



How Virtual Desktop Infrastructure (VDI) Can Help Your Business Survive the Pandemic—And Prevail in the Future

White Paper | Parallels Remote Application Server

Table of Contents

- Executive Summary 3**
- Introduction 3**
- Remote Work Adoption Accelerates in 2020 3**
- Key Considerations When Choosing a Remote Work Solution 3**
 - Speed and ease of deployment
 - Security
 - User Experience (UX)
- Why Use VDI? 4**
 - Remote PC
 - RDSH
 - VDI
 - Windows Virtual Desktop
- Benefits of Using VDI 5**
 - Enables rapid deployment
 - Inherently secure
 - Simplifies IT administration
- Challenges of Using VDI 5**
- Why Parallels RAS is Different 5**
 - Fast and easy to deploy
 - Low TCO
 - Superior User Experience
 - Printing
 - Native gestures
 - Multitasking on any device
 - Single sign-on
 - Full desktop functionality in a mobile device
 - Ultra-fast logons
- Enables IT agility 7**
- Reinforced Security Plus Monitoring 8**
 - Multi-factor authentication
 - Kiosk mode
 - FIPS 140-2 encryption
 - SAML SSO
 - Advanced reporting and monitoring
 - Client group policies
 - Advanced filtering
- Conclusion 8**

Executive Summary

Growing demand for remote working solutions in light of the pandemic is bolstering the case for virtual desktop infrastructure (VDI) adoption. In this white paper, we discuss why VDI is best suited for today's business environments, especially since remote work is poised to play a big role both now and in the "new normal" of a post-COVID-19 world. We discuss VDI's main advantages, its shortcomings and what can be done to address them.

Introduction

Remote work adoption has been growing at a pace never seen before. Fueled by the reality of COVID-19, most businesses are now allowing employees whose tasks don't require an on-site presence to work from the safety of their homes. This situation has increased demand for Virtual Desktop Infrastructure (VDI) solutions like Parallels® Remote Application Server (RAS). Later in this white paper, you'll learn how Parallels RAS can put your business in the best position to pull through this period of uncertainty and emerge victorious in the future.

Remote Work Adoption Accelerates in 2020

Remote work was on the rise even before the pandemic, with Global Workplace Analytics estimating a [173% increase from 2005-2018](#). This trend, however, spiked significantly with the spread of COVID-19 as companies scrambled to prevent employees from being infected by the virus and enforced a work from home protocol. A survey conducted by Gartner in 2020 revealed that [88% of organizations worldwide](#) encouraged employees to work from home as part of their COVID-19 contingency plans.

But the rise in remote work was happening even pre-pandemic—it's just now been accelerated out of sheer necessity. This trend has been largely driven by increased adoption of work-anytime-anywhere-enabling technologies like cloud-based, Desktop-as-a-Service (DaaS) solutions, such as Microsoft Windows Virtual Desktop.

Key Considerations When Choosing a Remote Work Solution

Pandemic-induced work-from-home initiatives have proven to be very fruitful. Not only did they help prevent employees from contracting the virus, but they also allowed businesses to experience first-hand the long-touted benefits of remote work. Several companies reported substantial [gains in employee productivity](#), particularly in individual and managerial tasks—an advantage that early adopters of remote work have been enjoying for quite some time now.

Speed and ease of deployment: The speed at which businesses were forced to adopt remote work in 2020 has been nothing short of hasty. Because coronavirus cases were rising so fast, almost all businesses had to roll out remote work setups with little to no preparation and planning. Many of them likely "panic-bought" solutions that they now find too expensive, too complicated, and unable to meet best practices. Their predicament highlights the importance of factoring in ease of deployment when choosing a remote working solution. The more complex a solution is, the longer it takes business processes to normalize.

Security: Remote work normally entails removing digital assets (i.e., corporate data and applications) from the safe confines of the corporate network. This increases business risk. What happens if a remote worker's laptop or desktop is stolen and the information on it is compromised? This could lead to a data breach and might even result in costly fines and penalties if the data involved is covered by laws or regulations such as HIPAA, PCI-DSS, or GDPR—not to mention the damage it can do to a company's reputation if they're forced to disclose the breach to the public.

Uncertainty and confusion created by COVID-19 has caused many businesses to let their guard down as they rush to implement remote work plans. This state of vulnerability hasn't gone unnoticed among cyber criminals, who have [ramped up attacks](#) on major corporations and critical infrastructure. Thus, it's become imperative for any remote working solution to be fundamentally secure.

User Experience (UX): Another crucial factor to consider is the user experience (UX) of the remote work solution used.

As much as possible, end users should NOT have to:

- Go to great lengths just to create/edit, share, store, secure or print a document.
- Abandon applications they're already accustomed with, e.g., Microsoft Word, Excel and PowerPoint or their company's Line-of-Business (LOB) software.
- Adjust to a different UX every time they shift to another device.
- Endure delayed logons, application accessibility problems and sluggish user interfaces.
- These UX problems will almost certainly hamper user productivity and breed discontentment.

Why Use VDI?

Virtual desktop infrastructure is a way of delivering virtual desktops and applications remotely to endpoint devices. In a VDI environment, operating systems and applications such as Windows 10 and Microsoft Office are typically placed in a central location—e.g., an on-premises datacenter or a cloud infrastructure—and then delivered remotely to devices in the organization.

(Note: In this whitepaper, we use "VDI" as an all-encompassing term that includes VDI, Remote PC, RDSH and other similar technologies, which are defined below.)

Remote PC: A remote PC can be a regular physical desktop computer in the office that's accessed remotely from an endpoint device. This functionality can come in handy when remote workers need to access files and applications on their office computers, but they happen to be at home or in another offsite location.

RDSH: Remote Desktop Session Host or RDSH is a component of Microsoft Remote Desktop Services (RDS) that provides session-based resource sharing so users can access desktops and applications simultaneously from a single instance of Windows Server. Since multiple user sessions may share a single host (physical or virtual machine), fewer resources (e.g., CPU, memory and storage) are consumed per desktop than pure VDI.

VDI: In contrast to RDSH, pure VDI assigns each user to a single virtual machine (VM). This allows each desktop (and consequently, the user of that desktop) to consume all the CPU, RAM and storage resources allocated to that VM instead of sharing it with other desktops. VDI is best suited for use cases that require more security as well as resource-intensive workflows, such as vector graphics editing, 3D modeling, modern technical computing and video editing.

Windows Virtual Desktop: Windows Virtual Desktop is a desktop and application virtualization service delivered by Microsoft Azure. It enables businesses to utilize Desktop as a Service (DaaS) capabilities and use Windows 7 with free Extended Security Updates, among other capabilities.

VDI solutions can deliver applications and desktops to a wide range of devices, including laptops, PCs, tablets, thin clients and smartphones. End users can then interact with this remotely delivered software as if it were running locally on the devices themselves.

Benefits of Using VDI

The centralized nature of VDI is ideal for remote work environments, especially those involving large numbers of endpoint devices. Here are three key reasons why:

- 1. Enables rapid deployment:** VDI's centralized architecture makes it ideal for quickly deploying virtualized applications and desktops to many devices. IT administrators just need to set up the virtualized applications and desktops in one place and then have them accessed through end user devices over a local area network or the internet. This significantly reduces if not eliminates application compatibility issues during upgrades and cuts down application/desktop deployment time and maintenance from weeks or months to just a couple of hours or days.
- 2. Inherently secure:** This centralized architecture is also the reason VDI is inherently secure. Because applications, desktops and data are all stored in a central location rather than on the devices themselves, these digital assets won't be compromised if ever a device gets lost or stolen. It's also much easier to apply security patches and policies if they're done in one place.
- 3. Simplifies IT administration:** Another benefit of this centralized architecture is that it simplifies certain administrative tasks, such as performing software updates, applying security patches, troubleshooting OS and application-related issues, implementing policies, etc. Instead of having to carry out these processes on every device individually, IT staff can work on them in one place, freeing up crucial time and resources.

While these benefits have long been identified, they were once again reiterated in a recent [survey conducted by ESG](#). These characteristics make VDI suitable for remote work environments, as it seemingly ticks all the checkboxes... Well, almost.

Challenges of Using VDI

While applications, desktops and data are generally easy to deliver once a VDI solution is already operational, the solution itself can be extremely difficult to deploy, set up and even maintain. There are certainly exceptions, but in most cases, VDI solutions have too many separate components that need to be connected and configured. Because of their complexity, it's common for companies to hire third party specialists just to get their VDI solution up and running.

That's not the only problem. Oftentimes, these components are licensed separately. Once you add up all those licensing costs and combine them with your consultancy costs, you're likely to end up with an extremely high total cost of ownership (TCO).

As if that weren't enough, the complexity of most VDI environments also makes them susceptible to issues that are very hard to troubleshoot. Each time you encounter an issue that your in-house IT staff can't handle, you'll be forced to, again, hire the services of a third-party specialist. That's going to push your TCO even higher.

Finally, VDI solutions are notorious for being replete with issues when it comes to printing documents. Yes, what might seem like a routine task may turn out to be a major pain in the neck with VDI. Some of these issues are caused by poorly maintained driver repositories, uncompressed print jobs, driver conflicts, misconfigured printing solutions or network misconfigurations.

Why Parallels RAS is Different

If there's one thing that characterizes most VDI solutions, it's excessive complexity. For some solutions, it's like jumping through hoops just to get a VDI environment up and running. No organization wants that. There are, however, a few exceptions. One of them is Parallels RAS.

Parallels RAS provides organizations with a VDI solution that matches their expectations, growth and needs without requiring unnecessary costs or complexity. For example, a company might first decide to implement a quick, cost-effective remote working solution using the Parallels RAS Remote PC option, which provides employees with remote access to office PCs when working from home or on-the-go.

Then, once that company is ready to take the next step, they can roll out more advanced setups like RDSH (for session-based desktops), VDI (for fully dedicated virtual desktops), or Windows Virtual Desktop (for Desktop-as-a-Service). There are several other advantages of using Parallels RAS. They include:

Fast and easy to deploy: Unlike other VDI solutions, Parallels RAS is built on a much simpler architecture. As a result, it's substantially easier to deploy, configure and manage. This benefit is clear right from the start: Installation is straightforward and accompanied by quickstart wizards, so most companies can be up and running within mere hours—without any formal training needed.

Even configuring RDSH and VDI is quick and easy. In addition, administrators can take advantage of the vast collection of built-in automated image optimization capabilities Parallels RAS offers. It also provides auto-provisioning and auto-scaling features to achieve highly efficient and streamlined delivery of virtual apps and desktops.

Windows Virtual Desktop deployments, as with all other deployments, are carried out through the same centralized console and assisted by configuration wizards. The same console also gives admins the ability to manage and configure FSLogix Profile Containers, which can reduce logon/logoff times, lower traffic and processing load on file servers, and mitigate risk of profile corruption, among other things.

Low TCO: The simplified architecture of Parallels RAS brings major advantages compared to traditional VDI systems. First, it means Parallels RAS is less prone to issues. Second, when issues do occur, they're much easier to troubleshoot. As a result, businesses who use Parallels RAS are no longer forced to hire expensive third parties to install, configure or maintain their Parallels RAS environments. They can do most tasks by simply relying on their own in-house IT team.

Another major benefit of this simple architecture is that, unlike most VDI solutions, Parallels RAS doesn't consist of several disparate components with separate licenses. It's an all-in-one solution with a single license.

These factors amount to a substantially lower TCO than what other VDI solutions can offer. The savings generated, which can add up to tens of thousands of dollars, can be reallocated to other undertakings such as hiring top talent, developing innovative projects, putting more focus on the IT strategy or launching strategic marketing initiatives. There will be a lot of new opportunities for growth once the pandemic eases up. Those organizations who have the resources to take advantage of them will be the ones who end up on top.

Superior User Experience: Parallels RAS offers one of the best user experiences (UX) in the VDI space. Through the Parallels Client, users can access line-of-business (LOB) and other Windows applications or desktops from practically any device, anytime, anywhere. Target endpoint devices include the following:

- Windows PCs and laptops
- Mac desktops and laptops
- IOS/ iPadOS (iPhones and iPads)
- Linux workstations
- Android tablets and smartphones
- Chrome OS
- Any device that runs an HTML5 browser

Other notable UX advantages include:

- **Printing:** In contrast to other VDI solutions, remote desktop printing with Parallels is utterly seamless. Parallels RAS Universal Printing technology enables users to print directly to local printers from any device, without extra configurations.
- **Native gestures:** Users can stay highly productive even when on the go. Working with Windows applications on mobile devices is made easy through familiar touch gestures like swipe, drag, tap-to-click and zoom in, along with Parallels-specific features such as the lock 'n go magnifying glass.
- **Multitasking on any device:** Users can simultaneously open multiple applications as well as multiple files. Switching and copy-pasting between applications and files is made easy through touch gestures.
- **Single sign-on:** Through SAML SSO or Microsoft Active Directory integration, users only have to log on once, and all subsequent logons to other applications happen automatically, and are transparent to the end user.
- **Full desktop functionality in a mobile device:** In addition to delivering desktops and applications to mobile devices, Parallels RAS also makes it possible for users to interact with them as if they were running on full-sized desktops through Bluetooth mouse and trackpad integration, and even Samsung DeX integration.
- **Ultra-fast logons:** Like printing problems, slow logons are among the biggest issues in VDI. Not with Parallels RAS. By leveraging AI-based session pre-launch technology, Parallels can analyze user habits and provide instant access to virtual workspaces as soon as they're needed.

Enables IT agility

Despite its relative simplicity compared to those of other VDI solutions, the Parallels RAS architecture is very flexible and scalable. This gives IT teams the agility they need to quickly adapt to changing demands in the workplace that call for new applications or desktop requirements.

Practically every administrative task that involves any component of the Parallels RAS infrastructure can be carried out on one central management console. In the latest version of Parallels RAS, some administrative tasks can be completed on any mobile device by using the web-based management portal. Common, complex and repetitive tasks can be automated using the REST API and the PowerShell cmdlets (lightweight commands in a PowerShell environment).

Parallels RAS also supports multiple deployment options, including:

- On-premises
- Public cloud (e.g., Microsoft Azure, AWS, Google Cloud, Alibaba)
- Hybrid (e.g., on-premises + Microsoft Azure)
- Hyperconverged infrastructure (e.g., Nutanix, HPE Hyperconverged, Scale Computing HC3)
- Windows Virtual Desktop

Reinforced Security Plus Monitoring

When it comes to security, Parallels RAS inherits the centralized architecture of VDI. This means the risk of data loss at endpoint devices is significantly reduced. In addition, Parallels RAS is further reinforced by a range of security features that include:

- **Multi-factor authentication:** Augments usernames and passwords to minimize the risk of unauthorized access through brute force attacks and social engineering.
- **Kiosk mode:** Limits user privileges in Windows devices to prevent unauthorized system setting reconfigurations and application installations.
- **FIPS 140-2 encryption:** Protects data in transit from eavesdroppers and ensures compliance with PCI DSS, HIPAA, GDPR and other well-defined security standards.
- **SAML SSO:** Provides single sign-on capabilities without sharing the local identity database.
- **Advanced reporting and monitoring:** Provides IT admins with a 360-degree view of the Parallels RAS infrastructure, enabling them to quickly analyze and proactively act on potential issues.
- **Client group policies:** Centrally manage client settings for connection, printing, network, and others through client policies based on Active Directory groups or end user devices.
- **Advanced filtering:** Restricts user access to published resources in the farm based on user, IP address, MAC address, and gateway.

Conclusion

Many businesses are struggling to stay afloat in these trying times. Their main goal is to make it through the pandemic and emerge with enough wherewithal to rebuild and prosper again. Parallels RAS can be the key to ensuring business continuity through the pandemic and beyond—all while elevating productivity, sparing valuable resources (financial or otherwise), and delivering protection from potential cyber threats (delivering a much-needed break to your IT department).

[Learn more about how Parallels RAS can help your business.](#)