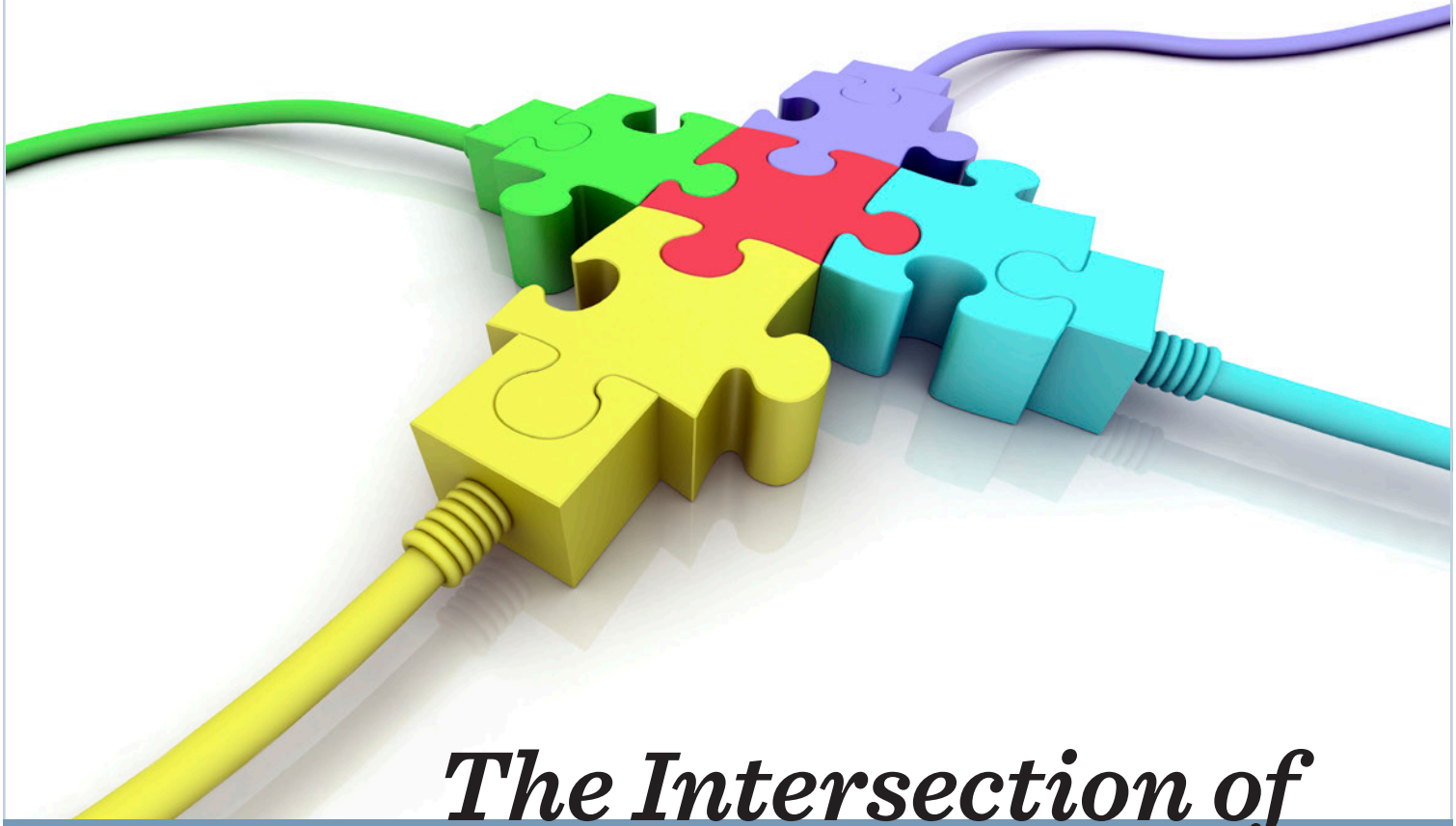

The Intersection of Desktop Virtualization and BYOD

Managing employee-owned devices has become a necessary task for many companies. Virtual desktop infrastructure can bring control back to the data center and support a stronger BYOD policy.

BY ALASTAIR COOKE

FOR MANY USERS, the ready availability and power of modern consumer mobile devices has caused a shift from laptops and desktops to smartphones and tablets as preferred methods of working. Many corporate IT departments have struggled to match the rate of change in consumer IT. Bring your own device (BYOD) policies can return control to IT, allowing staff to use devices that do not belong to the company—but under IT rules and supervision. Still, IT departments have struggled to find the best ways to exert that control and centrally manage BYOD devices.

CAN VDI SIMPLIFY BYOD MANAGEMENT?

Virtual desktop infrastructure (VDI) can reduce the administrative and management headaches introduced by user-owned devices in the enterprise. VDI enables sensitive applications and data to live in the data center where they can be centrally protected and managed. The VDI model puts a user's desktop operating system, applications and data on a virtual machine (VM) in a data center. In general, users get a desktop that they can customize and work with like their own PC, but they control the virtual desktop from a thin client at their desk. When VDI is done well, the user neither knows nor cares where his desktop VM runs or how it is assembled. This approach can also be applied to mobile devices, with a mobile device in place of a thin client. The device then allows the desktop to be accessed

from anywhere with a network connection. Staff can use various devices in different places to remotely access the same data and applications in the data center.

There are pros and cons to virtual desktop infrastructure. IT must also contend with performance, usability and licensing issues, so the decision to provide users with access to virtual desktops through their devices should not be taken lightly. Nonetheless, combined with a well-planned BYOD policy, VDI can prevent users from taking IT into their own hands and putting the organization at risk.

BENEFITS OF USING VDI FOR BYOD

If used properly, VDI can enable BYOD by delivering a full suite of company applications and data to an employee-owned mobile device, without having to modify existing applications or expose sensitive information. The first benefit of keeping the desktop inside the data center is improved security. Rather than the device becoming an uncontrolled security time bomb full of sensitive company information, it's simply an entry point to unmodified applications and data that reside in the data center. The VDI desktop continues to be the place where information is protected from disclosure and loss.

VDI can prevent users from taking IT into their own hands.

Confining data and applications in one place can also streamline the licensing process and reduce the licensing liability risks that can accompany BYOD. It can also help meet a company's backup, recovery and compliance needs by preventing employees from storing unique company data on their devices and in cloud-based applications.

All these elements contribute to another key benefit of using virtual desktop infrastructure for BYOD: easier management for the IT department. IT doesn't need to manage a whole lot of devices, allowing them to focus on managing the data and applications inside the firewall and, even better, inside the data center. Since any device with a virtual desktop infrastructure client can be used, employees gain flexibility without creating friction with IT or risks for the organization. With more secure options for getting work done remotely, there are productivity benefits for both IT and users.

POTENTIAL DOWNSIDES TO USING VDI FOR BYOD

While VDI reduces security and compliance risks and can remove the need for IT to manage disparate devices, there are two major drawbacks to using VDI as a BYOD tool. First, VDI works only with a network connection—preferably a strong one. Second, desktop user interfaces may not be compatible with every device.

Since a VDI client—whether it's a traditional thin client or a mobile device—is simply a way to access the virtual machine, there needs to be a network connection between the VDI client and the desktop. Most products have some sort of over-the-Internet transport using Secure Sockets Layer for encryption; these allow secure access to the VDI desktop from the Internet or any other untrusted network. The speed and latency of that network can become an issue on the user end, as all screen updates must move over the network and a slow network can make the VDI desktop slow to update its screen. Slowness is most often visible with mobile networks, although newer networks like LTE are raising the standard. In rural areas with 3G networks, staff are more likely to experience patchy coverage or reduced speed, leading to difficulties accessing their VDI desktop. Some VDI products enable downloading the VM from the data center to a user's laptop and running the virtual machine on the laptop, removing the need for network access. But these offline VDI technologies are not recommended, especially for BYOD, since they eliminate the benefit of keeping applications and data inside the data center. Moreover, they usually don't work with Apple laptops or with most tablets and smartphones. In cases where connectivity is a problem, it usually makes more sense to give staff members a corporate-built laptop than to allow them to use their own device for work.

Desktop interfaces may not be compatible with every device.

The other major obstacle to using VDI to facilitate BYOD is that putting a modern desktop operating system onto a small handheld device or a device designed for touch is a real challenge. The issue is that most desktop operating systems are designed for a windows, icons, mouse and pointer (WIMP) interface. Tablets and smartphones don't have W, M or P—instead, they have full-screen applications and typically use touch. Whether this translation works for your staff depends largely on their purposes for using the VDI desktop and where they plan to use a mobile device. Using a touch device as a VDI client may prove surprisingly useful with

support from newer desktop operating systems and VDI client releases, but your VDI mileage will vary. Testing by real users and the real devices they will use is important in deciding whether VDI should become part of your organization's BYOD policy.

ESTABLISHING A BYOD POLICY WITH VDI IN MIND

As IT professionals map out a BYOD policy, incorporating VDI options may help resolve many problems that crop up with employee-owned devices in the workplace. A major BYOD policy decision involves information security. Which kinds of data can reside on which types of devices? On the continuum of trust for devices, employee-owned mobile devices connected to the Internet with no corporate oversight and control are the least trusted, while servers inside corporate data centers are the most trusted. Most organizations map the degree of trust to a degree of access; the more trusted the location, the more access to applications and data. Sometimes the level of access granted is an all-or-nothing decision; in other cases, organizations create highly granular rules with a lot of inspection of the device before it is granted access to applications and data. Using a mobile device as a VDI client requires much less trust of the device, because the data and applications never reside on the device itself. For some organizations, this makes for a much simpler test of trust and more straightforward path to a BYOD rule. In that case, the policy might be that any device can have VDI access, but if it isn't a corporate device, then the only access allowed is through VDI.

Another policy consideration concerns the level of control IT has over personal devices. Users want to be sure that IT cannot see or delete their personal contacts, email, photos or anything else that they store on a personal device. Conversely, the company needs to be able to protect its data wherever it resides. One option is a corporate-supplied mobile application that wraps all the data and tools that are required to get work done into a single, centrally managed mobile application. This is a good approach if there is already a mobile wrapper for the data types and applications your business needs, but it's usually limited to mainstream applications with mass adoption. While you can access email and create Word documents and the like from a wrapped application, you are unlikely to find your billing system, customer relationship management or dispatch accessible from an off-the-shelf wrapper application.

The good news is that the types of data and applications that work inside these wrappers are usually allowed onto the least-trusted devices, while those that require more trust are likely not to be supported. VDI vendors are starting to add these application wrappers to their products to accommodate mobility needs, but conventional VDI can help here too. The data can remain inside the VDI desktop and be accessed from an untrusted personal device with no change to the existing application.

Software licensing also brings challenges. If privately owned laptops have licensed software installed, who should bear the cost? Software like Microsoft Office has solid rules concerning private-use rights that come with a corporate license, but what about other applications? Computer-aided design (or CAD) apps, video production and even project management software can be expensive and must be licensed for every PC on which it is installed, including the employee's PC if the software is installed onto their BYOD device. What happens if an employee leaves the company? Clearly he or she takes the device, but what happens to the software license? If the software uses license enforcement and places a software license token on the device, the token represents a (potentially expensive) purchased license. When an employee leaves, that token and software instance may be lost. Another licensing trap involves the software that a staff member installs on a personal device and then uses for corporate functions. Who is liable for the license, and if the staff member doesn't comply with licensing agreements, who is liable? Staff may use student-licensed software for business purposes or may illegally download pirated software and use this for business purposes or even for private purposes on the same device.

If a staff member doesn't comply with licensing agreements, who is liable?

VDI can help with licensing issues, because all the applications remain inside the desktop VM in a data center, so there is no loss of license when an employee leaves. Plus, only authorized applications are installed, and since the employee's device is used only as a portal to the desktop, there are fewer liability complications for the company.

Naturally, care is required with license compliance under VDI. IT should make

sure that the approved applications are fully licensed for their use in the organization. There may be special operating system licensing requirements for the VDI desktop because it is remotely accessed. Also, software installed on the VDI desktop may have special licensing for using it remotely, particularly if a single VM is shared by multiple people rather than dedicated to a single staff member. Another aspect here is the proliferation of devices that staff will use; many will have a laptop, a tablet and a smartphone. If your VDI licensing includes a cost for each device from which a desktop is accessed, this setup could get expensive.

CAN VDI SIMPLIFY BYOD MANAGEMENT?

BENEFITS OF USING VDI FOR BYOD

POTENTIAL DOWNSIDES TO USING VDI FOR BYOD

ESTABLISHING A BYOD POLICY WITH VDI IN MIND

Another BYOD issue that VDI can help prevent is employees storing unique corporate data on their devices. From a backup and disaster recovery perspective and from a legal discovery perspective, you want all data in your data center. Tools that sync data, like email and collaboration applications, are useful; the data center always gets an up-to-date copy. However, with content creation apps, like Word processing or Excel spreadsheets, the danger is that information can be generated on an employee device and not end up inside the company's four walls. Tools like Dropbox augment this hazard, as employees can scatter information among multiple devices that aren't yet included in corporate information management. This is even more likely to be a problem for organizations that block Dropbox sync through their firewalls, as this prevents staff from easily bringing documents into the corporate environment. Providing a full suite of applications in the VDI desktop, so that employees don't need to seek alternatives, can help keep information inside the company, as can a wrapped mobile application. Alternatively, most VDI products now recognize the growing importance of BYOD and include file-syncing applications that allow staff to sync files into the corporate file servers from anywhere, giving IT the chance to back up data and recover it should the need arise.

BYOD represents a big change for IT departments. But to prevent staff from circumventing corporate IT in a rush to do their jobs, IT needs to create new policies. VDI is a useful tool in the BYOD toolkit, enabling employee-owned devices to be safely used in ways that would otherwise be unthinkable, and providing IT a way to work *with* users rather than against them. ■

ABOUT THE AUTHOR

ALASTAIR COOKE *is a freelance trainer, consultant and blogger specializing in server and desktop virtualization. Known in Australia and New Zealand for the APAC virtualization podcast and regional community events, Cooke was awarded VMware's vExpert status for his 2010 efforts.*

TechTarget

Exploring the Future of Desktop Virtualization e-book series s a SearchVirtualDesktop.com e-publication.

Margie Semilof
Editorial Director

Lauren Horwitz
Executive Editor

Phil Sweeney
Managing Editor

Eugene Demaitre
Associate Managing Editor

Laura Aberle
Associate Features Editor

Linda Koury
Director of Online Design

Neva Maniscalco
Graphic Designer

Rebecca Kitchens
Publisher
rkitchens@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com