

VPN vs. VDI

What Should You Choose?

While the ability to remotely access an internal network has been around for decades, people have increasingly been working from home due to the COVID-19 crisis. Many organizations are using Virtual Private Networks (VPN) to provide employees with access to their digital workspaces. However, as VPN is posing a global data [security risk](#) to businesses, IT departments may want to re-think their strategy when it comes to providing remote access.

VPN isn't an optimal solution when providing remote access to employees as it simply doesn't have the degree of granular control needed to properly monitor and restrict users on a company's network. Cyberattacks are becoming more sophisticated and frequent and organizations using VPN may be exposed to compliance and regulatory risks.

Why a VPN solution is becoming outdated

With times changing continuously in the tech world, more and more workloads are moving to the cloud and a VPN solution is becoming outdated - services are no longer just located in your office or data center, but a hybrid combination of on-premises and public cloud services. Leveraging cloud-based solutions means that your company can centrally control access to applications while reinforcing security.

By switching to a Virtual Desktop Infrastructure (VDI) solution, you can enable employees to work from home on any device of their choice, while still keeping data safe. As long as users have an Internet connection, they can log in to their corporate virtual desktop and access all their work files and applications securely, with the latest encryption protocols.

In addition, large bandwidth connections aren't needed, as the data doesn't download to the endpoint - decreasing concern about encrypting the hard drive of the endpoint if the device is lost or stolen (something that is still needed for a secure VPN).

When using VPN, good end-user hardware is required since the processing is done on the client machine. However, with VDI, the processing is done in the datacenter - therefore employees using old machines can still easily access their virtual workspaces.

While VPN is a useful solution for organizations that distribute laptops to their mobile workforce so employees can access their work applications easily, it's a different story when employees have to use VPN on their home devices. For example, if an employee has a Mac but needs to access business-critical Windows applications, additional software needs to be purchased.



VDI advantages

- Provides centralized management of data.
- Seamless access to work files and applications with the latest encryption protocols.
- Optimized bandwidth usage.
- VDI processing is server based, powerful end-user hardware not required.
- Ability to use different devices, including tablets and smartphones.
- Access Windows applications on other operating systems such as Mac and Linux.

VPN limitations

- No granular control to monitor and restrict user access.
- Corporate data not centralized and harder to manage.
- Large bandwidth connection needed.
- Good end-user hardware required for client-side processing.
- Can't access Windows apps on other operating systems.



How can Parallels Remote Application Server (RAS) help?

While organizations may choose to implement VPN to provide remote access to business applications, along with lower costs and easier setup, Parallels RAS is a VDI solution that addresses all these issues, along with the other great benefits of VDI.

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

If your remote workers are set up on VPN and you're contemplating a VDI solution, why don't you give Parallels RAS a try by downloading our [free 30-day trial](#)? That way, you can check out all the security, and other benefits, for yourself!

Spend less time troubleshooting with VDI

With VDI, IT departments spend less time troubleshooting problems. As data is centralized, it's straightforward to support end-users. VDI's centralized format allows IT to easily patch, update or configure all the virtual desktops in a system, optimizing performance for the end-user. It's also possible to shadow a device to help figure out issues.

When having to install new OS updates and applications, a golden image is used in VDI. Changes installed on a single desktop are replicated to all virtual desktops in the pool, ensuring all users are always running the same exact version of the software. IT teams can first test customized applications on the server before rolling them out to everyone. Instead, with VPN, machines have to be set up individually and are therefore harder to manage.

While both VPN and virtual desktops can be secured, virtual desktops have the least amount of risk as they secure data all the way through the endpoint and provide IT admins with a faster and easier way to patch known vulnerabilities. With VDI, IT can set policies to restrict user access - establishing the right level of secure access for every user.

As VPN servers act as a gateway to a company's internal network, any breach would prevent remote employees from doing their jobs. While it's possible for malware to infect a virtual desktop operating system, at the end of each user session, the virtual desktop can be rolled back to a clean state, thereby eradicating the infection.

VDI has "built-in" security, since all applications and data are on servers in the office or the cloud. As VDI endpoints can't store corporate data, IT doesn't have to worry about them as a security threat. If employees access personal cloud storage or email services on their corporate devices, for instance, any breaches of those systems can't affect the corporate data on the user's virtual desktop because the data isn't local. Virus scanning is also centralized.

The security VDI offers extends IT control by restricting user actions, for example, when using the clipboard. Organizations can avoid any unwanted data leakage from published applications by disabling copy and paste on the clipboard, reducing the risk that sensitive data (such as credit card details) can be stolen.

For further information or to purchase Parallels products, contact us at +1 (425) 282 6400 877 (outside North America, +356 22 583 800), sales.ras@parallels.com or visit parallels.com/ras