

Preparing for the new normal

The rise of remote work and how to futureproof your company



Advised but unprepared

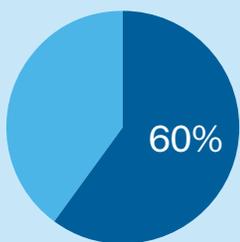
Boosted by the continued introduction of new tools and technologies, the adoption of remote work had been growing slowly but steadily in the United States for more than a decade.¹ But with the Covid-19 pandemic crisis forcing all but essential employees to work from their home environments, suddenly large swathes of the American workforce have been introduced to the concept of remote work. Research indicates that they like this new style of working and don't want to give it up.²

As recently as 2018, the World Health Organization (WHO) warned about the potential of a global pandemic, predicting where it might originate, how it might spread, and what form it might take.³ But, regrettably, the WHO had no idea when it might hit.⁴ Without a concrete and credible timeline, many businesses downplayed the risk and back-burnered business continuity and remote work planning in favor of other critical issues. The result: while some companies were prepared when the crisis hit, most weren't.

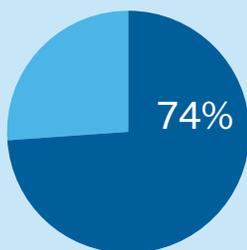
Trends and research indicate that what *Time Magazine* has coined "the world's largest work-from-home experiment,"⁵ is here to stay, and that employees feel good about the shift.⁶

With remote work likely to become a standard part of how business operates, companies are now challenged with managing its impact on culture, business processes, and IT systems. Those who embrace change and invest in technologies that provide flexible infrastructures, secure cloud-based access and endpoint management solutions will be best prepared to manage future changes and unanticipated crises.

In this guide, we outline three essential aspects of preparedness you can use to evaluate your own organization. Then, we review different types of technology solutions, examining how they work to provide the security, flexibility and scalability companies need to protect themselves from unforeseen events and succeed during periods of uncertainty and transition.



The New York Times reported that close to 60% of Americans intend to work remotely "as much as possible" after social distancing restrictions are loosened or lifted.⁷



Businesses also seem to be on board, with 74% of them saying that they will make work-at-home arrangements and environments permanent after the COVID-19 crisis subsides.⁸

Were you ready for what happened? Are you ready for what's next?

Were you prepared for the sudden shift to remote work? Did you have a business continuity plan in place? Were your employees able to access applications and data from home as easily as they did in the office? Or, did you find yourself scrambling to stitch together a patchwork of resources to support them?

Companies that handled the pandemic-related surge in remote workers without breaking a sweat share a set of common characteristics. They had already:

Recognized the importance of remote work and implemented solutions to support it

- Redesigned their infrastructures for flexibility and rapid scaling
- Deployed endpoint management solutions, so they could easily secure and manage personal devices
- Migrated data and applications to the cloud

When the crisis hit, their employees could work from home at the drop of a hat, and their workflows and processes felt like business as usual (albeit in pajamas).

Well-prepared organizations experienced little or no computing-related disruption. IT personnel didn't have to scramble to implement patchwork solutions or manage risks introduced by those technologies. Employees transitioned seamlessly to the remote environment, freeing managers and executives to focus on mitigating market threats, adapting operations, restructuring investments, and reevaluating business plans.

Although remote work was introduced to the masses via a sudden crisis, the cultural, technological and social forces that drove its evolution over the past decade, such as mobile technologies, WiFi networks and tech savvy young workers, will continue to influence our lives. Companies caught off guard by the rapid increase in remote work will have to catch up. But prepared and unprepared organizations alike will be forced to accommodate future change. Are you ready to evolve? Are you prepared for the next crisis?

Looking back at the common sticking points

Most companies experienced a common set of problems when their suddenly stay-at-home workforces began accessing applications and large quantities of data from personal computers and devices. Those problems can be broken out into three categories, which every

company should be prepared to handle when facing any type of catastrophe or threat:

1. Sustaining critical business processes
2. Ensuring security and compliance
3. Providing IT with visibility and control

To keep core business processes running after the flip to en masse remote work, companies needed to provide workers with immediate access to key data repositories and applications. Until this year, businesses had been able to ensure this access to their (relatively small) mobile workforces via VPNs, but this solution became untenable once pandemic conditions led to swift and exponential growth in the number of employees working from home.

IT teams found themselves required to massively scale access to core systems and applications for employees using personal computers and devices. They also had to deploy new regulation-compliant solutions that could replace in-person activities like sales meetings or executive briefings.

Expanding remote access and implementing point solutions without the opportunity for thorough testing introduces internal and external risk. To ensure that confidential information didn't fall into the wrong hands due to data leaks or breaches, IT teams were expected to secure infrastructures, personal devices and untested point solutions, whether or not they had the right tools to do so.

Providing solutions that enable employees to execute critical business processes, ensure security and compliance of the entire digital perimeter and provide IT with visibility and control.

Be ready for what comes next

The following key issues will help you evaluate your company's capacity to mobilize its workforce and support remote work. Use this section as a guide and reference tool to assess your preparedness for the next unforeseen business disruption.

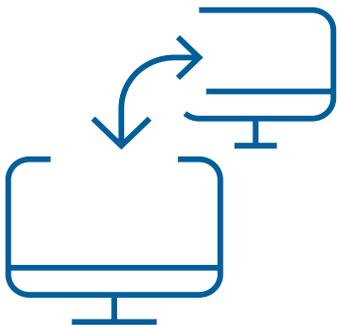
Critical business processes

In the event of a natural disaster or man-made crisis, employees must be able to continue executing on critical business processes regardless of where they are or what computing devices are available to them.

If a major disruption takes your local office network offline, can your employees continue working without skipping a beat?

Supporting remote workers involves much more than providing VPN or mobile access to important data. Remote work requires a comprehensive set of capabilities that can maintain critical business processes during disasters and other crises by delivering the same secure digital workspace experience to all employees on any device, regardless of the networks, cloud services or locations involved.

True remote work solutions wrap all data repositories, applications, workflows and services into a single workspace environment that is delivered to employees across devices, locations and networks. The user experience does not change when employees move from the office to a home or other remote environment, which enables employees to pick up where they left off using whatever devices and networks are available to them. The end result of being able to continue working as usual is a dramatic improvement in resiliency and flexibility that enables companies to stay competitive no matter the circumstances.



Security and compliance

Security and compliance requirements don't change when a power outage shuts down corporate servers or a snowstorm keeps everyone home for the day. Digital workspaces enhance security through a number of key capabilities. For example, fully-managed and globally available zero trust VPN alternatives provide access to data and applications at application layer while maintaining a secure and compliant company-wide digital perimeter.

Tools like single-sign on (SSO), multi-factor authentication, browser isolation, web filtering and data governance for SaaS applications ensure secure remote access and enforce compliance standards. Content collaboration and file sharing solutions protect data and documents at rest, in transit and during editing, so your employees can safely work on critical assets with colleagues and third parties. Together with other digital workspace security tools, intelligent and contextual access control solutions keep employees connected to all of their applications and data within a secure and compliant digital perimeter, even during massive disruptions.

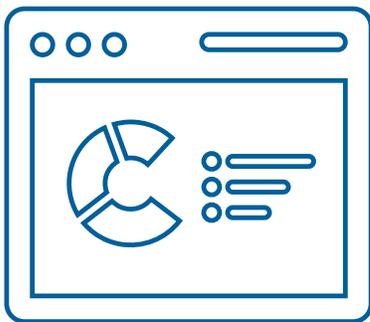


Visibility and control

Visibility and control are vital for maintaining security and business continuity under the best of circumstances, and they become even more crucial during times of crisis. Security monitoring solutions use machine learning to establish behavioral profiles

specific to individual users based on their typical interactions with files, applications and networks. They monitor for anomalous behaviors such as inordinately large data downloads, access requests from unknown devices or logins from unfamiliar locations. When a threat is identified, the system will shut it down before a malicious act occurs.

Intelligent workspace monitoring solutions also aggregate information, so IT teams can garner real-time, actionable insights about application performance, interrupted operations and user activity. With deep visibility, automated personalized activity monitoring and powerful controls that secure systems, data, applications and users, employees are free to work where and how they need, without posing a threat to IT security.



Conclusion

The onset of the COVID-19 pandemic crisis has led to an unprecedented, lightning fast rise in adoption of employees working remotely. Now that these employees have experienced the benefits and convenience of working from home, they don't want to give it up, and market trends and research indicate that remote work is here to stay.

Adapting to sudden changes or disruptions requires businesses to maintain secure, flexible and scalable infrastructure and services. Enabling employees across an organization to work remotely depends on IT's ability to provide a consistent workspace experience without sacrificing security or derailing critical business processes.

Digital workspaces integrate powerful multi-level security protections with contextual access to applications and data, unified endpoint management, intelligent activity monitoring and demand-based scalability to create a zero-trust digital perimeter.

Companies that recognize the importance of business continuity planning understand the critical role that remote work plays. By preparing for unforeseen events, an organization protects its core business and creates a competitive advantage that enables it not only to survive, but to thrive under adverse circumstances.

Use remote work to your advantage with Citrix Workspace

For more than a decade, Citrix has provided cutting-edge technology solutions that give organizations the flexibility and security they need to support today's remote workforce. Our solutions prepare businesses and their employees to adapt and thrive during a time of profound changes to work and the workplace.

[Learn more about](#) preparing for remote work with Citrix Workspace.

Sources:

¹ <https://www.flexjobs.com/blog/post/flexjobs-gwa-report-remote-growth/>

² <https://newsroom.ibm.com/2020-05-01-IBM-Study-COVID-19-Is-Significantly-Altering-U-S-Consumer-Behavior-and-Plans-Post-Crisis>

³ <https://www.nytimes.com/2020/02/27/opinion/coronavirus-pandemics.html>

⁴ <https://www.nationalgeographic.com/science/2020/04/experts-warned-pandemic-decades-ago-why-not-ready-for-coronavirus/>

⁵ <https://time.com/5776660/coronavirus-work-from-home/>

⁶ <https://www.washingtonpost.com>

⁷ <https://www.nytimes.com/2020/05/05/business/pandemic-work-from-home-coronavirus.html>

⁸ <https://www.google.com/url?q=https://www.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&sa=D&ust=1590->



Enterprise Sales

North America | 800-424-8749

Worldwide | +1 408-790-8000

Locations

Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States

©2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).