WHITE PAPER

Remote Work in this Economy

Overcoming the IT Challenges of Legacy Technology With Remote Access and Remote Management

Contents

Introduction:
The State of Remote Work

For some, the concept of remote work may seem like just a perk. In reality, the idea of working from somewhere other than the office has been growing in popularity for almost 50 years.

1970s

In 1973, while working remotely on a project for NASA, physicist Jack Nilles coined the term "telecommuting." His success as a telecommuter led him to propose that work should be moved to workers instead of forcing workers to travel to work.

1990s

The U.S. federal government began offering a limited number of telecommuting positions in the 1990s, and the Telework Enhancement Act was passed by Congress and signed into law in 2010, to make telecommuting universally secure and effective for federal workers.

2000s

In the early 2000s, due to the proliferation of malicious cyberattacks, businesses or anyone that wanted more secure internet connections turned to virtual private networks (VPN).

2010s

In the 2010s, the practice of remote work grew as technology improved and commutes got longer. According to "The Remote Work Report," published by GitLab and based on surveys taken between January 30, 2020 and February 10, 2020 — before the pandemic-induced remote work boom began — of 3,000 adult professionals who worked remotely or had the option of working remotely, "42 percent of people who are 100 percent remote said they have been working remotely for more than 5 years. 28 percent said they have been working remotely for 3 to 5 years. 19 percent said they have been working remotely for 1 to 2 years. And 11 percent said they had been working remotely for less than a year."[1]

COVID-19

The COVID-19 pandemic prompted the most rapid expansion of remote work in history. As communities and nations sheltered in place, remote work became standard operating procedure. Even companies with strict "no work from home" policies embraced remote work — at least on a temporary basis.

Several factors influence the prevailing belief that more employees will work remotely after the pandemic is fully under control than did before it began, including:

- Many people would prefer to work for a company that allows them to work from home, full-time or part-time
- Businesses see opportunities to cut their rent by reducing office floorspace
- An abundance of clear blue skies and clean waterways during quarantine periods have shown organizations that encouraging employees to work from home is one of the easiest and most effective ways to reduce their carbon footprint

43% **of full-time workers would work remotely more often[2]**

74% **of CFOs intend to shift some employees to remote work permanently[3]**

25%-30% **of the workforce are expected to work from home multiple days a week by the end of 2021[4]**

Organizations are beyond believing in the future of remote work, they are acting on it. *The Washington Post* reported in September 2020, that "head of remote work" is a hot new job title. According to the article, Facebook posted an opening for "director, remote work," and other organizations are following suit.[5]

Reactions to the recent surge in remote work show us that working from somewhere other than a centralized office is here to stay.

The new challenge in the current remote work phenomenon is that the future of many small-to-medium-size businesses (SMB) will depend greatly on how well their IT managers and managed service providers MSPs deploy and support technology that enables anywhere from five to 1,000 remote workers to remain productive, with no inherent risks of technical problems, connectivity bottlenecks, or security breaches.

Setting Up a Remote Workforce

Remote Work Model Options

For businesses, implementing remote work is not a one-size-fits-all scenario. Here are three popular models in practice today.

01

100 Percent Remote

The company has no office. Instead, employees are digital nomads, working from anywhere in the world, who meet and collaborate online.

02

Hybrid-Remote

This can be any combination of some employees working in the office full-time, some working from home full-time, and some splitting their time between home and work.

03

Split or Rotating Shifts

Half the employees come to the office on certain days, while the other half come on the other days. Workers commute less frequently, and office resources are less stretched.

For companies that want to maintain team cohesiveness and social ties, the split model still allows employees to see and work with each other in person. This enables them to keep office culture intact while supporting workers who prefer or need to work remotely. In some cases, having rotating shifts has also led to desk and resource sharing, which reduces office space requirements and leasing costs.

There's no data to support the notion that any one of these models is right or wrong. Companies can consult with experts and examine what other businesses are doing. But ultimately, each organization must decide for itself and adjust as necessary to see what works best for them.

Key Requirements

Regardless of the model, here are the key requirements for IT to support remote work environments.

Secure Connectivity
Remote work can be done from anywhere, while protecting corporate data

Remote Support
Fix software issues and install updates and upgrades without having to send technicians to remote locations or requiring employees to bring in or ship hardware to the office

Remote Monitoring
Enable proactive device support and maintenance, alerting IT of potential issues before they become serious problems

Remote Asset Management
IT can see and manage every company-managed device in one dashboard

Malware Protection
Safeguard every device from malware, such as viruses, phishing attacks, ransomware, spyware, rootkits, and more

Patching
Fix software vulnerabilities proactively and update applications before they become entry points for cyberattacks

Data Backup
Company files on remote devices are automatically backed up to the cloud, available for remote restoration

Videoconferencing and Collaboration Tools
Employees can work together and meet anywhere, regardless of their location

With all these tools, remote workers don't have to bring their devices to IT technicians in order to get support or services, and IT technicians don't have to travel to the devices to protect and manage them. But without secure connectivity, all of these tools and the devices on which they are used are at risk.

Two Questions to Ask While Evaluating Your Options

When evaluating options for your remote work infrastructure, there are two essential questions your organization must answer first.

1

Will you provide computers and cell phones for your employees to use to conduct business, or will you expect them (or ask them) to use their personal devices for work?

Every device that touches your network needs to be protected. This gets tricky if devices are owned by employees, because you don't want confidential business documents to be saved locally to personal devices.

2

How important is scalability to your remote work environment?

Scalability is a concern for any business that wants to grow. As an SMB grows, scaling involves making technology and support available to more people. A technology that scales easily allows you to add more users without incurring additional infrastructure expenses or having to make expensive software upgrades. While some costs are unavoidable, you shouldn't have to rebuild your IT infrastructure as your company expands.

Technologies can scale poorly in several ways. Some technologies, like VPN, were never meant to scale. Companies buy VPN because they've probably heard of it and the upfront costs seem reasonable.

But VPN was never meant to accommodate your entire workforce remoting in to your server for a full day. So, even if your workforce isn't growing, the bandwidth of your VPN must expand in order to perform at higher capacity. That will likely mean new hardware and upgraded software, which will mean more costs.

And when your business grows, the additional costs of new hardware and software upgrades will be required again.

Secure Connectivity: The Difference Between Remote Access and VPN

IT has to provide connectivity that allows remote workers to be as productive as they are in the office, enables technicians to provide remote support, and keeps remote sessions secure from hackers, malware, and other threats.

While VPN is the status quo solution for enabling employees to access corporate systems, the rapid increase in the numbers of remote workers caused by the coronavirus pandemic revealed several drawbacks of VPN as a tunneling protocol. With VPN, a virtual tunnel connects the remote user to a server. When users download files from the server to their own computer and make changes to documents locally before saving them back to the server, these problems can occur:

Bottlenecks
Like a tunnel you drive through with your car, the VPN fills up with traffic as more users attempt to access your corporate network. This is not usually a problem when only a few employees are working remotely. But when hundreds of workers in a company try to access the server at the same time, bottlenecks slow traffic to a crawl and may even keep some people from logging in to the server. When that happens, remote workers get frustrated and aren't productive.

Security
When remote workers download documents from the server to their personal devices, nothing stops them from saving files on those devices. Depending on the employee and their level of network access, you could be in danger of having valuable documents stolen by less-than-ethical employees. Also, VPNs sometimes shut down for no apparent reason, leaving the connection between the server and the device unsecured. For that reason, some VPN users install kill switches to immediately shut down the connection between the local computer and the server if VPN shuts down.

Processing Power
Employees who work on powerful desktops in the office will only be able to accomplish as much as the software on the machine they are using remotely and that machine's processing power allow them to. For example, some teams use CAD programs on their office desktop. Their computer at home doesn't have an advanced graphics card to support CAD software, which means they can't work on projects from home.

Remote access functions in a completely different way. First, there is no tunnel. Remote workers remote in directly to their office desktop. Once they have remoted in, they see a mirror image of what's happening on their in-office computer and operate it as if they were there in person. Unlike VPN, remote access performs differently in the three problem areas discussed above:

Bottlenecks
There aren't any. The only transfer between the machines is the mirror image, requiring negligible bandwidth.

Security
Every session and all file transfers are protected by end-to-end encryption. Remote employees can access desktop applications and work securely with huge files on the host computer that would otherwise take hours to download or transfer.

Processing Power
The local device doesn't have to be powerful, because it's simply operating as a mirror of the remote or in-office device, with the local mouse, monitor, and keyboard serving as ways to screen share and control the remote device.

Additionally, VPN is costly — especially if you need to scale it for more users. For VPN, the time from installation to deployment is weeks, whereas remote access can be set up and used within minutes. While VPN requires extensive setup and configuration, it also must be compatible with your router. In contrast, cloud-based remote access solutions do not require extensive setup, configuration, or maintenance. Everything is done in the cloud by the provider.

Simply put, VPN is legacy technology whose best days are in the past, as underscored by Paul Martini in Security Boulevard: "The future of the VPN, with certainty, has limited days. The coronavirus pandemic may have solidified and accelerated those days, leading ultimately to the death of the VPN."[5] Unlike VPN, remote access is future-proof and scales easily, keeping up with fast-paced business growth.

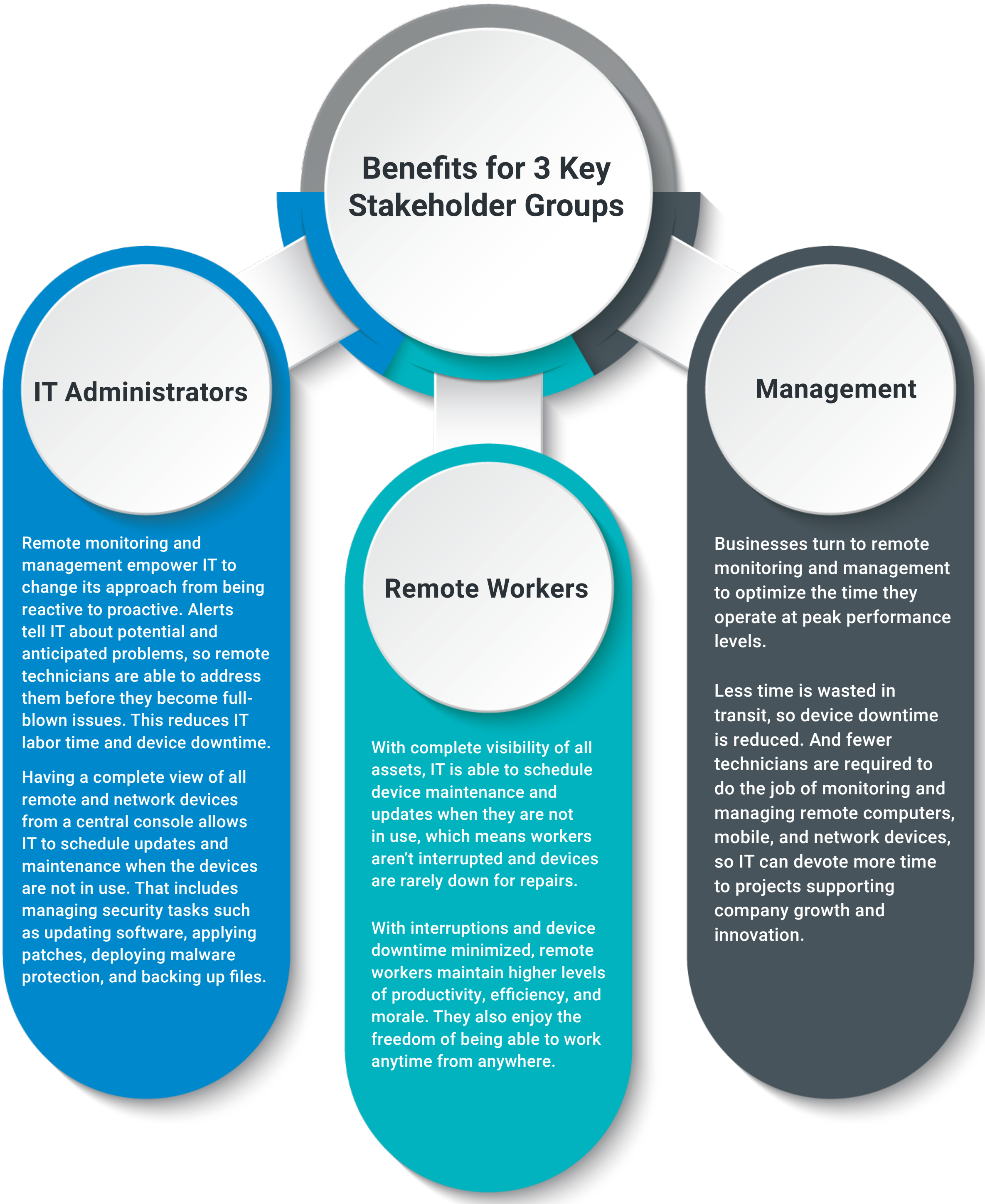
Remote Access with TeamViewer vs. VPN

Features	**TeamViewer** Remote access with TeamViewer allows you to connect to a target device, such as a computer or tablet. The only data transferred is an image of what's displayed on the target device's screen. Users can take control of the target mouse and keyboard or touchscreen to operate the devices, using all the applications and files as though they were there in person.	**Virtual Private Network (VPN)** A VPN, or virtual private network, allows you to send and receive data through a tunnel between two devices. All data is transferred through the VPN server to that user's local device, which places it at risk of loss and/or theft. This enables you to connect to a corporate network and access resources behind a firewall. All processing power depends on the user's local device.
Enables IT to provide remote support and users to receive remote support on their devices	✓	✗
Access workstations	✓	✗
Remote file transfers	✓	✓
Remote device control	✓	✗
Access unattended devices	✓	✗
Remote in to corporate network	✓	✓
Configuration and maintenance costs	Ø	$$$
Instant scalability	✓	✗

Understanding Remote Monitoring and Management

Giving employees the ability to work efficiently from anywhere at any time increases their potential output, productivity, and overall value to the organization. The challenge for IT is that the effort to support, manage, and maintain visibility of all the connected remote and network devices can be overwhelming, even if it is only a handful of devices.

The only efficient way for IT to support, monitor, update, and patch all the devices — both company-issued and BYOD — is to do it remotely and as much as possible, automatically. Otherwise, technicians waste time running from one physical device to another, reacting to problems that may keep people from working.



Benefits for 3 Key Stakeholder Groups

IT Administrators

Remote monitoring and management empower IT to change its approach from being reactive to proactive. Alerts tell IT about potential and anticipated problems, so remote technicians are able to address them before they become full-blown issues. This reduces IT labor time and device downtime.

Having a complete view of all remote and network devices from a central console allows IT to schedule updates and maintenance when the devices are not in use. That includes managing security tasks such as updating software, applying patches, deploying malware protection, and backing up files.

Remote Workers

With complete visibility of all assets, IT is able to schedule device maintenance and updates when they are not in use, which means workers aren't interrupted and devices are rarely down for repairs.

With interruptions and device downtime minimized, remote workers maintain higher levels of productivity, efficiency, and morale. They also enjoy the freedom of being able to work anytime from anywhere.

Management

Businesses turn to remote monitoring and management to optimize the time they operate at peak performance levels.

Less time is wasted in transit, so device downtime is reduced. And fewer technicians are required to do the job of monitoring and managing remote computers, mobile, and network devices, so IT can devote more time to projects supporting company growth and innovation.

Importance of Security

Without implementing strong security measures, remote devices are at risk, whether company-issued or employee-owned.

According to a survey of 411 IT and security professionals conducted by Check Point, **71 percent of security professionals noticed an increase in security threats or attacks since the beginning of the coronavirus outbreak**. There were big jumps in malware (28 percent) and ransomware attacks (19 percent).[6] The types of coronavirus-related threats included:

55%

Phishing emails pitching coronavirus news and cures

32%

Malicious websites offering advice or remedies for COVID-19

Malware, phishing, and malicious websites can all lead to security breaches that can result in data theft. What if an employee in your company who was working on VPN downloaded a customer database from your server to their computer, and then their computer was hacked and the database stolen due to insufficient security?

Suddenly, you're faced with a situation where your company has violated the privacy of every customer on that list by not keeping the list secure. The measures you take after the data breach, including notifying the customers, compensating for any losses suffered, and taking remedial action to make sure it doesn't happen again may determine the future status of your company's brand, reputation, and finances.

That's just one example of why it's important to keep all remote devices protected from all types of cyberattacks. It's also why a remote monitoring and management solution isn't complete unless it includes the ability to remotely manage security and IT maintenance tasks such as deploying malware protection, patching vulnerabilities, updating software, and backing up files.

When choosing solutions for remote access, remote support, remote monitoring, and remote management, security needs to be the top priority. Without security, it doesn't matter how fast your connection is.

TeamViewer Remote Access and Support Plus Remote Monitoring and Management

Supporting remote devices and network devices is essential to any remote work model.

The TeamViewer Remote Access and Support plus TeamViewer Remote Monitoring and Management solutions provide everything needed to support remote workers, all in one centralized management console — all by one vendor.

With TeamViewer Remote Monitoring and Management, start with as few as five endpoints and scale to as many as you need without outgrowing the solution.

Key Features

Remote Access
Securely remote in to a Windows or macOS device and take control of it as if you were there, without requiring VPN.

Remote Support
Remote in to desktops, laptops, and mobile devices* to analyze and fix problems, change settings, and make updates.

**Requires TeamViewer Mobile Device Support AddOn*

Remote Device Monitoring
Stay proactive instead of reactive by identifying device problems before they happen, allowing you to address potential issues before they escalate.

Network Device Monitoring
Get visibility into the availability, status, and issues of network devices such as routers, printers, and more.

Asset Management
View and manage all IT assets from a single dashboard.

Patch Management
Automatically detect and patch vulnerabilities in outdated third-party software and operating systems.

Endpoint Protection
Ensure all devices are safeguarded against malware, viruses, trojans, spyware, rootkits, ransomware, and more with **VB100 certified antivirus protection.**

Backup
Prevent data loss by automatically backing up files from endpoint devices to the cloud, available anytime for remote disaster recovery.

Scalability
Add as many remote access users as necessary at any time, no hardware or software upgrades required. For RMM, start monitoring and managing as few as five devices, and add hundreds or thousands as your business grows.

Security

Industrial-grade security is built into TeamViewer.

- **End-to-end 256-bit AES encryption** so every session is protected
- **Two-factor authentication** to prevent unauthorized users, even if a device is lost or stolen
- **GDPR compliant**
- **Certifications include:**
  - SOC2
  - HIPAA/HITECH
  - ISO/IEC 27001
  - ISO 9001:2015
  - VB100 certified antivirus solution for endpoint protection
- **24/7 Data center monitoring** helps ensure 24/7 network availability
- **DigiCert Code Signing** to verify that code is authentic and has not been tampered with
- **Brute-force protection** to keep hackers out
- **Black screen** keeps your in-office device locked and the screen black, so no one can see what work you are doing or access the device

Conclusion

While the 2020 boom in remote work was forced by the global pandemic, business analysts and news reports say that a considerable part of the workforce will continue to work remotely. That means the challenges IT departments and MSPs face in deploying remote workspaces that are affordable, fast, secure, and scalable while enabling workers to work productively — on any device, anytime, anywhere — will remain.

At the same time, IT is challenged with supporting devices of all formats, manufacturers, and operating systems, including devices owned by employees. Applications that allow IT to remotely monitor and manage all networked devices improve IT efficiency and effectiveness.

The combination of TeamViewer Remote Access and Support plus TeamViewer Remote Monitoring and Management addresses all remote work requirements in one integrated platform, so you can consolidate your IT tools and work with one vendor. The result? This enables remote workers to work securely and productively from anywhere at any time on any device. Moreover, IT can remotely manage and repair devices anywhere in real time with full visibility into the operational status of your IT infrastructure in one management console. The best part? IT can automate routine tasks, including patching, monitoring, and backing up devices — without toggling between different applications, resulting in more efficient workflows and less downtime for your organization.

Next Steps

See how TeamViewer Remote Access and Support work with TeamViewer Remote Management with a free demo and trial.

Request Free Demo

Request Free Trial

Resources

Learn more about TeamViewer Remote Access and Support

Learn more about TeamViewer Remote Monitoring and Management (RMM)

TeamViewer

References

1) GitLab (2020): The Remote Work Report. Retrieved from https://page.gitlab.com/rs/194-VVC-221/images/the-remote-work-report-by-gitlab.pdf

2) getabstract (2020, April): National Survey, A Majority of US Employees Want Remote Work Arrangement to Stay. Retrieved from https://journal.getabstract.com/wp-content/uploads/2020/04/ga_remote_survey_2020_compressed.pdf

3) Gartner (2020, April): Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently. Retrieved from gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

4) GlobalWorkplaceAnalytics.com (2020): Work-At-Home After Covid-19—Our Forecast. Retrieved from https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

5) *Washington Post* (2020, September): "Hot new job title in a pandemic: 'Head of remote work." Retrieved from https://www.washingtonpost.com/business/2020/09/09/head-of-remote-work-jobs/

6) Security Boulevard (May 2020): The Coronavirus Pandemic and the Death of the VPN. Retrieved from https://securityboulevard.com/2020/03/the-coronavirus-pandemic-and-the-death-of-the-vpn/

7) Security Boulevard (May 2020): The Many Ways Your Employees Can Get Hacked While Working From Home and How to Respond. Retrieved from https://securityboulevard.com/2020/05/the-many-ways-your-employees-can-get-hacked-while-working-from-home-and-how-to-respond/

About TeamViewer

As a leading global remote connectivity platform, TeamViewer empowers users to connect anyone, anything, anywhere, anytime. The company offers secure remote access, support, control, and collaboration capabilities for online endpoints of any kind and supports businesses of all sizes to tap into their full digital potential. TeamViewer has been activated on approximately 2.2 billion devices, up to 45 million devices are online at the same time.

Founded in 2005 in Göppingen, Germany, TeamViewer is a publicly held company listed on the Frankfurt Stock Exchange, employing about 1,000 people in offices across Europe, the US, and Asia Pacific.

www.teamviewer.com