VDI: The Perfect Solution for the Workforce of the Future

As technology becomes more present in every aspect of our lives, professionals want to utilize new and powerful devices to become more productive and flexible, with the ability to work anywhere.

By Reed Martin

The modern workplace continues to evolve. Offices around the world have become as vibrant and active as the employees working inside them, and within this evolution sensitivity to the preferences of the employees has grown as well. As technology becomes more present in every aspect of our lives, professionals want to utilize new and powerful devices to become more productive and flexible in their positions, and the ability to work from anywhere allows for a more cohesive work-life balance.

An issue that organizations are seeing with this new desire to use a variety of devices, including personal devices, is maintaining their security standards while also allowing their employees to have access to critical data that's necessary to complete their respective tasks. Employees are already using personal, unapproved devices and SaaS applications, so the question is, how do you enable a mobile workforce and keep data-in-flight secure and reduce the potential fallout in the event a device is lost or stolen?

Today's workplace is evolving

In researching our second Evolving Workplace Report, we started by interviewing 4,676 full time professionals across 12 countries in both emerging and developed markets. What we found consistently among these employees was a desire to be more efficient and effective regardless of their location. Fully 60% of the professionals in our survey reported using more than one device when working, and expressed the view that this approach was necessary due to various limitations. While the desktop was still the preferred device by 75% of office workers, it is important to note that this number was 85% two years ago. This 10% decline is indicative of the ongoing shift in preferences for alternate devices such as smartphones and tablets.

Fully 60% of the professionals in our survey reported using more than one device.

Allowing your employees to reach their full potential

Mobility is a fact of life in the modern workplace. Our recent study showed that 48% of the professionals in developed markets, and 83% of workers in emerging markets, perform some aspects of their jobs from home. Employees desire a higher degree of flexibility to allow them to be more efficient and dynamic. As mobility becomes a more frequent demand in the modern work environment, people expect access to their data, applications, and workloads when working remotely. This necessity, however, has posed many problems for employers, such as an inability to keep tabs on what applications their users are leveraging from the public Internet and on their mobile devices which they often leverage for work purposes.

As previously stated, a majority of employees use multiple devices to perform their jobs. Younger employees whose ages range from 18 to 35 reportedly use the most devices. While older workers still prefer the use of a desktop or laptop, all-in-one devices are rapidly gaining popularity among senior executives. This diversity in preference of technology has made it increasingly difficult for employers to keep their networks secure.

The cost of upgrading user devices to the latest-and-greatest offering users have in their personal lives is an untenable proposition. As a result, as innovation continues to advance, personal devices are often outpaced by several generations ahead of the enterprise refresh cycle. While an employee may be using a desktop equipped with Windows 7 in their office, he or she could be utilizing a newer Windows 8 desktop from home. If employees feel their personal devices are more elegant or can outperform the devices provided by their organizations, how can an employer ensure their productivity while also maintaining data security? A newly-embraced practice among over 50% of employers in developed markets is the concept

While the desktop was still the preferred device by 75% of office workers, it is important to note that this number was 85% two years ago.

of "Bring Your Own Device" (BYOD). In emerging markets, BYOD is a practice shared by 75% of employers. This allows employees to work on their personal devices while the organization strives to avoid any degradation in security.

Among the employees that are allowed or encouraged to use personal devices, only 50% of these devices are secured by the employers using secure software containers (a.k.a. "sandboxing") or mobile device management (MDM) software. Our research showed that half of the employees in developed markets (85% in emerging markets) access personal websites at work. Still others leverage unapproved online storage lockers to time-shift workloads so they can access their deliverables from home or while traveling. Though this affects productivity, the larger concern is for potential security breaches. How should companies allow employees to securely access sensitive or confidential files while prohibiting programs or content on workers' personal devices from impeding performance or compromising vital company assets?

Virtual Desktops Enable BYOD

One answer to maintaining security and performance is virtual desktop infrastructure (VDI). VDI allows for the separation of a desktop environment (along with its associated applications and documents) from a physical client device, and allows employees to access it from their own personal devices. The benefits of VDI include:

- **Secure, mobile access to documents & applications:** Because the desktop operating system, applications, and user data are streamed from a centralized datacenter, the desktop delivery model is inherently more secure and flexible.
- **Simplified recovery process:** Because none of the virtualized components are saved directly to the user's personal device, it facilitates a much more swift and simple recovery process. The employee would simply have to log on to the server from the new device and their tools would be just as they were on the previous device or session.
- **Ease of maintenance:** While the ease of recovery is a significant boon on its own, maintenance of virtualized desktops is simplified as well. When the employee logs off from his or her computer, the desktop can be reset, removing any downloaded software or customizations that they may have added to a legacy endpoint. This not only prevents employees from installing unauthorized applications, but also provides an easy way to troubleshoot: if the system freezes, the employee can simply reboot and have the desktop restored.
- **Flexibility in providing several types of desktops:** Rather than configuring individual desktops for each employee, an administrator can create multiple virtual desktops with settings and layouts that cater to a specific department's workloads.

48% of the professionals in developed markets, and 83% of workers in emerging markets, perform some aspects of their jobs from home.

- **Security measures to set administrative permissions:** Administrators are able to have a level of more granular control over who has access to the network. In the event that a device is stolen or falls into the wrong hands, the person using the device would be unable to view or retrieve the critical data it contains.
- **Reduced costs in both technology and IT:** In the end, all of the benefits of desktop virtualization lead to the same place: a lower total cost of ownership (TCO). VDI architectures allow organizations to ultimately spend less on individual desktops and applications for employees, boost productivity by reducing downtime, and allow employers to redirect IT employees towards more strategic projects.

What we see in virtualization software is the ability for a professional to remotely access data and workloads without compromising security. In a nutshell, desktop virtualization is a compelling answer to meet the evolving needs of the workforce while enhancing productivity and security.

While the tried-and-true, traditional office may never go out of style completely, it is important to embrace recent trends toward mobility. By providing employees with the flexibility to access the data and applications they need from any device without the inherent security risks, VDI gives employees the ability to be their most productive while giving organizations peace of mind. Desktop virtualization has evolved to offer new capabilities and a level of centralized IT control that is perfectly positioned to meet the demands of the workforce of the future.

In emerging markets, BYOD is a practice shared by 75% of employers. This allows employees to work on their personal devices while the organization strives to avoid any degradation in security.

For additional information about the vWorkspace virtualization software and the reference architecture for Wyse Datacenter for Microsoft VDI and vWorkspace, visit **www.dell.com/wyse/vWorkspace** or **contact us.**

Dell is the global leader in Cloud Client-Computing. The Wyse portfolio includes industry-leading thin, zero and cloud PC client solutions with advanced management, desktop virtualization and cloud software supporting desktops, laptops and next generation mobile devices. Wyse has shipped more than 20 million units and has over 200 million people interacting with their products each day, enabling the leading private, public, hybrid and government cloud implementations worldwide. Dell partners with industry-leading IT vendors, including Cisco®, Citrix®, IBM®, Microsoft®, and VMware® as well as globally-recognized distribution and service partners.

For more info, please visit **www.dell.com/wyse**

Reed Martin is a Senior Technology Marketing Manager in the Cloud Client-Computing division at Dell.