ncomputing.com

Solving the BYOD and Mobility Dilemma with Desktop Virtualization

Mike Pagani

As an IT manager, you want the benefits of Bring Your Own Device (BYOD), and you want the productivity boost and competitive advantage that comes from having personal mobile devices in your workplace. You want to be seen as a trusted business partner, working at aligning IT with the company's internal and external directions. For that matter, if some of your co-workers want to provide their own hardware, its great to be able to save the ear-marked costs within your equipment allocation budget and use the savings for other initiatives.

However, you're not quite sure how you are going to effectively support these new devices, are you?

I don't blame you. You don't know what's on them or how their owners use them outside of work. You may not even want them on your network.

Think about mobile devices such as smartphones and tablets. As they continue flowing into your organization – Juniper Research shows the influx will double between 2012 to 2014 – you may find yourself considering strategies that depend on embracing two new acronyms:

- Mobile device management (MDM) – knowing and approving all the smartphones and tablets coming in, tracking them, protecting the data on them and deciding which apps employees can access.

- Mobile application management (MAM) – delivering and maintaining up-to-date and specialized versions of your applications that will need to be installed and run now on each device, monitoring performance, managing group/user access control and probably running an enterprise app store too.

Do you have the time and headcount for all that this entails? Even if you go the smart route and implement ready-made platforms for MDM and MAM, it's still likely to pull your IT effort in yet another direction.

You want the functionality, muscle and physical attributes and user friendly design of the device – screen, keyboard, network connection – so that employees can work remotely and go mobile, but you're not ready to support the devices or the apps running on them, and you don't want to disrupt your standard configuration of operating system and applications. What you don't want is to re-engineer your whole IT delivery strategy.

So, how can you get the brawn of mobile devices without the brain?

You can solve the BYOD-mobility dilemma with desktop virtualization client software that runs on the device, opening a Windows 7 environment centrally hosted and managed from your server. Users launch the app to access your organization's resources – apps, storage, printers, network – isolated from everything else on the device.

The device can be a smartphone, tablet, netbook, laptop or even a PC running Windows 8. Your users have access to a virtual Windows 7 desktop running as an independent image on the device.

Desktop virtualization helps get you out of the BYOD-mobility dilemma by letting you focus on controlling internal assets instead of trying to control the devices themselves. You manage your server and your network connections to users' own devices, and you stay out of the business of MDM/MAM.

Consider it a simple support policy for your co-workers: "Mobile devices can access internal resources only by installing desktop virtualization software. You may use your smartphone or tablet for anything you like inside the company, as long as it's in your Windows 7 desktop session. When you end the session and disconnect from our network, you still have all the usual functionality of your mobile device."

Ready to see what desktop virtualization would look like in your organization? Create an account and try vSpace Client Software for a desktop virtualization session on your computer.