Microsoft Azure

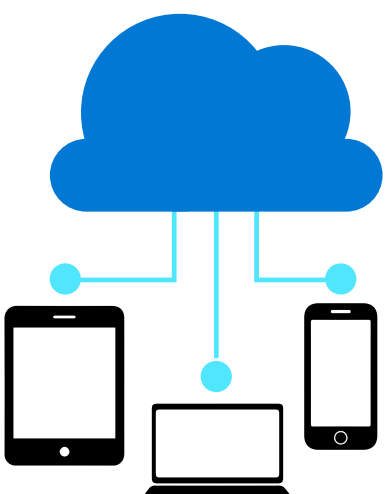
Five benefits of migrating Remote Desktop Services to Windows Virtual Desktop

As companies adapt to new ways of working, enabling secure, remote work through virtual desktop infrastructure (VDI) is becoming increasingly important. Remote Desktop Services (RDS) is a common on-premises solution; however, it doesn't realize the full value of modernization.

Windows Virtual Desktop is a managed VDI-delivered solution hosted on Microsoft Azure that provides a secure remote desktop experience with the benefits of cloud.

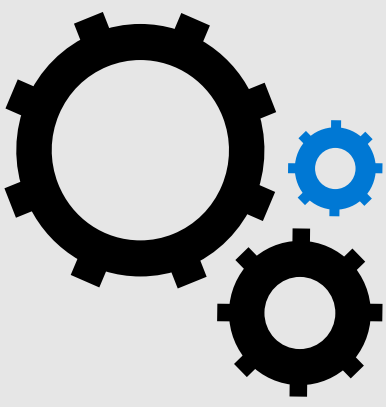
Read below for five key benefits Windows Virtual Desktop will enable for your business, and to learn more.

1. Enable secure and productive remote work from anywhere



- Windows Virtual Desktop provides full Windows 10 and Windows Server desktop and application virtualization on personal devices from any internet-connected location.
- Improve application capabilities with Microsoft 365 Apps for enterprise and Microsoft Teams integration helps end users be productive with the desktop experience they are used to.
- Offer familiar desktop experiences to users when you migrate Server 2012 RDS host and newer versions.

2. Reduce costs of licensing and infrastructure



- With an eligible Windows or Microsoft 365 license, which many businesses already have, you can access Windows Virtual Desktop without any additional license cost, and pay only for what you use. This also includes using the recommended User Profile Management solution, Microsoft FSLogix.
- No RDS Client Access License (CAL) is required with Windows 10 multi-session, which means instant licensing savings.
- Free Extended Security Updates (ESU) until January 2023 are included with Windows Virtual Desktop and you can also make use of the Microsoft App Assure program in case you experience any application compatibility issues.

3. Keep application and user data secure

- Easy apply the right access controls to users and devices with Azure Active Directory Conditional Access.
- Reduce vulnerabilities and help keep your virtual desktops secure by leveraging reserve connection and security solutions like Azure Firewall, Azure Sentinel, and Azure Security Center.
- Use MSIX App attach to deliver applications to your users quickly and securely.

4. Simplify IT management

- Windows Virtual Desktop manages the VDI for you, including infrastructure components such as brokering, Gateway, and Web Access like you do with RDS, so you can focus on users, apps, and OS images.
- Lift and shift RDS session hosts to Windows Virtual Desktop or use Windows 10 multi-session.
- Gain efficiency by using Azure Resource Manager (ARM) and Azure DevOps to implement automation for your Windows Virtual Desktop deployment. You can also leverage advanced monitoring tools, such as Log Analytics and Azure Monitor, that help you understand performance and proactively identify issues.

5. Protect against outages to stay productive

- Help keep your team running during outages by leveraging built-in Azure Site Recovery and Azure Backup technologies managed by Microsoft.
- Mitigate downtime and prepare for planned maintenance with personalised alerts and guidance through Azure Service Health.
- Use FSLogix Cloud Cache to protect user profiles across multiple regions.