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 delivering remote access.

Cyberattacks are becoming more sophisticated and frequent, and organizations using VPN may be exposed to compliance and regulatory risks. Thus, VPN isn't an optimal solution when providing remote access to employees. Although most VPNs enforce security health checks before allowing end-point connections to the corporate network, your IT department may find it challenging to configure and regularly update all client devices.

Why a VPN solution is becoming outdated

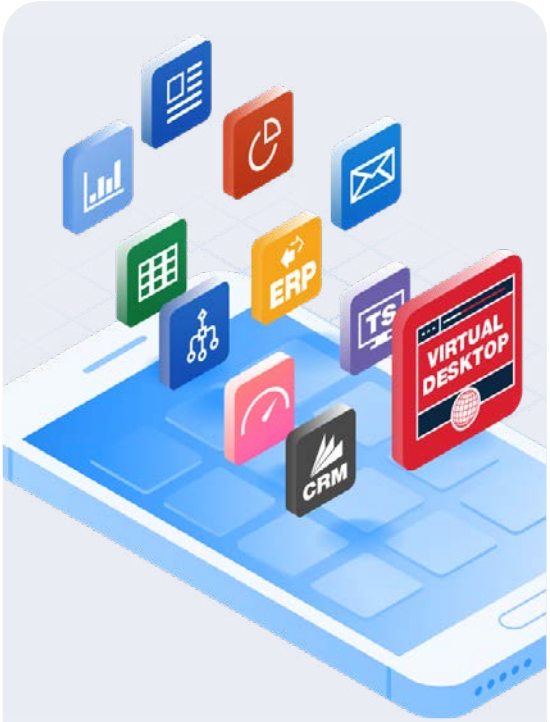
With times changing continuously in the tech world, more and more workloads are moving to the cloud and certain VPN solutions are a little outdated - services are no longer just located in your office or data center, but a hybrid combination of on-premises and public cloud services. Leveraging cloud-based 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 securely access all their work files and applications.

In addition, large bandwidth connections may not be required for certain use cases because information resides in the company datacenter - 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 may be required under some scenarios since the processing is done on the client machine. However, with VDI, most of the processing load is done in the datacenter – therefore employees using old machines, thin, or zero clients, can still easily access their virtual workspaces.

While VPN is a useful solution for organizations that distribute laptops to their mobile workforce for easy access to applications, it's a different story when employees have to use VPN on their home devices, because it is far more difficult to control and solve potential security breaches.



VDI Advantages

- Secure and seamless access to work files, desktops and applications
- Optimized bandwidth usage.
- VDI processing is server based, powerful end-user hardware is not required for certain scenarios.
- Thin-clients and Zero-clients can be used.
- On-demand scalability, easy to add or remove published desktops based on previously generated golden images or templates.

VPN Limitations

- Large bandwidth connection may be required.
- Difficult to solve security deficiencies for endpoints: OS patches, antivirus pattern files.
- Good end-user hardware required for client-side processing under certain use cases.
- A VPN client installation may be required and it might not be available for some device types.

Spend less time troubleshooting with VDI

With VDI, IT departments spend less time troubleshooting problems. As data is centralized, it is straightforward to support end-users. VDI's centralized format enables 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 can be 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.

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 be configured not to 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.

VDI extends greater security to IT by enabling them to restrict 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.

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 enables 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.

Flexibility

Parallels RAS can be deployed on-premises, or in hybrid and cloud scenarios, thus providing companies flexibility when deciding which virtualization solution best fits their needs when building VDI solutions. Parallels RAS is able to provision Guest Virtual Machines over a complete set of different hypervisor-based VDI providers when working within the company data center, and over Microsoft Azure if a native cloud solution is required. Additionally, Parallels RAS is fully compatible with Microsoft's Windows Virtual Desktop cloud service; therefore, enterprises will be able to separate their VDI workloads among different providers according to their requirements, and centrally manage them from a single point.

Optimized resource usage

Often, the number of available desktops required by a company varies according to its needs in the moment. Parallels RAS includes auto-provisioning and auto-scaling features that provide enterprises on-demand scalability when provisioning VDI workloads, thus optimi-zing resource usage and reducing costs. Combining cloning technologies, preparation, and customization tools such as RASPrep and profile persistence tools such as FSLogix containers, enable enterprises to generate fully operative desktops within minutes. This ensures business continuity and achieves the required service level.

Clientless, HTML5 access

When working with published desktops in Parallels RAS, resources may be accessed using the native Parallels Client and the HTML5 Client. One of the main advantages of using the HTML5 Client is that there is no need for any installation or configuration on the client-side. This is of great benefit to administrators as they can reduce their management tasks while accelerating the deployment time. Users can securely access their desktops from literally anywhere with an Internet connection and an HTML5-enabled web browser, without the need for any specific device or setup.

Built-in security features

In terms of security restrictions, Parallels RAS includes different built-in features that can be configured to help enterprises build secure VDI solutions. In addition to supporting different multi-factor authentication providers, Parallels RAS equips companies with the ability to allow or to decline incoming connections based on different criteria such as client type or the Secure Client Gateway used. Furthermore, different configuration policies can be applied to the clients and it's possible to turn them into thin clients, preventing users from running or installing undesired software.

Give Parallels RAS a try!

If your remote workers are set up on VPN and you're contemplating a VDI solution, why not give Parallels RAS a try by downloading our 30-day trial? Within minutes you can install a fully functional Parallels RAS deployment from the Microsoft Azure Marketplace and from the Amazon AWS Marketplace. That way, you can check out all the benefits highlighted here, including more flexibility, security and optimized resource usage.