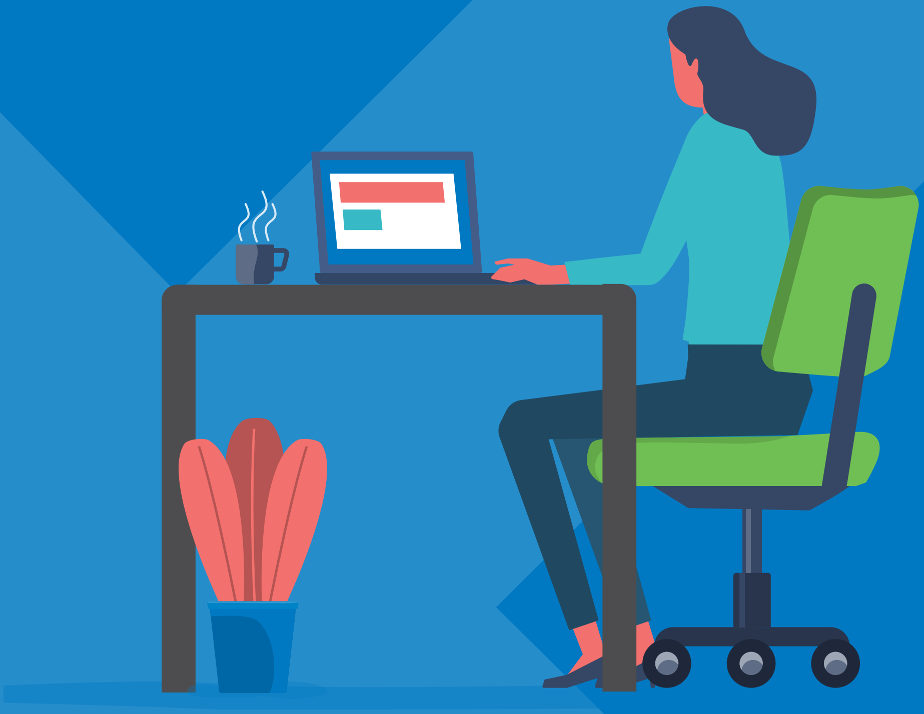
A Comprehensive Guide to

Setting Up IT for Remote Work

FROM THE MANAGED SERVICES EXPERTS AT TPX



Executive Summary

The past couple of years has revolutionized the way we work. Thanks to an unprecedented global pandemic, the world's businesses were forced to adjust to working outside of a traditional office to maintain social distance and keep everyone safe from infection. Thankfully, we now have the technology to support successful and productive remote work – and it looks like it's here to stay. And that means new processes for IT management.

With that in mind, our Comprehensive Guide to Setting up IT for Remote Work details everything you need to keep your remote employees connected, along with suggestions for making the operation as seamless and simple as possible.

Key Takeaways

Post-pandemic, 76 percent of global employees want to continue working from home. On average, Americans would like to work away from the office 2.5 days per week.

There are three types of remote work, including Work from Home (WFH), Work from Anywhere (WFA) and Hybrid Work, which is a combination of any or all of these.

Remote work provides several notable benefits, such as improved work-life balance, increased employee happiness, company access to more talent, augmented productivity, and reduced cost and carbon footprint.

Successful WFH/WFA deployments hinge on Internet connections/ speeds, security measures and collaborative platforms. Without these key measures in place, productivity could suffer.

Partnering with an MSP enables you to design and deploy effective remote work solutions often for less than doing it in-house. Plus, service level agreements (SLAs) put guarantees around timelines, support, uptime and quality of service (QoS).

Table of Contents

PART 1

What Is Remote Work?

Remote work refers to employees working from their homes or other locations, with a particular focus on the technology and mobility solutions that facilitate their work. Remote work, which also often is referred to as “telecommuting,” has decentralized the day-to-day functions of many companies, moving some, most or all operations away from a traditional office environment.

What Are the Types of Remote Work?

Remote work can take place practically anywhere with an Internet connection, so it inherently looks different from person to person, business to business, location to location. The three main types of remote work include:

- **Work from Home (WFH):** In this scenario, the employee is almost entirely and permanently assigned to working from home, using their home Internet to access applications in the cloud.
- **Work from Anywhere (WFA):** In this scenario, the employee is enabled to work from anywhere with reliable Wi-Fi, usually via a secure VPN or through a mobile firewall.
- **Hybrid Work:** In this scenario, the employee works from multiple locations – any combination of working from home, working from anywhere or working in a traditional, centralized office.

Why is Remote Work on the Rise?

Companies switch to remote work due to its many benefits like significant real estate cost savings, greater access to talent and a more loyal workforce. The rise in remote work before 2020 pales in comparison to what has happened since the pandemic. Technologies that once enabled select employees to work remotely became an absolute necessity for a majority of workers practically overnight, bringing about an unprecedented shift in the way we work.

In an August 2021 report aiming to dispel myths about remote work, Gartner researchers called the COVID-19 pandemic "the biggest experiment in the history of work." Companies all over the globe grappled with unknown timelines, fluctuating protocols, the responsibility of keeping employees safe, and the obligation of keeping their businesses up and running. It was – and still is – unlike anything we've ever seen. And it will change how we work forever.

PART 2

What Are the Benefits and Challenges of Remote Work Models?

As the saying goes, there are pros and cons to everything, and that includes remote work. However, if your work environment is going remote (partially or fully), there are proactive measures you can take to mitigate the challenges of WFH and WFA.

	BENEFIT	CHALLENGE	PROACTIVE MEASURE
Employee Focus	WFH can provide a quiet space for employees to concentrate, especially compared to open offices.	For some, WFH can increase distractions if there's no designated home office space or pets or kids in the home need attention/ assistance.	Encourage employees to be open about distractions so adjustments to schedules and projects can be made to ensure continued productivity.
Independent Work	WFH can increase an employee's ability to work independently and autonomously on projects without excessive meetings or input.	WFH employees might find they miss being part of team projects and collaborative environments.	Institute additional team-based activities, whether in person or via digital platforms, to help team members feel connected and supported.

	BENEFIT	CHALLENGE	PROACTIVE MEASURE
Work-Life Balance	No commute sometimes means more time with family or for exercise, chores, etc. Additionally, many employees can work from various locations while caring for or visiting loved ones.	Sometimes, a home office that's only steps away or a work setup that's mobile can be an invitation to work too much. Overworking should be monitored as much as underworking, and you should encourage your employees to unplug.	Set clear parameters and expectations. Start by acknowledging that WFH and WFA arrangements are indeed different from working in a traditional office. Being honest, open and communicative from the get-go is the best way to take on this challenge.
Productivity	Several reports show increases in productivity for WFH and WFA teams due to fewer distractions.	Some managers fear employees will be less productive if not made to work in a traditional office setting.	Build trust among teams and continue to keep an eye on outcomes. Productivity is usually fairly easy to monitor – at least cumulatively.
Talent and Skill	WFH gives you a wider pool of talent, thanks to the lack of geographic limitations.	Training and onboarding can be challenging with a dispersed workforce.	Have the right collaboration technologies in place to keep employees in the loop at all times.
Employee Satisfaction	WFH and WFA means happier employees and lower turnover for many companies.	The challenge is staying continually in touch with how employees are feeling especially after the novelty of WFH wears off.	Maintain personal relationships with employees to make sure you know how they feel. This practice is just an amped-up version of what you would do in an office environment.
Cost	Eliminating or downsizing your brick-and-mortar location means lower overhead. Additionally, less business travel is required as people continue to embrace WFA.	While real-estate and related costs may go down, managing new costs could become challenging because employee needs vary from one situation to the next.	Hiring an MSP to help you manage your remote workforce's needs can help to mitigate this challenge.

	BENEFIT	CHALLENGE	PROACTIVE MEASURE
Carbon Footprint	WFH and WFA reduce the carbon footprint for your company and its employees.	Is there really any con here?	Be intentional about measuring the adjustments to your footprint. You might be surprised at what a difference it makes.
IT Issues	Thankfully, we now have sophisticated communication and collaboration technologies to support seamless remote work.	WFH and WFA present unique challenges when it comes to connectivity and security.	One way to ensure you’re providing the appropriate tech, security and support to your WFH employees without overwhelming your IT team is to partner with an MSP.

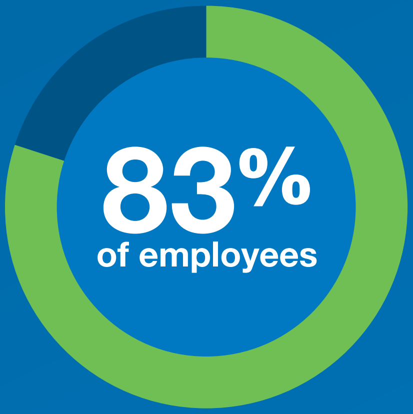
PART 3

What Is the Outlook for Remote Work?

According to the **Global Work-from-Home Experience Survey** conducted in 2020 by Global Workforce Analytics, 97 percent of North American office workers worked from home more than one day a week during the pandemic (88 percent globally). It was a mass exodus like we had never experienced. Before COVID-19, a whopping 67 percent had not worked remotely on a regular basis (69 percent globally).

While many workers are being asked to return to the office, there is a growing resistance to do so, as we have become accustomed to the benefits of remote work.

Global Workforce Analytics found that 76 percent of global employees want to continue working from home. On average, Americans would like to work away from the office 2.5 days per week. Since meeting those demands is essential to talent recruitment and retention, working 50 percent of the time from somewhere away from a centralized office environment is not a short-term trend to accommodate – remote work is here to stay.



83% of employees say they are at the same productivity level — or higher — working from home compared to the office.

– State of Remote Work 2021, Global Workforce Analytics

What Are the Growth Projections for Remote Work?

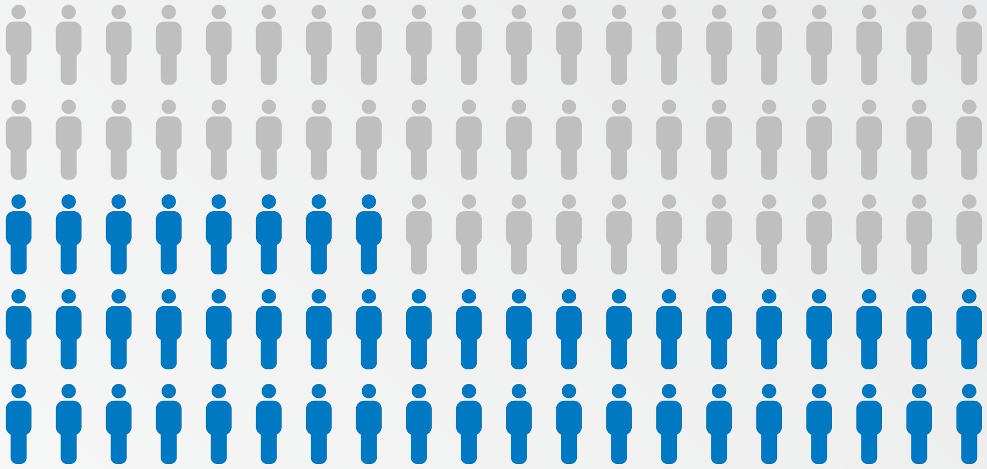
Gartner research, as reported in HR Leaders Monthly, suggests 48 percent of employees will continue to work remotely at least some of the time in the post-pandemic world, compared to 30 percent pre-pandemic.

Businesses are beginning to make commitments to remote workforces. Since the pandemic began, 22 percent of companies have reduced their office space, while 21 percent have increased their team footprints, according to the **2021 State of Remote Work report from Global Workplace Analytics**.

Many companies also have begun to make significant investments in infrastructure and applications to support remote work moving forward. According to Nigel Fenwick, Vice President and Principal Analyst at **Forrester**, the **firm's latest research** on digital business maturity shows that business leaders are now considering further digitalization as their most critical priority moving forward.

48% **of employees will continue to work remotely at least some of the time in the post-pandemic world."**

– Gartner



PART 4

What Are the Challenges in Setting Up IT for Remote Work?

Insecure Residential/Public Connections

Using residential and/or public Internet connections can be among the biggest concerns with WFH/WFA—especially on the security front. Unsecured Wi-Fi connections in public locations are well-known, longstanding concerns. However, poorly secured home networks have been widely exploited by cybercriminals during the pandemic, when employees began working from home.

Managed endpoints and VPNs can go a long way toward reducing threats from remote employee connections—especially when paired with security awareness training (see below).

Residential/Public Bandwidth Speeds

Poor connections can mean lost deals, misunderstood conversations, poor customer service and low productivity. Ultimately there are instances wherein WFA becomes work from “almost” anywhere. An employee’s home — or other remote location — must support an acceptable connection speed.

For employees at home, their broadband options are usually cable or DSL but, in some cases, fixed wireless or satellite. Some are faster than others, with access defined by geolocation.

Mobile remote employees using Wi-Fi from establishments (e.g., coffee shops, cafes, etc.) can often get usable connection speeds when they connect via their mobile devices or use them as hotspots over wireless carrier networks. 5G connectivity – which is becoming more widely available – is excellent at facilitating high-quality remote work. 4G is sometimes workable, especially in areas where there have been infrastructure upgrades in advance of 5G deployments. This, too, depends on the location and, of course, the employee’s job function.

Equipment

Most households have a computer, and nearly everyone has a mobile phone, but outdated equipment can become an issue when setting up for remote work. Many firms will realize the initial cost of setting employees up with equipment to support newer, more sophisticated collaboration technologies, whether voice, video, or data. Some devices (and software) deliver security at the employee location as well.

If you decide to allow employees to use their own devices to access company infrastructure, establishing clear “bring your own device” (BYOD) policies is a must. These policies should include security protocols, restrictions on sensitive information (particularly in industries with governing laws and compliance bodies, such as HIPAA and the SEC). BYOD policies should also include specifications on how much support your IT team can offer across so many differing devices and how much, if any, of the employees’ services will be paid for by the company.

Staying connected is literally and figuratively the most pervasive challenge for WFH models.

Staffing

Decentralizing your office also means decentralizing your IT department and help desk. Remote work also usually means more flexible schedules, and sometimes it means workforces spread across multiple time zones. Depending on the nature of your work, if you manage all IT functions in-house, you might consider ensuring support staff is on-call to address problems outside normal business hours.

Training

As a culture, we prefer to train people in person. That's why long-distance employees would spend a week at headquarters for onboarding, or why offices would gather people in conference rooms to go over new benefits or policies.

Applications are no different. And while we might prefer to train employees on critical apps by hovering at their desk and jockeying for the mouse, remote work doesn't allow for that. However, utilizing the right collaboration platforms can facilitate effective employee training, which is essential given that WFH and WFA are app-intensive.

Staying Connected

Staying connected is literally and figuratively the most pervasive challenge for WFH models. Finding the right voice and data applications for how your team works will help everyone feel like they still connect with each other.

Apps like Slack, Zoom, Google Drive, Microsoft Teams, and Microsoft 365 unite remote employees for easier collaboration. But since employees may be easily overwhelmed by multiple communications apps, all-in-one platforms like TPx's UCx with Webex, which facilitates voice, messaging, video, whiteboards, audio and conference calling, deliver significant productivity and morale benefits.

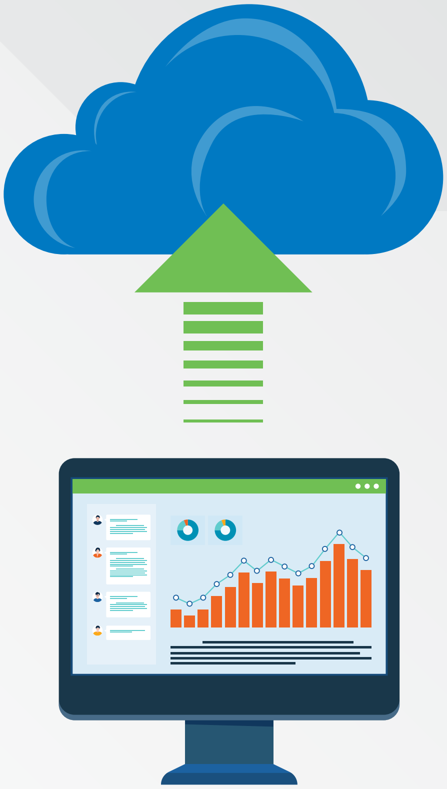
Remaining Collaborative

Remote workforces sometimes find it difficult to maintain collaboration and interaction among employees. While eliminating excessive watercooler conversations might be one of the benefits of remote work, small talk is still necessary to building camaraderie and trust among coworkers.

Here again, the apps and platforms you choose will have a big impact on how successfully your team continues to engage and collaborate. Many facilitate multichannel communications in a single app or suite, which keeps everyone connected while simplifying app sourcing and management.

Systems Access

When setting up employees for remote work, you must ensure they can access critical information, files and systems. Cloud storage applications such as Dropbox or Microsoft OneDrive are enough for some businesses. But, sometimes, applications specific to the line of business might be required. Advanced Unified Communications as a Service (UCaaS) offerings can facilitate access to CRMs and file-sharing as part of your overall collaboration package.



Security

Maintaining security is a challenge for any business, and when part or all of your workforce is remote, there are new security challenges to consider. As mentioned in the discussion of Wi-Fi risks earlier, endpoint security and VPNs are essential components, as are other managed security solutions. But given that humans are commonly exploited attack vectors via phishing, whaling, etc., security awareness training is indispensable.

And make sure you put policies and plans in place to ensure devices and applications are patched whenever needed to avoid exposing your network to unwanted threats.

PART 5

What IT Solutions Are Required for Remote Work?

Now that you're prepared to face the challenges of remote work and ready to reap all the benefits, what technology do you need to get started? Here's a list of the IT solutions required to enable your remote workforce securely.

Internet Access

Various types of broadband are available, whether that be cable, DSL, fiber-optic, fixed-wireless or satellite (in rare cases). Dedicated Internet is also an option for guaranteed uptime.

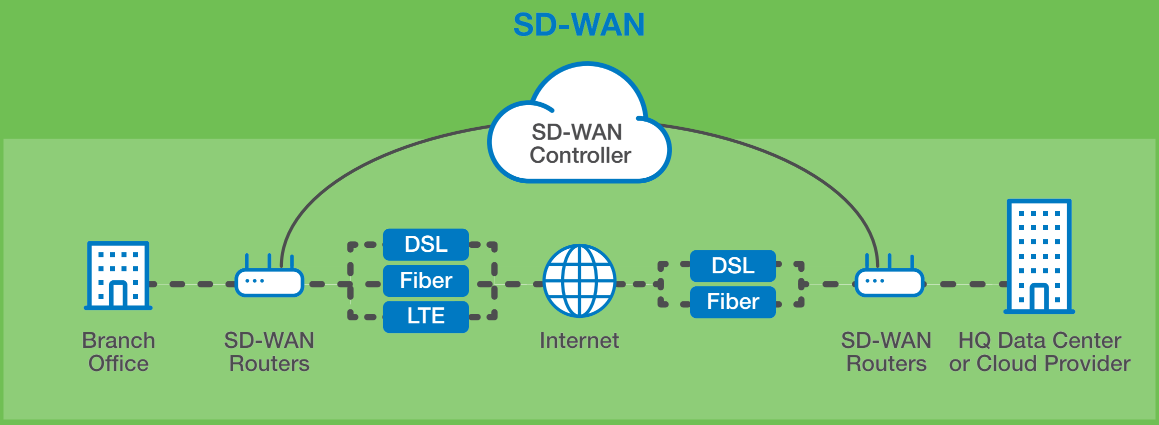
Software-Defined Wide Area Networking (SD-WAN) & Virtual Private Networks (VPNs)

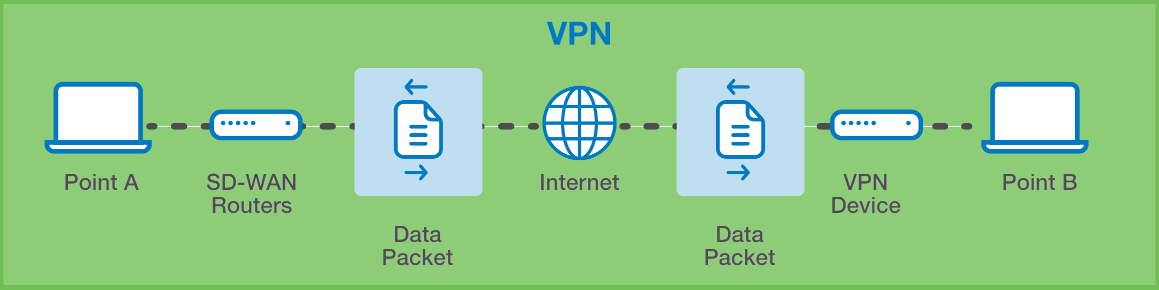
- **SD-WAN:** A Software-Defined Wide Area Network (SD-WAN) creates a software-based management layer over top of your network infrastructure, including low-cost broadband connections to deliver unprecedented control over routing and traffic prioritization.
- **VPN:** A Virtual Private Network (VPN) creates a safe, encrypted online connection to access the Internet. VPNs extend a private network across a public network, allowing secure sending and receiving of data cross the Internet.

Should You Deploy SD-WAN or a VPN?

Before the pandemic VPNs were the preferred choice for mobile workers and **SD-WAN** was deployed in branch offices primarily for cost reasons – SD-WAN was simply too expensive for remote-working employees. Now, economics for home use of SD-WAN for permanently remote employees work out better for the right business users who can't afford any downtime.

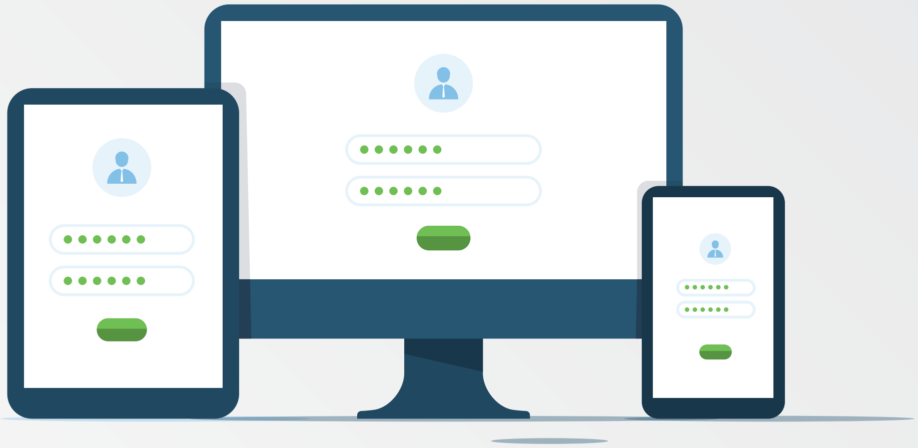
SD-WAN security is more flexible than a VPN, resulting in more persistent connections. SD-WAN also has more control, so work traffic and non-work traffic can be segmented, and priority is given to mission-critical applications like voice and video. With VPNs, all traffic typically is routed over the connection, including non-work traffic, with no prioritization in place – potentially resulting in reduced QoS.





Hardware

- **Router:** A router sends and receives data over a network. With many households running a variety of digital applications at any time, an employee's existing router might not suffice. You may need to fund an upgrade to a newer router for the best prioritization, speed and range.
- **Switch:** A switch enables you to connect all devices within a remote office, e.g., desktop, laptop, printer, server, etc.
- **Wi-Fi Access Point:** A Wireless Access Point (WAP) is an appliance that connects Wi-Fi-enabled devices to the network, essentially creating a WLAN (wireless local area network). The appliance connects to the network via Ethernet cable and provides wireless access to a designated range. A range extender also can be used to widen the reach of the wireless network or hotspot. Access points often pull double-duty as routers.
- **Laptop/tablet/phone:** WFH/WFA employees need appropriate devices to get the most out of their remote work experience. Devices should be selected based on the occupation and mobility of the worker. For example, someone with a lot of creative or design responsibility might need a larger screen display and more RAM than the typical user. And, if that person works from anywhere, he or she might also need a smaller, more portable laptop or tablet.
- **Camera**: Working remotely is usually supported by lots of video calls and meetings. If employee devices don't have good cameras embedded in them, add-on cameras are an additional need. Features such as pixel resolution, rotate-ability, automatic focus/light adjustment and mounting/portability will factor into choosing a camera. 720p or 1080p and 4K HD resolutions are ideal quality for the webcams currently on the market.



Communications & Collaboration

- **Cloud PBX:** A cloud PBX takes the functionality of a business PBX and puts it in the cloud, enabling remote workers with access to seamlessly route calls over the Internet to one another.
- **UCaaS:** Unified communications as a service (UCaaS) uses a cloud-based delivery model to combine your Internet-based phone system with other collaborative apps like videoconferencing and instant messaging.
- **Softphone:** A softphone is a piece of software that enables you to make calls over the Internet.
- **UC app:** Choosing the right app to integrate all of your communications functionality is vital. You need a mobile app that allows you to call, chat, videoconference and start online meetings from anywhere.

Virtual Call Center

Whether your company has five employees or 5,000, you can give your customers the impression of a large, professional organization with a hosted call center solution. This allows you to distribute inbound calls from a central phone number to groups of agents located anywhere.

Productivity Apps

Productivity apps like Microsoft 365, for example, give employees the ability to meet, share files, chat back and forth, etc., regardless of where they are. Productivity apps for remote workers should provide accessible, intuitive user interfaces (to facilitate independent work), along with a seamless experience. Interfaces should look the same to all team members regardless of how (system- and device-neutral) or where (home, office, anywhere) they are accessing it. What do you need to facilitate your team's productivity?

- Email platform
- File sharing capability
- Meeting platforms (voice and video)
- Document applications (creation, collaboration and storage)
- Spreadsheets (creation, collaboration and storage)
- Presentations (creation, collaboration and storage)
- Project management (with an easy-to-use interface, updated in real time)

Security

Layering security is vital for protecting networks, especially when you have remote workers.

- **IAM:** Identity and access management (IAM) is essential for remote work. IAM is a framework of policies and protocols that ensures only approved users access your network and files.
- **MFA:** MFA, or multifactor authentication, is a part of any good IAM strategy. Examples of MFA include security questions and access codes texted or emailed to a user.
- **VPN:** Setting up a VPN or virtual private network is a good option for providing remote employees secure access to your network via authentication and encryption.
- **Firewall:** A firewall establishes a barrier between an untrusted network, like the public Internet, and your trusted business network.
- **EDR:** Endpoint detection and response (EDR) monitors the various endpoints on your remote network in order to detect threats and respond to them.
- **Additional controls:** Other security controls include anti-virus software, IDS/IPS (intrusion detection system or intrusion protection system), web filtering (to block specific URLs or types of content), application control and DPI-SSL (deep packet inspection-secure sockets layer), and disaster recovery and backup.

Business Continuity

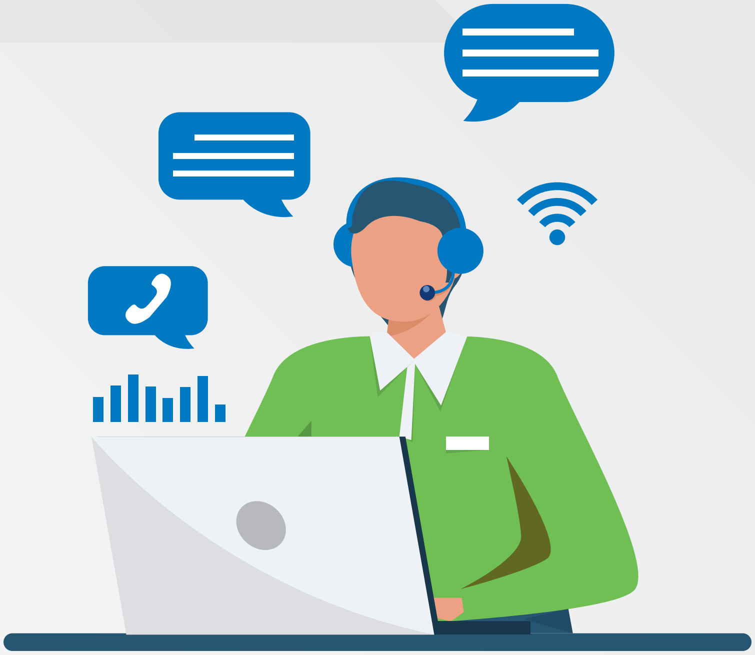
Business continuity planning is important to maintain service in the event of a service interruption, cyberattack or other disasters. Disaster recovery and backup services are also essential to achieving business continuity.

24/7 User Support

Dispersed workforces usually mean that some employees work earlier and/or later than others, requiring around-the-clock support for optimized efficiency and productivity.

24/7 Remote Management & Monitoring

Visibility into productivity, system health and security is needed to manage remote users effectively. Policy adherence, patch management and business continuity are all reasons to have 24/7 remote management and monitoring.



PART 6

Why Consider an MSP to Enable Remote Work?

Enabling remote workers securely and effectively has many moving parts. How will employees access the network and with what devices? Is the transmission secure and reliable? What apps are needed and do they work well with each other? Have you secured the required licensing? How can you support disparate locations, equipment and forms of connectivity?

These are just a few of the questions that your business must answer to get set up your IT environment for remote workers.

The professional expertise and practical experience offered by a managed service provider (MSP) can ensure those answers are informed by best practices learned over thousands of deployments.

An MSP's skills and scale also mean quicker time to success and lower total cost of ownership. Partnering with an MSP enables you to design and deploy effective remote work solutions often for a fraction of a cost of doing it in-house. And, with guaranteed service levels.

Typically, an MSP delivers applications and management services under a contractual service-level agreement (SLA). The SLA details qualitative and quantitative performance metrics that govern the engagement between the MSP and the customer, putting guarantees around timelines, support, uptime and QoS.

Key Benefits of MSPs in Remote Work Environments

Reduced Technology Costs

MSPs serve multiple clients with similar needs and spread-out financial costs between them, letting even small businesses take advantage of seven-figure technology investments like NOCs, SOCs and firewalls for a fraction of the price.

Domain Expertise

MSPs eat, breathe and sleep on IT solutions for customers of all sizes and can handle unique requirements. If you have a problem, an MSP has already run into it and knows how to solve it.

Specialized Talent

MSPs have specialist expertise in-house to design an optimized IT setup and troubleshoot issues.

Fast Scalability Up or Down

MSPs have to be able to serve large enterprises and have built the capacity to grow with companies or scale down rapidly as needed so they can adapt to any work environment.

Emerging Tech Know-How

MSPs are tapped into the most up-to-date best practices and standards, making them more effective than most internal IT teams.

Future-Proof Environments

Remote work deployments are built with business continuity in mind.

24/7/365 Support

MSPs have the resources and staff available to support companies and resolve issues at all hours.

Freeing Up Internal IT's Time

Business IT departments can be freed up to work on projects that proactively benefit the organization instead of putting out IT fires.

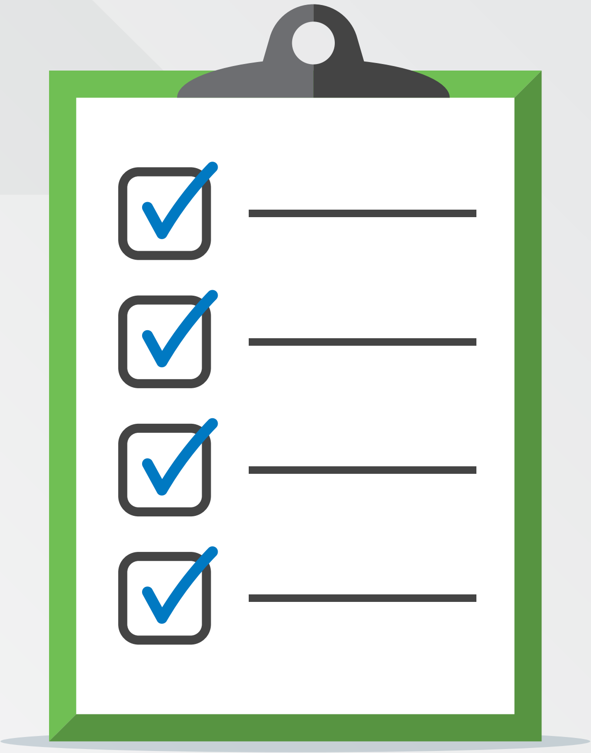
Network Integration

MSPs designing your remote work environment already understand how all your work-from-home solutions deploy over-the-top of your business network, leading to faster installation and problem resolution.

From Expertise to Extra Hands, MSPs Fill Gaps

MSPs can handle a number of complex or repetitive tasks in your remote deployments, including:

- Sourcing and managing IT infrastructure
- Procuring best-of-breed established and emerging technology
- Leasing equipment in an OPEX model to avoid capital expenditures
- Filling skills gaps in networking, integrations and applications
- Providing IT support for daily operations so internal IT can focus on other projects
- Delivering managed communications and collaboration services
- Offering technical and software training and support
- Sourcing and managing cybersecurity solutions, including security awareness training
- Managing client user accounts in applications and portals
- Handling contract management and communication for underlying technology vendors
- Delivering 24/7 IT support for dispersed workforces on varying schedules
- Assisting with compliance and risk management
- Providing **expense management** services
- Ensuring incentive alignment so that problems are permanently resolved (as opposed to a break-fix model)
- Many more – the MSP landscape is complex and growing



PART 7

Why Choose TPx to Manage Remote Work Deployments?

Facing the challenges that remote work presents can be daunting, but your organization doesn't need to tackle it alone. **TPx** provides the solutions and skills you need to create a productive and secure **remote work** environment for your employees.

Why Choose TPx?

We solve the biggest remote IT issues – cybersecurity, connectivity and collaboration – under one umbrella.

Our buying power enables us to customize your solutions for maximum effectiveness, within your budget.

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.

We combine everything you need – communications, collaboration, security and more – to be your single-source provider.

We provide enterprise-class and white-glove support for ongoing, proactive support tailored to your business.

Our experts become your team members. Instantly gain access to a multitude of remote work expertise without adding personnel.

We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.

With 23,000 clients in 50,000+ locations, we're big enough to get the job done and small enough to be agile.

We mix and match solutions and deliver a variety of service levels customized to meet your needs, including managed and co-managed options.

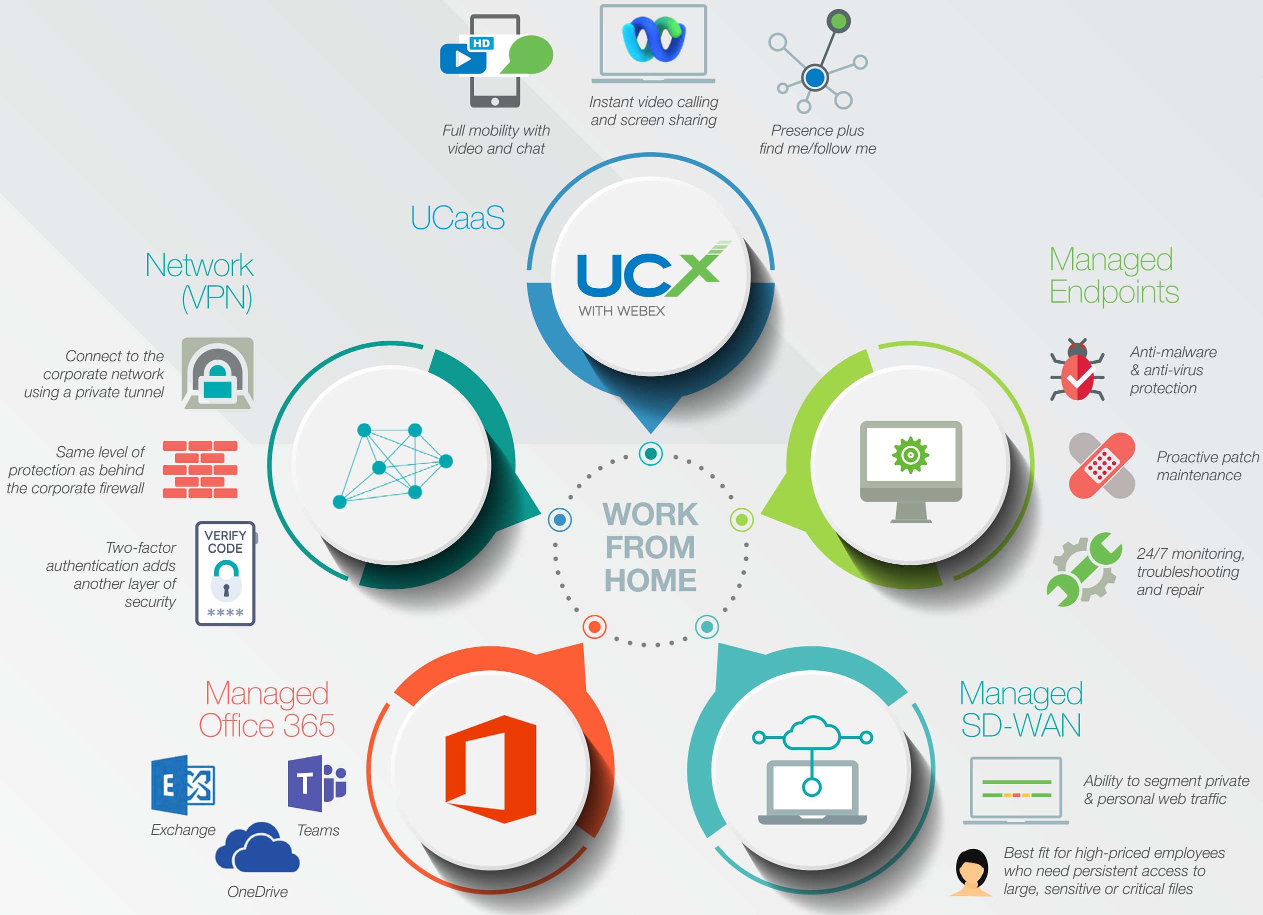
We offer a complete WFH solution, including managed endpoints, UCaaS, firewall/ VPN and Microsoft 365.

We provide remote administrative support for operating system configuration changes, such as adding users and changing passwords.

On top of the WFH solutions, you can add on other TPx services, such as managed connectivity, to create a custom solution for your business.

TPx Work from Home Solutions Suite

TPx provides a complete solution for your WFH employees with Unified Communications as a Service (UCaaS), Virtual Private Network (VPN), Managed Microsoft 365, Managed SD-WAN and Managed Endpoints. We make everything work together perfectly, so you don't have to.



WORK FROM HOME
UCaaS
UCX WITH WEBEX
Full mobility with video and chat
Instant video calling and screen sharing
Presence plus find me/follow me
Network (VPN)
Connect to the corporate network using a private tunnel
Same level of protection as behind the corporate firewall
Two-factor authentication adds another layer of security
VERIFY CODE
****
Managed Endpoints
Anti-malware & anti-virus protection
Proactive patch maintenance
24/7 monitoring, troubleshooting and repair
Managed Office 365
Exchange
Teams
OneDrive
Managed SD-WAN
Ability to segment private & personal web traffic
Best fit for high-priced employees who need persistent access to large, sensitive or critical files

All-in-One Managed Services Portfolio Built for Work at Home and Beyond

Managed IT

TPx delivers fully managed and co-hosted IT services that enhance performance, optimize networks and improve system stability. Our best-of-breed technologies combined with our service expertise keep critical IT systems operating smoothly. Join the thousands of companies that trust TPx to manage their IT infrastructure and get the peace of mind you deserve.

Managed Security

With cybersecurity threats growing in frequency and complexity, you need the right security in place to prevent, detect and stop cyber threats. TPx offers a multilayered approach to security with best-in-class software that is backed by our highly trained security experts. Protect your business and keep your data secure with TPx.

Cloud Communications

Bringing people virtually together is easy with an intuitive unified communications solution like UCx with Webex. It's a single app for calls, messaging, meetings, video, screen-sharing and more. Whether you're a small business, enterprise, or call center, you can experience quality voice and unmatched collaboration capabilities with UCx.

Ready for Efficient, Secure and Reliable Remote Work Solutions?

CONTACT US TODAY