CDW·G PEOPLE WHO GET IT™

VIRTUAL DESKTOP INFRASTRUCTURE GOES MOBILE

VDI gives agencies a reliable option for addressing BYOD challenges.

Executive Summary

The ubiquity of mobile devices is no longer surprising. As smartphones, tablets and notebook computers proliferate, many users have more than one of these devices — whether personally owned or issued by the user's organization.

Users are increasingly demanding the right to use their personal devices instead of agency-issued devices to access applications and data, a trend better known as "bring your own device." BYOD reduces the number of devices that users need to carry around and maintain, and it allows users to choose the platforms and form factors that work best for them.

BYOD has great potential benefits for government agencies. It is hailed as a solution that can increase productivity and staff satisfaction, while simultaneously streamlining operations and reducing hardware and service costs.

TWEET THIS!

Table of Contents

This is a rare combination, and it's noteworthy enough that many agencies are seriously investigating the merits of adopting BYOD policies and solutions. Some agencies have already established BYOD programs, which increases the pressure on other agencies to follow suit.

But BYOD poses unique technical and security challenges. These challenges, particularly those related to securing sensitive data (such as tax and medical records), are critically important to address so that the information is not compromised. This white paper examines one of the most promising solutions to BYOD security, mobile virtual desktop infrastructure (VDI) technology, and explains how it can effectively address today's BYOD challenges.

Government's Path to BYOD

Allowing workers to access network resources on their own computing devices may seem new, but it's been in practice at many government agencies for over a decade, just known by different names. With the rise of personal computing in the late 1990s, many agencies found that workers were acquiring their own home computers (desktops and notebooks).

Some agencies decided to take advantage of this by allowing staff to access agency email, calendaring and other basic functions from their home computers, generally through dial-up modem pools. This practice increased user satisfaction while also supporting continuity of operations and keeping data from being transferred on data networks over the Internet.

However, these early remote deployments were not full-fledged telework solutions. They typically supported only a few fundamental productivity applications, such as email, and could not support other operational applications because it was impractical — or impossible — to install and configure application client software on each home computer. These home systems used a variety of platforms and had vastly different hardware characteristics and capabilities, making for a support nightmare to install and run most operational applications on them.

These setups also posed considerable security risks by allowing too much access to agency data from computers that were not owned by the government (and thus could not guarantee the same level of protection). Viruses, worms and other forms of malware were rampant and often infected home computers, which tended not to be secured against threats.

They often were running without personal firewalls, antivirus software or other security controls that are in common use today. And home computers were usually shared among members of a household, increasing the risk of malware infection and potential compromise of sensitive agency data.

Some agencies chose to provide enhanced remote capabilities by turning to thin client solutions, such as developing web-based client interfaces for major enterprise applications or using early virtualization technologies to provide portals to the enterprise. These solutions provided access to an increasing number of agency resources while not requiring client installations, or at most requiring the installation of a single web browser or virtualization client. This made support much easier and provided a more consistent experience for users, regardless of the type of personal computer they owned.

Now, some 15 years later, the way workers access the network is evolving again, but with mobile devices such as smartphones, notebooks and tablets in addition to home computers. And once again, the same issues are being raised: How does the agency reduce support costs for operational applications that are accessed from personal devices? How does the agency mitigate the security risks, inherent in BYOD programs, of allowing access to sensitive agency data through nonagency devices?

This white paper will also address these questions and others related to ensuring secure and manageable BYOD access to agency resources.

The Current Security Environment

Mobility inherently poses a security risk, whether a device is issued by an agency or owned by the user. Today's mobile devices are incredibly powerful, capable of much more functionality than the mobile devices of just a few years ago. This makes them useful for many purposes, but in turn it exposes them to many more threats.

Threat exposure is also increased because of the wide variety of unsecured networks that they use. And because the devices are so convenient — small enough to be held in one hand and carried and used anywhere — they are more likely to be lost or stolen.

What makes personal mobile devices riskier than organization-issued mobile devices is that the enterprise usually has full control over the security configuration and installed security controls on the devices it issues. On personal devices, the organization has at best only partial control of device security.

If agencies had trust in the security of these personal devices, then the risk would generally be acceptable. But the truth is that most personal devices don't have the same robust security as agency-issued devices, and because they tend to be used in a wider variety of environments, they face more threats.

Lulled into Complacency

Some observers don't consider mobile device security to be a high priority because of the general lack of attacks against smartphones and tablets. While it is true that these devices have yet to face widespread attacks, it's foolish to think that they aren't at risk.

For example, numerous "applications" for smartphones and tablets have turned out to be malware. Also, smartphones and tablets have vulnerabilities, same as any other computing device, that require patches and security configuration changes.

The possibility exists for any mobile device to be targeted by an attacker at any time. Worse, because personal devices generally lack the security monitoring capabilities that other computing devices have, it's often difficult if not impossible to detect that an attack has occurred. This creates an environment that's friendly to attackers, with a multitude of devices that are vulnerable, exposed to threats and incapable of detecting malicious activity.

Enterprise MDM: A Partial Answer

Enterprise mobile device management (MDM) technologies have been proclaimed as the solution to BYOD security and device management. Unfortunately, enterprise MDM technologies can do only so much to secure personal devices.

These technologies control just a small portion of the mobile device, attempting to sandbox the agency's data and applications so that other applications on the mobile device cannot access them. However, this is technically difficult to accomplish on personal devices because the organization doesn't control them.

In short, enterprise MDM technologies are not foolproof. While they are a major step forward in managing the security of personal devices in BYOD programs, they have inherent limitations that leave sensitive data on such devices at significant risk.

For example, an MDM solution may store sensitive information in an encrypted container on the mobile device, but this information is accessible whenever the container is unlocked (that is, whenever the user is accessing enterprise resources). This creates the potential for data leaks. Enterprise MDM technologies are still maturing, so they often lack key features that would help improve security.

How Mobile VDI Addresses BYOD Challenges

Most government security concerns boil down to one thing: protecting the confidentiality of sensitive information. This is certainly the case for BYOD programs. An agency wants to enable its staff to access applications and data from whatever devices and locations are convenient for them, while simultaneously safeguarding the data. An emerging technology that strongly supports this goal is mobile VDI.

Mobile VDI Basics

As the name implies, mobile virtual desktop infrastructure technology refers to the infrastructure that provides a virtual desktop of sorts to mobile devices, such as notebooks, tablets and even smartphones. The mobile VDI solution provides a thin client experience that is intended to be consistent across different types of devices, except for those physical characteristics that are device-specific (such as screen size and input method).

Mobile VDI has two basic client architectures:

Client-based mobile VDI: Typically, a mobile VDI client application is installed on each mobile device. This application creates a VDI session between the mobile device and the organization's computing infrastructure. The VDI session allows the mobile device to access various applications and data through a virtualized interface.

Browser-based mobile VDI: An alternative architecture uses a web browser (generally, one that supports HTML 5) to access a web-based mobile VDI client. With this architecture, it's unnecessary to install a mobile VDI client application on the mobile device itself, and it is assumed that the mobile device already has a web browser.

Regardless of the client architecture, mobile VDI works by giving the mobile user an image of a virtual desktop. This means that the data and applications stay at the organization's facilities and aren't present on the mobile device.

Only a snapshot of the virtual desktop is transmitted to the user's mobile device. The user's interactions with this snapshot, such as entering data into dialog boxes and clicking on menu options, are transferred back to the VDI infrastructure and converted into their application equivalents.

This arrangement minimizes the storage of sensitive agency information on the mobile device while providing access to the user. The snapshots and the user's interactions with the snapshots are transferred securely between the mobile device and the VDI infrastructure, and each snapshot on the client device is discarded once the next snapshot arrives.

Screen Size and Input Device Differences

Mobile VDI technologies were originally designed for notebooks. The idea was to give the user an experience very similar to using a desktop computer, because the notebook included a keyboard and a traditional input device (mouse, pointer or trackpad).

But today, most smartphones and tablets don't have hardware-based keyboards or traditional input devices. Although some users acquire separate keyboards for use with smartphones and tablets, traditional input devices are virtually unheard of for smartphones and tablets because these rely on touch-screen technology for input.

Without a keyboard or traditional input device, it can be difficult — sometimes impossible — to use certain applications through mobile VDI on a smartphone or tablet. The experience is similar to using a mobile device to access a website that was designed for a desktop or notebook computer.

The user cannot view the entire screen; drop-down menus may not function properly; and other problems may occur because of the diminished screen size and the lack of an input device. Imagine trying to view an enterprise application on a smartphone with half of that smartphone's screen being used for a virtual keyboard — in some cases, it's just not feasible to use an application in this way.

Agencies need to thoroughly test all applications before making them available to smartphones and tablets through mobile VDI technologies. In some cases, applications will need to be reworked for mobile VDI use, such as redesigning web client interfaces or creating a whole new user interface specifically for mobile devices.

Mobile VDI vs. Other Client Solutions

It is important to understand how mobile VDI differs from other types of client computing for mobile devices. With other client solutions, a mobile device often uses a combination of technologies to gain access to applications.

Some applications are accessed through client applications built into the mobile device, such as a web browser or an email client. Other applications require the installation of client application software on the mobile device (generally, one client application per enterprise application). This means each mobile device may have several client applications installed and in use for limited enterprise application access.

This arrangement presents significant security and operational drawbacks. Each client application exposes another vector that attackers and malware can try to take advantage of to compromise the device and its data. Also, each client application needs to be managed — patched, configured securely and updated. With personal mobile devices this is often not feasible, because these client applications are beyond the agency's control.

To address these concerns, enterprise MDM software has become a popular way of securing personal mobile devices. As mentioned earlier, MDM essentially creates a secure sandbox within the mobile device, and all of the organization's applications and data accessed from the mobile device are contained within the secure sandbox.

This prevents other applications on the mobile device from accessing the agency's sensitive data. It also prevents the sensitive data from "leaking" into other parts of the mobile device that aren't protected by the MDM software.

Note that with enterprise MDM architecture, it's still necessary to install client software on each mobile device. The enterprise MDM software has its own client software, and then other applications need to be installed within the secure sandbox controlled by the MDM software.

But enterprise MDM software is not infallible, and any vulnerabilities or misconfigurations in the MDM client software can place the data within it at serious risk of compromise. It's not impossible, though very difficult, for attackers (and annoyed users) to circumvent enterprise MDM technologies.

Mobile VDI: The Goods

Mobile VDI technologies can provide several benefits to agencies, particularly for users who participate in BYOD programs.

Access to agency and personal data: For many environments, secure BYOD would not be feasible without the use of mobile VDI technologies. In these environments, mobile VDI enables secure access to agency data and applications from personally owned computing devices — all from a single device.

Minimal data transfer to mobile devices: An agency's sensitive data (and nonsensitive data, for that matter) is kept on centralized servers within the organization's

facilities. This data is not transferred wholesale from the data center to the mobile device.

Keeping the organization's data off the mobile device reduces the impact of a data compromise, such as the loss or theft of a device. It also somewhat reduces the need to further secure the mobile device, although strong security is still highly recommended. But certain security controls, such as disk encryption, aren't as important when mobile VDI is being used.

Technically, some data is transferred to a mobile device through the screen-rendering interface of mobile VDI. This displayed data can be harvested by malware that can take screen captures.

However, this risk is no different than if the data were stored locally. Screen captures can be taken of any computing device. While mobile VDI does not technically keep all data off mobile devices, it greatly reduces the amount of data received by mobile devices and makes the recovery of stolen displayed data a largely manual (and thus less attractive) process.

Reduced need for client software on mobile devices: Both of the thin client options mentioned earlier (client-based and browser-based) provide a significant benefit compared with the thick client alternative. A thick client requires installing many client applications on each mobile device, perhaps one client for each application that needs to be accessed through BYOD (and for more complex applications, multiple clients).

Minimizing the installation of client software provides multiple benefits. Obviously, it reduces the amount of technical support involved in installing the software, but it also reduces related maintenance concerns, such as patching and security configuration.

It provides a more consistent experience for users, which should cut technical problems and associated support costs. And it also improves security by reducing the number of pieces of potentially vulnerable software being run on the mobile device.

Support for different mobile device platforms: Without a mobile VDI solution, many client applications would need to be installed on each mobile device. It is highly likely that these client applications are available only for a few of the mobile device platforms being used by BYOD program participants.

Agencies may implement a workaround for this (deploying web-based client applications in place of mobile device–based client applications), but this may not be possible for many commercial off-the-shelf applications. And a workaround may be prohibitively expensive for in-house applications, especially for platforms that have relatively few users.

A much more efficient arrangement is to install a single client application on each mobile device. Most mobile VDI clients support a variety of platforms, and mobile VDI products that are HTML5-compatible obviously should work on any platform that supports an HTML5 browser.

The latter option is the most flexible, potentially allowing mobile VDI technology to work on virtually any mobile device. However, because support for HTML5 is still emerging, this option may encounter more technical problems than a mobile VDI client solution.

Single sign-on capabilities: By centralizing access to many applications through a single client interface, mobile VDI technologies can enable single sign-on capabilities for these applications. The mobile VDI technology requires users to authenticate, and this authentication can be integrated with enterprise single sign-on technologies.

An example is deploying a remote access authentication architecture that requires the knowledge of a password and the possession of a cryptographic token. Entering these two factors of authentication into the mobile VDI client application provides assurance that the user is legitimate. From that authentication, the agency can choose to allow access to multiple enterprise applications without requiring separate authentication for each of those applications.

Remote Desktop Access

Some mobile VDI solutions can grant users remote access to their active agency desktop or notebook computers from their mobile devices. From a functionality standpoint this can be highly beneficial, because it places the user in a familiar environment (his or her own computer's interface). And remote access provides a path to anything that he or she could access from that computer, including all data stored on the computer, network file shares and other resources.

Unfortunately, serious security concerns arise from permitting remote desktop access by mobile devices, both personal and agency-issued devices. The risk lies in the need to expose these internal desktops and notebooks to direct access from unknown devices residing on the Internet, and it's a risk agencies must weigh carefully. At a minimum, agencies should have a strong protective layer requiring multifactor authentication between the mobile device and any desktop or notebook authorized for remote desktop access.

Mobile VDI's Fine Print

Although mobile VDI technologies provide many benefits, particularly for BYOD deployments, they also present some challenges that need to be considered.

Introduction of a single point of failure: Any technology that provides access to many resources through a single interface necessarily introduces a single point of failure as well. If the mobile VDI solution experiences a significant failure, then it's likely that none of its users will be able to access any agency resources. Worse, if this failure results from a security compromise, then all of the resources available through the mobile VDI solution — the agency's data and applications — are themselves at an increased risk of compromise.

As with any other important enterprise technology, a mobile VDI solution should be architected and deployed to be highly resilient. This means redundant servers, networking equipment and other solution components, configured to fail over as gracefully as possible when problems occur.

It's also important to strongly secure the mobile VDI solution because it is a natural target for attackers who want to gain access to an organization's sensitive data and applications. These challenges — redundancy and resistance to attack — are common to any major enterprise IT deployment, and they are by no means insurmountable.

Increased IT governance complexity: Adding mobile VDI technology to an agency's existing architecture increases the complexity of IT governance. For example, the agency must alter its policies to include the mobile VDI solution as well as the personal mobile devices that make use of it. Likewise, procedures must be updated to reflect the use of mobile VDI technology.

However, these are largely one-time activities that take place only when the mobile VDI technology is first deployed. In many environments, a more significant challenge to IT governance complexity is the need to ensure compliance with agency security practices.

Using mobile VDI technology lessens the need to ensure compliance of the BYOD clients themselves because it prevents data from being stored on the devices. But it doesn't entirely eliminate security concerns. Managing and monitoring the security of these devices often requires the use of enterprise MDM software or similar technology.

Finally, the mobile VDI solution itself brings its own governance issues. As a new component in the IT architecture, mobile VDI requires considerable administrative overhead to acquire, design, deploy and maintain the technology, not to mention managing and maintaining its security.

New Security Risks

Although mobile VDI technologies may aid in improving some aspects of security, they also introduce security risks that must be mitigated. For example, many agencies will want to sandbox any mobile VDI client application to prevent accidental data migration between agency resources and other resources on the same mobile device. Creating a sandbox is not a trivial matter and may require the installation, configuration and maintenance of additional security controls, such as enterprise MDM software, to provide the sandboxing capability.

Other security risks are dependent on the architecture of the mobile VDI software, such as whether it is based on HTML5 and therefore running within a web browser. Relying on a web browser to serve as the mobile VDI client exposes the VDI solution to a different set of threats.

It may be prudent to install a "clean" browser within an enterprise MDM sandbox and to allow mobile VDI access through only that browser, while also prohibiting the browser from accessing anything other than the agency's mobile VDI server. This strongly reduces the risk of a web browser compromise that would affect the security of the mobile VDI solution.

Due Diligence

Before selecting and implementing mobile VDI technology, an agency should conduct extensive planning to ensure that the full impact of mobile VDI is well understood. The following are additional focal areas related to mobile VDI technologies that should be taken into account when planning an implementation.

Network Considerations

Government departments likely will need to update some of their network infrastructure to handle the traffic generated by a mobile VDI deployment. Mobile VDI works primarily by transmitting virtualized screen images from the enterprise to the mobile device.

These images can take up considerable bandwidth, depending on the size and resolution of the mobile device screen, the graphics characteristics of the agency's applications and the efficiency with which the mobile VDI solution minimizes data transmissions while achieving

the necessary quality. Quality is always an important consideration when looking at networks and bandwidth.

High latency is likely to frustrate users, who will expect virtualized refreshes to occur nearly instantaneously for many applications. Agencies should carefully consider quality of service (QoS) issues when evaluating their network capacity — particularly for peak usage expectations — and should conduct extensive testing of the quality of any mobile VDI technology's network performance before rolling it out to a large number of users.

Another network consideration involves disaster recovery and continuity of operations. An agency may think of peak usage as being peak standard usage. But BYOD technologies are most widely utilized when workers are unable to report to the office, such as during severe weather.

Some agencies even require users who are homebound during such events to telework if at all possible, and this telework will likely involve a large number of personal mobile devices. Agencies should consider how effectively a mobile VDI solution's network can support users during disasters and should plan accordingly to provide these users with the necessary services through mobile VDI.

Policy and Guideline Changes

Any implementation of a new technology, including mobile VDI, requires adjustments to existing policies and guidelines. One obvious example is BYOD.

If mobile VDI technology is being deployed to enable BYOD for an agency, then the policies regarding acceptable use, remote access and other related topics should undergo review and revision to ensure that they take into account both BYOD in general and mobile VDI technology specifically. Guidelines related to these policies should also be reviewed and revised appropriately.

It's important to specify which personal mobile devices are permitted. This is often necessary due to technical limitations of the mobile VDI software or associated security controls.

For example, the mobile VDI software may require installation of a client application that is supported only on particular versions of a designated operating system. Agencies may also want to restrict access to platforms that offer certain security features. Making it clear upfront which platforms are acceptable for BYOD use can save a lot of operational and security headaches down the road.

Many other topics should be addressed in these policies and guidelines as well. Departments typically specify which resources may be accessed through BYOD and mobile VDI technology.

Many organizations also have concerns regarding BYOD access provisioning, such as deploying mobile VDI clients and enterprise MDM software to personal devices, and issuing user or device credentials for BYOD participation. Another common topic is security requirements, such as what security features must be present and enabled on a personal mobile device.

It is also important to update acceptable-use policies and associated training and awareness materials to help users understand the proper and improper use of mobile VDI technologies. For example, agencies will want their users to be aware of major physical security risks and how to mitigate them, such as configuring mobile devices to limit damage caused by loss or theft.

Case Study: VDI Rollouts

Read about how some agencies are improving their security by implementing VDI: **CDWG.com/mobilevdi1**

Technology Updates

Agencies may find that they need to perform some technology updates in order to support mobile VDI for BYOD users. An example is increasing network bandwidth within the enterprise or between the enterprise and the Internet. Organizations may need to upgrade their network equipment along the path from the mobile VDI solution to the border with the Internet, as well as possibly purchasing additional bandwidth from Internet providers.

Agencies also need to evaluate the bandwidth capabilities of their internal BYOD networks, including wireless networks dedicated to supporting personal mobile devices. There could be a surprisingly large amount of mobile VDI traffic occurring on these networks or passing through intermediate agency networks to the mobile VDI infrastructure.

The servers that will house the mobile VDI infrastructure also may need to be updated. Because of the graphics-intensive nature of mobile VDI and virtualization, agencies may need to acquire servers with processors that can handle greater workloads.

Organizations should perform "stress testing" on VDI servers before going into full production. This will allow the IT team to determine how many concurrent sessions and applications they can truly support and what loss of performance may be encountered as the number of concurrent sessions and applications increases.

Application Usability

A final area of strategizing for mobile VDI is application usability. To some extent, this involves performance concerns, but usability reflects much more than just performance.

Some applications may not be suitable for mobile VDI use because of their interfaces. Applications that have been specifically designed for large screens and mouse input may not be usable on a smartphone touch-screen, for example. Some applications that are particularly graphics-intensive may also be too constrained by the communications model used by mobile VDI technologies.

Agencies also should consider the general usability of the mobile device. When the mobile VDI client software is running on the mobile device, how much of a performance impact does it cause for the other applications on the device? Are users able to switch between the mobile VDI application and other applications without disruptions in functionality? How do performance and behavior change when different combinations of agency applications are run through mobile VDI software?

These are all considerations that agencies must give attention to when planning mobile VDI deployments.

The Value of Mobility

A 2013 report indicates that while mobile devices improve productivity and that many government users bring their own devices to work, the vast majority of agencies do not have an official BYOD policy. What follows are some relevant responses.

■ **Federal users** | ■ **State/Local users**

95% | 98%
Say their work has improved as a result of having access to mobile devices, including better communication with colleagues, improved customer service, better collaboration and increased productivity

49% | 71%
Say they use personal devices for work-related tasks

11% | 13%
Say their agency has implemented a BYOD policy

57% | 56%
Say they would consider paying to have their personal device upgraded or certified as safe

Source: *The 2013 Digital Dilemma Report: Mobility, Security, Productivity – Can We Have It All?* (Mobile Work Exchange,, 2013)