CIO

The New Remote Work World: New Tools to Securely Support All Employees are Essential

TeamViewer

Remote work is the new normal, and it's here to stay.

Some 24% of employees say they expect to work exclusively remotely in 2022 and beyond, according to a Gallup poll, while 53% anticipate they'll be working in a hybrid style (both in-office and remotely). For companies, this type of work flexibility is key. In fact, employees are demanding it.

In the midst of the Great Resignation, all professionals have more choices, and they're pursuing opportunities that give them a better work-life balance. Companies that want to succeed need to deliver and embrace this new reality, giving employees – including IT teams– the tools required to get their job done no matter where or when they're working. At the same time, security must be prioritized as the volume of cyber security breaches and level of sophistication continues to grow.

Out of necessity during the pandemic, many companies cobbled together piecemeal solutions to handle remote work. But the number of applications introduced as quick fixes has only served to increase IT departments' workload, putting a strain on teams that are already under pressure from the growing complexity of their work plus chronic staff shortages.

Today's businesses need a seamless, reliable system to ensure the security and functionality of remote work, but also one that provides IT teams with a more sophisticated form of remote assistance to handle the new dispersed workforce.

"Security has always been an underlying challenge," says Michael Polaczy, director of product marketing at TeamViewer, "but recently the hurdles to overcome have become more elevated. With the hybrid workforce comes a whole new set of security challenges."

Many employees have shifted when and how they do their work, demanding more frequent and flexible IT support.

A multitude of new challenges

In the past, when many businesses were primarily work-on-site only, IT leaders needed only to focus on securing their on-premise environment to protect their data and privacy. IT setups were also mostly standardized and easily accessible by IT staff to administer, maintain, and support. Now, remote and hybrid work have vastly expanded the number and types of locations that businesses need to manage and secure. Employees might work from the corporate office, home, a hotel room, a co-working space, or coffee shop – all of which are outside the known, safe premises of the company network. Each additional location adds to the complexity of a decentralized work environment, and can result in a loss of critical visibility. This new reality requires a different approach to asset management and endpoint protection.

What's more, those endpoints run the gamut – desktop and mobile platforms, including remote PCs, smartphones, servers, payment terminals, and IoT devices, anytime and anywhere. Complicating this further: Bring your own device (BYOD) policies greatly expand the number and type of different equipment IT must support and secure.

Companies can be left vulnerable, in the dark about what software employees are using on their personal devices and whether or not that software complies with internal IT policies. IT teams need secure, remote monitoring capabilities to know which employees are using which applications and systems, to take governance of their IT environment if needed, and proactively spot small issues before they balloon into large issues.

"Every additional application poses a new security risk, increasing the surface area for cyberattacks and cyber adversaries," says Polaczy.

On-site service calls used to be the norm. But today's hybrid work environment depends on IT's ability to easily provide secure, remote support to devices.

Many employees have shifted when and how they do their work, demanding more frequent and flexible IT support. An employee working at night or over a weekend may need a problem fixed by IT right away, meaning IT staff must be more "on call" than ever before.

Simply put, IT teams need a fast, simple way to evaluate and fix issues to ensure business continuity.

Add to this on-going maintenance, such as patch management, which must also be done remotely. IT must plan needed maintenance proactively – and automate wherever possible.

Automating recurring tasks can help with the current challenge of overextended IT staff. By scripting manual tasks, IT team members can perform maintenance on multiple devices at once while freeing up time to focus on other important tasks.

Working towards a solution

Solving these pressing challenges requires a sound strategy. Companies need a plan that allows for employee flexibility when it comes to remote and hybrid work, while also maximizing safety and security when it comes to privacy and data so they can protect the organization against ever-present cyber criminals.

Companies must develop a remote work strategy and use tools that help them to:

1. **Gain better visibility into the IT environment.** Organizations need to have full visibility in order to solve IT issues. IT team members should know at all times which employees are using which applications and systems and be able to take governance of their IT environment.
2. **Improve foresight with proactive planning.** IT leaders can gain foresight and plan ahead by setting up checks that send alerts when attention is required. A well-organized checks system can help IT teams fix smaller issues before they snowball into larger ones, causing a cascade of problems.
3. **Remotely connect to devices, with ease.** To ensure business continuity and to efficiently provide employees with consistent support, IT departments must easily connect remotely to any device employees are using. The best tools will also offer remote support beyond the computer screen through augmented reality (AR) to assist with hardware-related issues.
4. **Centralize software patch management.** IT teams can protect against software vulnerabilities by centralizing updates and ensuring devices are always up to date.
5. **Automate tasks wherever possible.** By automating recurring tasks and scripting previously manual tasks, IT team members can perform maintenance on multiple devices at once and free up time to focus on higher-priority tasks.
6. **Reevaluate your cyber defense strategy.** Ask yourself, is your strategy holding up with today's challenges? A remote workforce requires a cyber security mesh, and also a solution that protects against zero-day exploits.

Companies need a plan that allows for employee flexibility when it comes to remote and hybrid work.

The benefits of one integrated solution

Companies need stable, secure partners to help address all these challenges. TeamViewer provides secure and stable remote access, remote control, and remote support to almost every desktop and mobile platform, including remote PCs, smartphones, servers, payment terminals, and IoT devices, anytime and anywhere.

TeamViewer solutions remove the disconnect between what support is saying and what the user sees.

With TeamViewer's Remote Access and Support, employees can safely access and control remote devices as if they were sitting in front of them, and all without a VPN. The tool also allows for secure, flexible file sharing.

TeamViewer's Remote Management means IT can easily view employees' devices that are located anywhere in the world to deliver instant, remote support when a computer glitches, a device fails, or when a system crash happens. It also offers Patch Management to keep every device's operating system up to date as well as next-gen Endpoint Protection – which protects against cyber threats, including zero-day exploits, and is completely integrated into the TeamViewer environment.

Using TeamViewer's Assist AR – a visual assistance tool that uses augmented reality – makes it easy to identify and solve problems. Its features include:

- **Easy visibility.** During support, employees can use their phone to allow an IT team member to provide support and help solve the issue in real time.
- **Interactive tools.** Interactive tools remove the guesswork and eliminate the need to verbally describe the actions users need to take to address an issue. IT teams can utilize augmented reality to draw on support videos in real time using pointers, arrows, circles, and text, pointing out to employees exactly what needs to be addressed so there's no confusion. By pointing and drawing on-screen, issues can be fixed quickly and efficiently. Even if the phone is moved, dropped, or set down, the IT team member's direction will still be there when the device is picked up again.

TeamViewer solutions remove the disconnect between what support is seeing and what the user sees and also help increase employee productivity, as well as decrease costs and delays by reducing onsite and desk-site visits, resulting in less travel and less downtime. The tools help to provide business continuity, allowing businesses to be proactive with issues, plan their time, and react quickly.

TeamViewer can help small and large businesses face the challenges posed by the vastly expanded IT environments of a hybrid work world . Small businesses can use TeamViewer Remote Access and Assist AR products, while a large enterprise can use TeamViewer's Tensor or Frontline products.

In today's new world of remote and hybrid workplaces, companies can't get by without a sound, efficient solution to manage and secure the growing number of work locations and devices. Those organizations that prioritize investing in the right technology to help protect their data and privacy, while also giving employees their desired flexibility, are the ones that will succeed.

Speak to a TeamViewer consultant today and see how one solution can make all the difference.