over the phone, all you have to go by is the user's description of what they see on the screen. This can turn a very simple problem into an unsolvable conundrum — mainly because they do not see the screen the same way you do. Things that are immediately obvious to you when you see them they will not catch.

Use a remote desktop tool rather than relying on a user's description of what they see on the screen. One IT professional noted "this can turn a very simple problem into an unsolvable conundrum. Mainly because they do not see the screen the same way you do."

He recommended Teamviewer QS, which is a free software that is very easy to set up, and it will allow you to see exactly what the users see. It enables you to take control of their machine without having to route Remote Desktop or VPN into the network. All they need is an internet connection. Teamviewer is just one example. There are many alternative solutions.

Challenge: There are inherent issues with training your team on new software in the midst of a flood of support calls, but it'll be easier than the alternative.

Lesson: Seeing the problem and being able to drive is easier than having it described and relying on memory of an operating system to fix a problem.

Challenge 18: Keeping Documentation Current

Every single IT professional we interviewed mentioned documentation as the key piece that either got them through — or the element they wish they had. While often overlooked, documentation is vital to the success of any IT operation. When it comes to documentation there can be several target audiences. These can be broken down into four categories: management, peer, support, and end-user.

Management documentation provides a high-level view of the environment. Peer documentation is akin to architectural blueprints and standard operating procedures. Support documentation and end-user documentation can really shine during a crisis. In particular, documentation for the end-users will let users know what to do, thus cutting down on support calls. Documentation is also valuable to support staff. Once they know the problem, they can refer to documentation, which enables the service desk to assist users consistently.

Previously when a user was going to be working remotely, we would work with them to set up the VPN and the Remote Desktop Connection. This was not a big deal since we only ever had to do one user at a time. If there was something difficult to understand in the documentation, they could simply come to us and we would explain it. When your entire office is going remote this becomes a much bigger hassle. The best way to avoid this is to have up to date documentation.

Challenge: Documentation can be a challenge in itself — both in quality and keeping it current. While getting everyone remote, it may take more time to document a process that's regularly occurring in support calls, but it will save time in the long run. When developing that documentation make it clear. Break the process down into steps, and leave nothing out. Where possible use pictures and screenshots.

Lesson: Done correctly, support documentation can elevate your service desk, allowing your engineers to focus on managing the crisis and not just responding to it.

Challenge 19: Training Your Staff

Along the same lines as documentation, training for the service desk staff is essential to empowering your service desk and keeping them from having to forward tickets to already busy engineers. At this point you want your engineers focused on the bigger picture. Their focus should be on prevention and remediation of issues. Effectively training your support staff ahead of time is key to operational efficiency.

Challenge: In larger companies, most support is routed through a central service desk with dedicated staff and a clear escalation structure. In these cases, it's also typically remote, so call volume may increase, but fundamentally it's no different than a busy day on the help desk. For small companies, training for everyone going remote means thoroughly learning the technologies that comprise the remote infrastructure.

Lesson: There's no substitute for well-trained technical staff. By training just 30 minutes a day with CBT Nuggets, team members will be prepared for certification exams, advancement in their career — and even a mass exodus of users going remote.

Make sure your VPN instructions cover different Operating Systems that the users may be accessing with. In some cases you will need to include documentation for Notepads and even smart phones. Take lots and lots of pictures and test everything thoroughly. Last week we found a lot of mistakes in our documentation that gave the user erroneous instructions which would create a ton of confusion.

Pay attention to the VPN settings. In our case we are using Windows Server VPN "Routing and Remote Access" service. The default settings for Windows when creating a new VPN connection were sufficient. On some devices we had to specify PPTP as the VPN protocol.

CBTnuggets

Becoming Remote Ready

We developed this whitepaper as a way to consolidate the challenges IT professionals experienced — and share the solutions they found to ameliorate them. Some challenges were esoteric and industry-specific. Some solutions may have been ad hoc, but not necessarily scalable. Most, however, were common across companies and industries.

When everyone is back in the office, you should have an after action report about what went well and what went wrong. It's evident now that the capability to work remotely should not only be an elective, but necessary to continue business operations in the event of a pandemic or natural disaster. Start planning your remote working strategies early. You will need input from everyone involved so that you have all the parameters to start testing your remote working solutions.