



AFTER THE LOCKDOWN – REINVENTING THE WAY YOUR BUSINESS WORKS.

White Paper | Parallels After The Lockdown

Some businesses already had technology platforms that were ready for the kind of disruption that Covid-19 has caused. The CIO's and Business Continuity Managers of these companies can take credit for pushing the importance, designing a user architecture, and getting the budget approvals needed to build a system that allows their business to run normally when most staff are remote, just as it does when staff are in the office.

Many businesses, managers and staff have been pushed by Covid-19 into the understanding that work is indeed not a "Place"; rather, work is something that you "do". This is a mindset shift that will change the way we work forever.

01 AFTER THE LOCKDOWN

Now that we are emerging from the most stringent lockdown measures, most people realize that their business continuity plans were not ready for "whole of business" use and were designed for short emergencies where only a percentage of the workforce would be catered for. With the benefit of hindsight many companies are noting that their Business Continuity technology was found to be:

- Slow Insecure
- Provided only partial access to what was really needed to get the job done.



Businesses are ready to start planning on how to gear their business for more agility, with a more robust business continuity plan for their employees and their technology. A plan that includes technology which enables their business to work at full capacity rather than just getting by.

02 BUSINESS CONTINUITY PLANNING

Whether it was carefully planned or created “on-the-fly”, a Business Continuity Plan is what most businesses of any size have invoked since the Covid- 19 lockdowns were announced. This type of plan is described as:

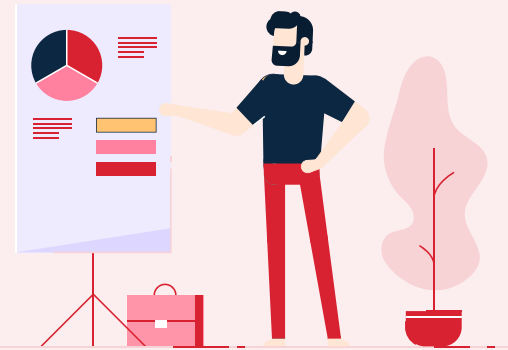
Business continuity is an essential part of any organization’s response planning. It sets out how the business will operate following an incident and how it expects to return to ‘business as usual’ in the quickest possible time.

Reference: <https://www.cpni.gov.uk/business-continuity-planning>

While the Covid-19 pandemic has certainly focused the mind of business and technology leaders on their Business Continuity Plans, there are many other possible scenarios that can cause partial or total loss of business where a BCP is also needed.

For example:

- 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



Businesses reviewing their procedures must conduct careful research and understanding when designing and amending their future Business Continuity Plans.

There is a need to consider:

- A risk management plan with a business impact analysis which identifies the activities of a business that are key to its survival.
- An incident response plan which contains all the information you will need to respond immediately before and after an incident or crisis.
- A recovery plan which outlines the steps you will need to take to get your business running again after an incident or crisis.

- Economic shocks such as the collapse of Lehman Brothers in 2008 Failure of key suppliers
- Industrial action or loss of key staff Health Emergencies (e.g. Covid-19, Swine Flu)
- After easing of the Covid-19 restrictions

03 BUT HOW DOES THIS RELATE TO OUR TECHNOLOGY?

Many business leaders are now looking for a way to invoke the incident response and recovery plans without the resulting business shock that has been evident during the Covid-19 lockdown. Companies are looking to make “Virtual” and “Remote” work a part of regular business processes but on a much larger scale than ever before. In this way the technology systems that will be used to power their BCP will be tested every day, by many staff, as they work remotely and virtually on a much more frequent basis. In turn this approach will increase confidence that BCP technology systems are capable from a functional and load perspective. And employees will be familiar with the systems, requiring no adjustment to their workflow in order to be 100% productive during a future incident response.

HOW DO WE GET OUR APPLICATIONS AND DATA TO OUR STAFF SO THEY CAN BE 100% PRODUCTIVE WHEN REMOTE?

With the Covid-19 lockdowns, a successful Business Continuity Plan includes five key technology attributes needed for employees to be 100% productive before, during and after a Covid-19 type event. The technology must be:

- A Device Agnostic, Simple, Intuitive and Responsive user experience
- It must Enhance Data Security Must increase the Agility of IT Service Delivery options
- Reduce the Total Cost of Ownership of staff technology delivery
- Must be simple to deploy, manage and expand remotely

Business technology leaders have a number of tools that can help with some of the attributes shown above.



For example, Virtual Private Networks (VPN's) can provide secure access from a remote staff members home back to the business datacentre.

VPN's can be relatively simple to manage and simple for staff to deploy themselves. However, it should be considered a legacy approach for reasons that include:

- VPN's can expose business systems to non-business computers such as home PC's which may be infected with malware, which could lead to potentially huge impacts such as malware /cryptolocker attack.
- VPN's allow users to download, save, and edit company files and data on the endpoint device. Regardless of whether the company or the end user owns the endpoint device this data at rest is now outside of the company and could easily be lost or stolen.
- VPN's require a lot of bandwidth with file traffic constantly moving forwards and backwards over an internet link. This can lead to slowness in working with large files at the client end and require huge increases in internet capacity at the datacenter end.
- To protect against security breaches, VPN access is generally deployed in a way that provides a staff member with limited access to internal systems. They still remain outside of the network with partial access, blocked from many of the same systems that staff use on a daily basis, reducing the ability of staff to conduct normal business from home.

A secure digital workplace with virtual applications and desktops provided by Parallels RAS enables the device-agnostic, simple, intuitive and responsive user experience needed for day to day and incident response use.

04 ENHANCE DATA SECURITY

During an incident response like Covid- 19 lockdown there is often a rush to keep the business running by providing remote access to staff as quickly as possible by loosening the normal security controls that govern access to a business's network and their data. In April 2020 Microsoft shared their threat intelligence data and found that hackers were launching attacks while companies were scrambling and emotions were running high. Some companies commit stunning lapses in their normal security postures in order to provide remote access, sometimes with detrimental consequences to their business.

The key to reducing the risk posed by loosened security controls and increased potential for data breaches, is to utilize a secure digital workplace as your main computing platform used day-in day-out. This helps by creating a secure digital fence around your organization, and by integrating this with the normal workflow of staff, they get to test and familiarize themselves with the Business Continuity tools every.

DAY OF THE WEEK

A secure digital workplace lets people connect with apps and data using any device, network or cloud datacentre. When they connect to their applications or their desktops in a secure digital workplace, they are essentially running the applications from inside the network. There is no need to download data to their client device, be that a home PC, work laptop, tablet or phone. When these staff disconnect from their secure digital workplace the data stays in the company's datacentre with no remnants on the client device. Data security is enhanced.

During an incident response event like Covid-19 lockdowns, data and applications that are delivered in a secure digital workplace use the same infrastructure as for regular operations, with the same inbuilt security.

Centralized management and automation enhances policy enforcement, regulatory compliance, and antivirus protection of the businesses applications and data.



The business IT department maintains control of the digital workplace with tracking, reporting and auditability to assist with security and compliance. Staff can securely access sensitive business data and applications from any device from any location enabling them to be 100% productive during the incident response.

A Secure Digital Workplace

with Virtual Applications and Desktops provided by Parallels RAS that is used day to day ensures that your data security is enhanced during incident response.

05 INCREASE THE SERVICE DELIVERY OF IT OPERATIONS

By centralizing the delivery of applications and data into your business datacentres, whether these be in your office or in the cloud, a secure digital workplace removes the heavy reliance on endpoint devices and reduces the need to heavily manage client devices and the installed applications. Staff can connect to the digital workplace using either a company device or a staff owned home computer.



Once they connect to the digital workplace all of their applications and data are provided within the virtual applications and desktops without the need to centrally manage devices and the installed applications on these clients. Any updates required to the applications and desktop are implemented quickly because they reside within the company network and are fully managed by the business technology team.

By putting staff mobility and remote access as key elements of a company's technology workplace when delivering applications and data to their employees, businesses:

- Increase the value of these investments by making the business BCP Ready
- Eliminate the need for many separate business continuity processes
- Eliminate additional technology acquisition and deployment projects
- The need to train and enable staff on how to be 100% productive in the case of a BCP event is greatly reduced because they use it every day.

06 **REDUCE THE TOTAL COST OF OWNERSHIP (TCO) OF STAFF TECHNOLOGY DELIVERY**

Harmonizing delivery of the day to day employee technology platform and the Business Continuity platform with a secure digital workplace, provided by virtual applications and desktops, enables businesses to eliminate the cost of BCP technology by leveraging existing assets and outlays.

Many companies are moving to a Choose Your Own Device approach, whereby staff and



They connect from perimeter networks set up for staff managed BYOD computers, but access applications and data in the same method as their colleagues with company owned devices.

departmental managers choose the specifications of endpoint devices that are distributed to staff that are under their budgetary control. By utilizing a digital workplace with virtual applications and desktops, businesses are able to select a variety of devices including Thin Client and Chrome devices. This means endpoint maintenance and acquisition costs can be greatly reduced, reducing the overall Total Cost of Ownership of the technology workplace.

Some businesses offer a Bring Your Own Device (BYOD) policy where employees are offered an additional stipend in their wage so they may go out and buy an endpoint device of their choice that they will own in a form factor that meets their job requirements. When BYOD users connect to virtual applications and desktops from their office location.

07 SIMPLE TO DEPLOY, MANAGE AND EXPAND REMOTELY

A key requirement for a Secure Digital Workplace platform for mass adoption during a Business Continuity event such as the Covid-19 response is the ability to automatically configure client devices for connection. The staff user then only needs to select their relevant application or desktop icon, whereby the application will open securely “inside”

As a secure digital workplace platform, Parallels RAS provides virtual applications and desktops with TCO far lower than many customers expect due to its 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.

Parallels RAS reduces the Total Cost of Ownership of your business technology platform due to it's simple licensing approach and also the elimination of BCP technology costs by using the platform as the primary daily business workplace.



the business network with all the access required for the staff member to be 100% productive during the BCP event. In addition, users should be able to select another device regardless of the client operating systems and connect to the secure digital workplace in the same manner.

Central management and control of a secure digital workplace should enable administrators to provide access and securely apply policies in a granular method, enabling access to client resources for some users (for example: printers, usb drives and webcams) but disabling these for other users.

Expansion of these services should be flexible and quick. Templates for additional compute capacity and the flexibility to deploy services to business owned hardware or cloud hosts such as Microsoft Azure will allow businesses to scale their digital workplace quickly and avoid rollout delays.

A Secure Digital Workplace with Virtual Applications and Desktops provided by Parallels RAS provides powerful tools for the management and expansion of the technology, allowing the capacity and control needed during a BCP event such as the Covid-19 lockdown.

08 HOW CAN PARALLELS REMOTE APPLICATION SERVER (RAS) HELP?

As a result of the Covid-19 lockdown experience, temporary measures will be scaled back and adoption of fully functional “Remote” workplaces will now be accelerated. A reduction in the obstacles for moving to virtual desktops and applications will be required so that businesses can be 100% productive during Business Continuity events. The winners will be those organizations who use and explore the possibilities of a virtual workplace every day. Anything that can be done virtually should be done so that it is ready to go at the outset of the next BCP event.

Our customers use Parallels Remote Application Server (RAS) for their daily digital workplace, whether they are in their office or at home. The experience is the same.

As an affordable but scalable all-in-one virtual desktop and application solution, Parallels RAS allows users to securely access virtual workspaces from anywhere, on any device, at any time. Parallels RAS centralizes management of the IT infrastructure, streamlines multi-cloud deployments, enhances data security and improves process automation.

Now that the Covid-19 lockdown is lifting, when you consider “what worked” and “what didn’t”, consider how good it would be if your staff tested your Business Continuity Plans every day without even asking them. With Parallels RAS, we can change the way you work.

[Contact Us](#) to get started.
