Parallels®

AFTER THE LOCKDOWN: HOW PARALLELS CAN HELP YOUR BUSINESS NAVIGATE A POST-COVID-19 WORLD

White Paper | Parallels After the Lockdown

Connection®
we solve IT®

Table of Contents

01 Introduction

When coronavirus disease 2019 (COVID-19) hit, few businesses were prepared for the massive disruption the pandemic would cause. With many offices around the globe completely shuttered to employees, non-essential work instantly became remote Many companies scrambled to put together reliable, secure and accessible remote work practices and processes to minimize productivity loss.

While some companies may have had some form of contingency plan in place in case of an unplanned disruption, such as a natural disaster or temporary server failure, it's safe to say that most were completely unprepared for the challenges COVID-19 presented.

With employees forced to turn their couches and dining room tables into at-home workspaces, businesses scrambled to figure out how to give them the proper access to certain applications so they could work remotely.

Businesses must prepare to be more agile and create a robust business continuity plan (BCP) that includes both employees and the technology they use. This plan must include technology that enables staff to work remotely at full capacity, from any device, at any time.

After the Lockdown

Now that many countries are emerging, in some form, from the strictest lockdown measures, most companies realize they need to create more thorough plans. These plans must address the current state of the world, as well as prepare for future scenarios that present challenges similar to COVID-19.

In business speak, this type of planning is known as business continuity planning, or BCP.

02 What is Business Continuity Planning?

Business continuity planning can be defined as the following:

"[BCP] is an essential part of any organization's response planning. It sets out how the business will operate following an incident and how it expects to return to 'business as usual' in the quickest possible time."

What Should Your Business Continunity Plan (BCP) Include?

- A risk management plan with a business impact analysis that identifies all activities that are key to the company's survival.
- An incident response plan that contains all information you'll need in order to respond immediately, whether you're planning for an incident or crisis or after one occurs.
- A recovery plan that outlines the steps needed to get your business up and running again after an incident or crisis.

While the COVID-19 pandemic is perhaps the most drastic scenario to invoke the need for BCP, there are many other situations that could require such a plan to be put into action.

This Include:

- **Natural disasters, such as floods and earthquakes.**
- **Technology failures, such as the loss of a server or entire data center.**
- **Accidents or disasters in or around the vicinity of a business's physical location(s).**
- **Failure of key suppliers or manufacturers.**
- **Union strikes or loss of key staff (e.g., mass layoffs).**
- **Economic shocks, such as the Great Recession of 2008.**
- **Public health emergencies (e.g., COVID-19, swine flu and Ebola).**

4 Key Benefits of Parallels RAS

Parallels Remote Application Server (RAS) is a device-agnostic, simple, intuitive and responsive technology solution that can help keep your workers connected and productive.

Benefits of RAS include:

- Enhanced data security
- Increased service delivery of IT operations
- Reduced total cost of ownership (TCO)
- Simple to deploy, manage and expand remotely

03 BCP Related to Remote Work Technology

Virtually all incident response and recovery plans developed through BCP will require some type of virtual or remote work. Many companies may already enable remote work on some level, but moving all regular business processes to a virtual setting requires the use of technology on a much larger scale.

This is because, when employees use virtual technology to perform their roles all day, every day, these systems are tested like never before, particularly from a functional and load perspective. And employees need to be able to use this technology with little training and downtime in order to be fully productive in a remote setting.

One type of virtual technology commonly used is virtual private networks, or VPNs. They can provide remote staff with secure access to business data centers.

VPNs are relatively easy to manage and simple for staff to deploy. However, their use is generally considered a legacy approach that isn't as secure as other technology solutions out there. There are also several other risks that may lead companies to think twice about using VPNs.

The Downsides of VPNs

Here are a few potential downsides of using VPNs:

- **Large bandwidth requirements.** VPNs require a lot of bandwidth because they send traffic back and forth over the internet. This can slow systems down when working with large files, and can require significant, costly increases to your company's internet capacity.
- **Potential loss of secure data.** VPNs allow users to download, save and edit company files and data on the endpoint device they're using. Regardless of whether the company or the employee owns this device, this means that data is stored outside of the company, and can be lost or stolen.
- **Exposure to malware.** VPNs can expose business systems to non-company devices, such as home PCs, which may be infected with malware. This can lead to devastating situations such as malware or CryptoLocker attacks.
- **Limited user access.** To protect against security breaches, IT administrators deploy VPN access in a way that provides employees with limited access to internal systems. This partial access blocks employees from many systems they would normally use daily. This reduces employees' ability to conduct normal business from home.

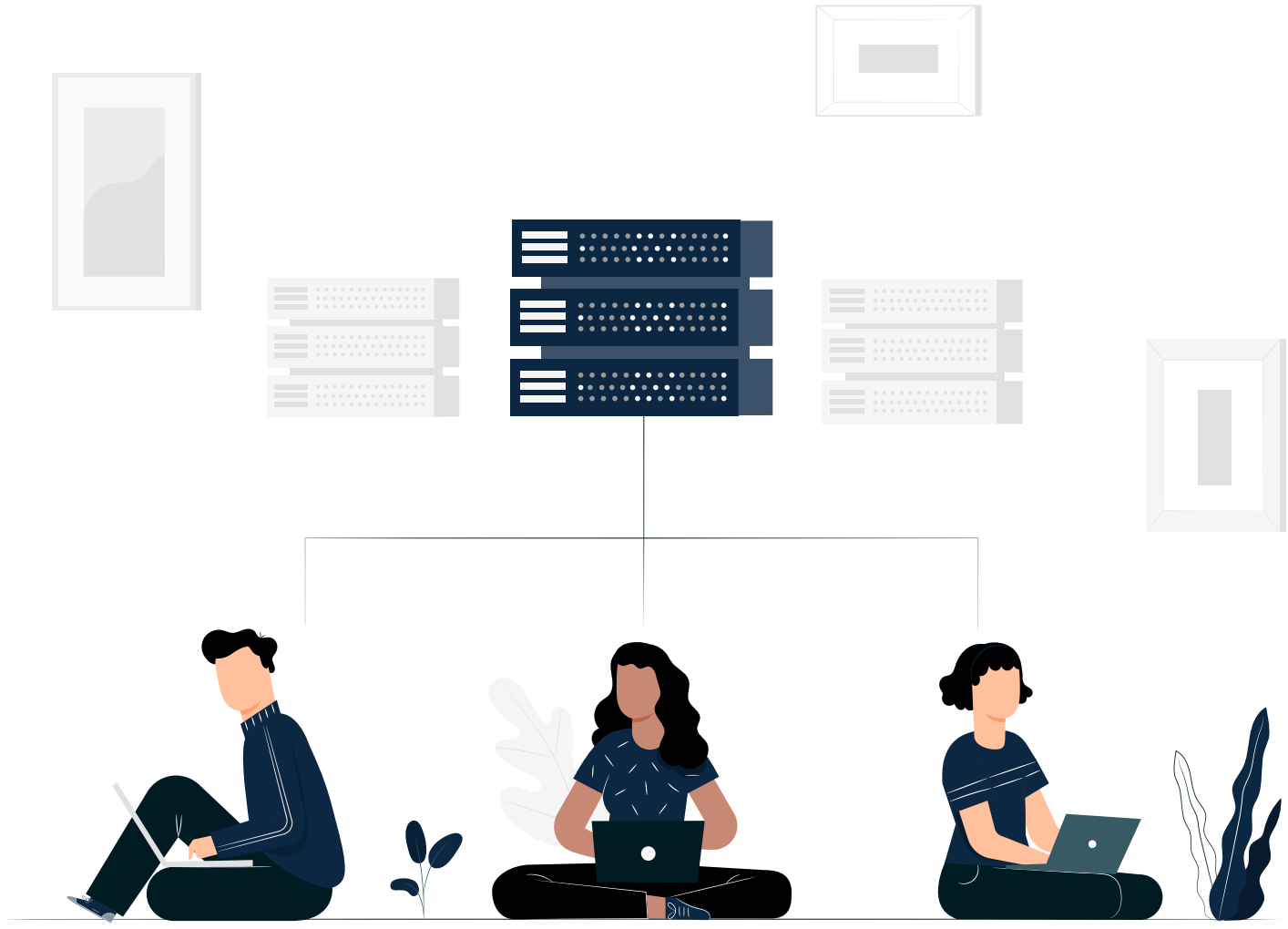
04 Benefits of a VDI Solution

Instead, a virtual desktop infrastructure (VDI), solution can be a smarter alternative. A VDI solution like Parallels ® Remote Application Server (RAS) provides a secure digital workplace with virtual applications and desktops. This enables a device-agnostic, simple, intuitive and responsive user experience needed for incident-response use.

While there are many benefits of using a VDI solution such as Parallels RAS, there are four that stand out:

- **Enhanced data security**
- **Increased service delivery of IT operations**
- **Reduced total cost of ownership (TCO)**
- **Simple to Deploy, Configure and Maintain**

Let's take a closer look at each.



Enhanced Data Security

When a major incident like the COVID-19 lockdown happens, there's often a rush to provide staff with remote access as quickly as possible to keep things running. In the process, normal security controls can be loosened or bypassed, leaving a company's network and data exposed.

For example, Microsoft found that **attacks peaked in March** of 2020, when COVID-19 was just starting to really impact the world and companies were scrambling to find workarounds. It's not uncommon for companies to allow stunning lapses in normal security procedures to quickly provide remote access, which can lead to serious consequences.

The key to reducing risk is to use a secure digital workplace as your main computing platform. This helps by creating a secure digital "fence" around your organization.

With Parallels RAS, data and applications are delivered in a secure digital workplace and use the same infrastructure as regular operations, with the same built-in security. Centralized management and automation enhance policy enforcement, regulatory compliance and antivirus protection of businesses applications and data.

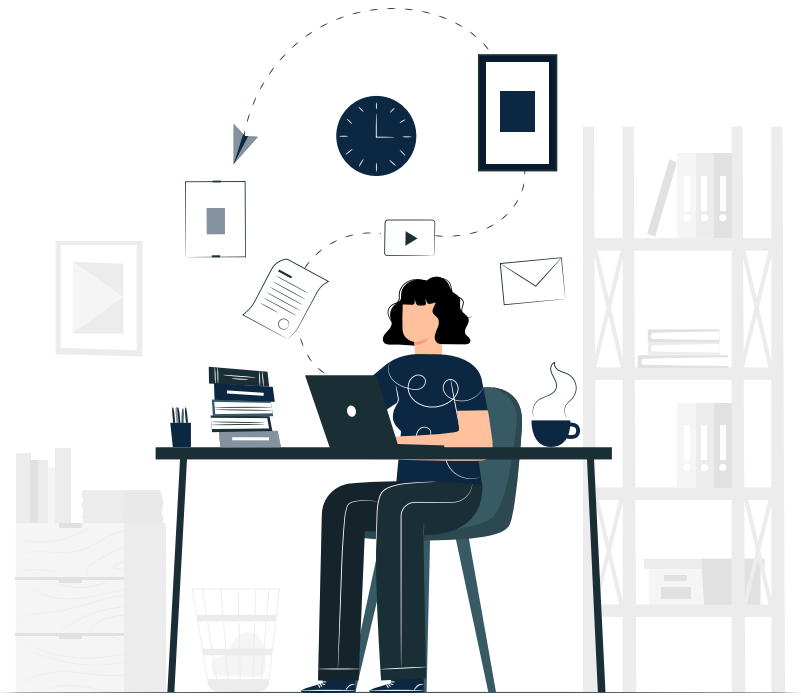
A secure digital workplace lets employees connect with apps and data using any device, network or cloud data center. When they connect to their applications or their desktops, they are essentially running the applications from inside the network. There is no need to download data to the device they're using, be it a home PC, work laptop, tablet or phone. When these staff disconnect from their secure digital workplace the data stays in the company's data center; not on the client device.

This centralized management and automation enhances policy enforcement, regulatory compliance and antivirus protection of business applications and data—all of which enhances overall data security.

Increased Service Delivery of IT Operations

A VDI solution such as Parallels RAS centralizes the delivery of applications and data to your business data centers, regardless of whether these centers are in a physical office or in the cloud.

A secure digital workplace removes the heavy reliance on endpoint devices. It also reduces the need for strict management of client devices and any installed applications. Staff can connect to the digital workplace using either a company device or their home computer, smartphone or tablet.



Once connected to the digital workplace, employees are provided with virtual access to all applications and data. There is no need to centrally manage the devices or applications installed on these clients.

Any updates can be implemented quickly because the applications reside within the company network and are managed fully by the company's IT team.

Increase Your ROI With Parallels RAS

Keeping costs low is top of mind for many companies today. With Parallels RAS, you can:

- Eliminate the need for separate business continuity processes.
- Eliminate additional technology acquisition and deployment projects.
- Allow employees to connect from perimeter networks and personal devices.
- Get staff up and running in no time, with minimal training required.

Reduced Total Cost of Ownership (TCO)

Even before COVID-19, many companies were already moving to a Bring Your Own Device (BYOD) approach, where staff choose to use their own personal devices (e.g., laptops, tablets and smartphones) to conduct work. If a personal device is not compatible, some businesses offer a BYOD stipend that employees can use to purchase an endpoint device of their choice that also meets their job requirements.

By using a VDI solution such as Parallels RAS that provides a remote workplace with virtual applications and desktops, businesses can allow employees to use a wide variety of personal devices safely, including thin client and Chrome devices. Leveraging employee's existing assets can reduce endpoint maintenance and acquisition costs greatly, thus reducing the overall TCO.

Simple to Deploy, Configure and Maintain

A key requirement for a successful mass adoption of a secure workplace environment is the ability to configure client devices for connection automatically. With a solution like Parallels RAS, an employee needs only to select their relevant application or desktop icon, and the application will open securely “inside” the business network, where they are granted all access required to perform their role productively. This technology also allows users to select alternate devices, regardless of the client operating system, and connect to the secure digital workplace in the same manner.

Central management and control of a secure digital workplace also allows administrators to provide access and apply policies securely in a granular method. In other words, administrators can provide access to client resources for some users (e.g., printers, USB drives and webcams), but disable them for others, using a tiered approach.

Parallels RAS also allows these services to be expanded quickly and flexibly. Templates for additional computing capacity and the ability to deploy services to business-owned hardware or cloud hosts, such as Microsoft Azure, allows businesses to scale their digital workplace quickly and avoid rollout delays.

05 Use Parallels Remote Application Server (RAS) to Navigate a Post-Covid-19 World

Now that the COVID-19 lockdown is starting to lift in many places, many businesses are deciding whether temporary measures should evolve into permanent ones. Many fully functional remote workplaces will be accelerated as companies adopt long-term work-from-home policies. But these remote workplaces can only be effective if they are secure, easy to deploy and allow employees full access to every application they need to perform their roles successfully.

That's where a VDI solution like Parallels RAS comes into play. As an affordable, scalable all-in-one virtual desktop and application solution, Parallels RAS allows users to access virtual workspaces securely from anywhere, on any device, at any time. Parallels RAS centralizes IT infrastructure management, streamlines multi-cloud deployments, enhances data security and improves process automation.

All of this is offered through a simple concurrent user licensing model. A single license for Parallels RAS covers all components, from load balancing and session brokering modules, to secure client gateway modules for remote access.

While COVID-19 has thrown many factors of daily life into uncertainty, successful deployment of remote workplaces doesn't have to be one of them. With Parallels RAS, you can ensure your company is able to provide employees with secure access to their digital workplace all day, every day.

A solution that works seamlessly whether staff are at home or in the office, Parallels RAS can help your company navigate the transition from total lockdown to a post-COVID-19 world in 2021 and beyond—no matter what new challenges may come.