WHITE PAPER

CDW·G PEOPLE WHO GET IT

CLIENT VIRTUALIZATION

With more computing device options entering the workplace, client virtualization's traditional benefits become even more appealing.

Executive Summary

Government IT leaders today face conflicting demands. On the one hand, they must operate under ever-tighter budgetary restrictions. On the other hand, they are under increasing pressure to provide a greater range of services, operational flexibility and improved security.

This continuous push and pull is happening in the shadow of the largest infrastructure upgrade challenge of the past 12 years: Microsoft Windows XP is finally approaching the end of its operational life. The best way to address this combination of challenges is to fundamentally reassess how IT departments deliver client computing.

Many public-sector organizations have been quick to recognize the security, performance and ease-of-use benefits that can be achieved using the latest client virtualization technologies to support mobile users. Yet, few have considered the benefits of client virtualization as a means for delivering desktop services. In light of today's challenges, it's time to rethink client virtualization; not as a niche solution for mobile users, but as a strategic end-user computing platform.

TWEET THIS!

Table of Contents

Client virtualization — in the form of presentation virtualization, virtual desktop infrastructure (VDI) and other related architectures — comprises robust technology that helps IT leaders manage their desktop environment more effectively. Moreover, client virtualization can help lower costs while boosting productivity in government organizations.

This white paper outlines the attributes and benefits of client virtualization, including operational and security benefits, cost of ownership, technology selection criteria and implementation guidelines. It offers recommendations for starting out on a client virtualization overhaul to ensure successful adoption — not just for mobile staff, but for all in-office workers too.

What Is Client Virtualization?

The first recognizable implementation of client virtualization was the X Window System, a graphical remote display standard that was introduced in the mid-1980s. As a Unix-based technology, the X Window System had little relevance to most mainstream workplace environments. It was not until 1995, when Citrix Systems introduced WinFrame and extended the use of remote display technology to Microsoft Windows itself, that client virtualization saw significant adoption in workplace environments.

Early adopters of client virtualization used it as a point solution to overcome application performance and compatibility problems, remote access challenges, and other more complex issues not easily solved with conventional distributed-desktop technologies. However, in recent years, client virtualization has diversified and expanded to incorporate multiple new technologies and system architectures, extending its reach to the point where it now offers significant advantages over legacy Windows management systems.

Client virtualization technologies now support all of today's mobile, general-purpose and secure computing requirements. As a result, government IT departments can use a single platform to address multiple technical requirements and operational needs.

As the number of different client virtualization technologies has increased, so too has the need to understand the strengths and weaknesses of each. Similarly, as individual products have matured, the degree of overlap among competing solutions has increased, which makes the job of identifying the most appropriate solution more important.

Finally, as desktop computing environments have grown more complex, it's become critical for government agencies to seek expert advice and in-depth experience with desktop infrastructure transformation projects to ensure the success of a client virtualization project.

Client Virtualization at Work

On the federal level, the Air Force is leading the way in adopting client virtualization technologies. In line with plans issued by the Defense Department to rely less on PCs and more on mobility and thin clients, the Air Force is planning to deploy 9,000 virtualized desktops on the military's unclassified network and 6,200 on the classified network at Scott Air Force Base.

Located in Illinois, the base houses the headquarters of numerous Air Force and military organizations. Ultimately, the Air Force's client virtualization plan will support at least 80 percent of Air Force users on a virtual desktop infrastructure for both unclassified and classified network access.

In Virginia, the Newport News Police Department has already transformed patrol cars into mobile offices by outfitting its vehicles with Panasonic Toughbook CF-30 and CF-31 notebook computers running Citrix XenApp client virtualization software. XenApp delivers applications from the department's data center over a cellular network to the notebooks.

Client virtualization lets officers immediately access critical data in the field, enhancing their ability to make informed decisions quickly. Officers use XenApp to access an array of applications hosted in the data center: to query existing records and the FBI's National Crime Information Center, access dispatch operators, and tap into jail management systems.

In many respects, client virtualization represents a logical progression from server virtualization. Much of the core technology used in server virtualization is also used to deliver client virtualization. And client virtualization delivers many of the same operational benefits as server virtualization. But client virtualization should not be mistaken for server virtualization at the desktop level.

Client virtualization is more extensive. It's not about consolidating desktop workloads into fewer physical boxes, although that is (frequently) part of the equation. Rather, client virtualization is about being able to centrally orchestrate the creation of personalized working environments (applications, data and user profiles) and enable access to them in the manner most appropriate to each user's computing and communications environment.

Client virtualization moves control of desktops from endpoints to the data center, eliminating the need for administrative privileges on the desktop and ensuring full compliance with organizational governance, risk and regulatory policies.

Client virtualization transforms desktop management from a device-centric service to a user-centric service. In adopting a user-centric management paradigm, client virtualization ensures the seamless delivery of applications, data and resources to users, regardless of the computing device they use.

The Five Architectures of Client Virtualization

Client virtualization architectures fall into five main groups, broadly categorized by three main characteristics:

- Where the processing takes place, either on the desktop/device or in the data center
- What is delivered to the user, individual applications or an entire desktop environment
- How user specific settings (user profiles) are managed

Presentation virtualization, also referred to as terminal services or remote desktop services (RDS), is the most mature and most widely used client virtualization architecture, with approximately 100 million licenses in use today. In a presentation virtualization environment, applications run on shared Windows servers hosted in a remote data center with only the application's user interface presented on the user's desktop.

User input is redirected over the network to the server using a dedicated remote-display protocol. The client can be either a dedicated hardware device, a thin client (essentially, a stripped-down PC with no hard drive) or a software client that runs on a converted PC, tablet or smartphone.

Virtual desktop infrastructure (VDI), also referred to as server-hosted virtual desktops, is an evolutionary step beyond presentation virtualization that has yet to achieve widespread acceptance. By late 2011, approximately 20 million VDI desktops had been deployed, although adoption is accelerating as the technology matures and projects move beyond pilot stages.

Like presentation virtualization, VDI runs on a shared infrastructure hosted in a central data center and uses the same thin client remote display technology. But, whereas presentation virtualization utilizes a shared-server operating system to deliver individual applications, VDI uses a standard desktop operating system running on a hypervisor.

This offers greater application compatibility than server-based presentation virtualization implementations — but at a cost. VDI is significantly more expensive than presentation virtualization. Moreover, government IT organizations have to give careful consideration to choosing the appropriate VDI technology.

Presentation Virtualization vs. VDI

Although presentation virtualization is most often used to deliver individual applications, it can also be used to deliver a full desktop environment. These "published desktops" can be made to appear almost identical to a standard Microsoft Windows XP or Windows 7 desktop.

However, not every application is fully compatible with Windows Server, which can lead to performance or stability problems. Furthermore, even when applications are compatible, some vendors will not support the applications when they are run on a server operating system. Under these circumstances, a virtual desktop infrastructure (VDI) environment can overcome both application compatibility and vendor support challenges.

Using presentation virtualization to deliver published desktops can be administratively complex. Strict change-control rules must always be followed, and a comprehensive test of any change is always recommended. Strict change control and comprehensive testing can lead to delays in releasing changes to production, which creates operational difficulties in environments that are subject to frequent updates.

That being said, because presentation virtualization shares a single instance of Windows Server between multiple independent sessions, each session uses significantly fewer resources than an equivalent VDI session. This can significantly reduce the cost of presentation virtualization compared with an equivalent VDI implementation. Lower resource utilization directly contributes to lower capital costs, and fewer servers can also significantly reduce operating expenses.

VDI does offer benefits beyond application compatibility. Running each virtual desktop on a dedicated operating system can provide improved security and limit the impact of any operating system failure.

VDI also supports both persistent and nonpersistent virtual desktops, allowing for greater flexibility in system design. For instance, VDI can accommodate environments where personalization of the desktop is desirable, as well as environments such as call centers where IT would like a pristine desktop every time the virtual desktop is launched. This degree of granular control is not possible with presentation virtualization.

Given the strengths and weaknesses of each technology, a general rule of thumb is to use presentation virtualization wherever possible and VDI only when necessary. As always, detailed analysis is required before making fundamental architectural decisions.

Intelligent desktop virtualization (IDV), also referred to as distributed-desktop virtualization, is the reverse of VDI. Whereas VDI replaces a conventional desktop PC with a thin client or tablet and hosts the desktop OS on a server hypervisor in the data center, IDV implementations retain a conventional desktop PC at the endpoint running a locally installed client hypervisor to host the desktop environment.

The IDV approach is potentially less disruptive than VDI in that it does not require a large data center investment. And because all the applications are installed locally, it allows for offline operation. At the same time, however, IDV requires greater security, especially when used with mobile PCs. Plus, at present, IDV does not support mobile clients such as smartphones and tablets.

Application virtualization and **application streaming** are closely related technologies that can form the basis of a complete client virtualization solution. Or they may be used in conjunction with both presentation virtualization and VDI. With application virtualization, applications run locally on the computing device, but they are not installed on the device in the conventional sense of the term.

Instead, applications are packaged so that they run inside a virtualization layer that controls access to the underlying operating system. This removes many operating system-specific dependencies and allows applications to run in environments that would otherwise cause compatibility problems.

Application streaming extends application virtualization to the data center by optimizing the package so that the components needed to launch the application get delivered first, with the rest of the package components delivered on an as-needed basis. This allows organizations to host applications in a central location and stream them to the desktop at run-time instead of loading them on a desktop or other computing device in advance.

Both application virtualization and application streaming can be used in conjunction with presentation virtualization and VDI to simplify operational management challenges by reducing the number of applications installed directly into the operating system. This reduces both application compatibility issues and the amount of regression testing needed following any application or operating system changes.

It is also beneficial in environments where VDI is used in conjunction with conventional or IDV desktops. A single application virtualization package can be used across presentation virtualization, VDI, IDV and conventional desktops. This eliminates duplication of effort in developing application installation packages for each different environment.

User profile virtualization (or simply user virtualization) seamlessly delivers a standard client configuration not only to users' desktop PCs, but also to all other forms of client virtualization. Regardless of how client virtualization is implemented, it is important to understand that a successful, productive environment must account for the user experience.

As smartphones and tablets proliferate, the number of computing devices that a user might interact with in the course of conducting government business increases. Because of this, it is important to ensure a consistent user experience across all platforms at all times.

For example, a change to application preferences on one device must be reflected across all of them, whether the user is accessing the application on a mobile device or at a conventional desktop. Through user profile virtualization, what a worker sees on one device is what is seen on all devices.

User profile virtualization can also be invaluable during planned desktop infrastructure upgrades. For instance, with less than two years before support for Windows XP officially ends, government agencies are looking to migrate to Windows 7. User profile virtualization can make it significantly easier for IT to transition user profile settings from one operating system to the other.

Client Virtualization Benefits

From an IT standpoint, client virtualization can be extremely beneficial for desktop management. Unlike conventional desktop infrastructures, which rely on a patchwork of device-specific hardware and software components to provide remote support, all client virtualization solutions (regardless of product architecture) offer the ability to centrally manage every aspect of each user's desktop environment — with no operating system dependencies.

IT departments can safely and securely manage every aspect of a desktop, even when the desktop operating system is infected with malware or incapable of booting up. Any patches that must be made to the virtualized desktop environment can be performed remotely through a single point of management, minimizing both end-user disruption and IT administration costs.

Today, the most advanced thin client running a virtualized computing environment can not only replace a conventional desktop PC, it can also incorporate unified communications features that replace conventional telephones as well.

As significant as the benefits to desktop management are, client virtualization solutions offer their most tangible advantages at the desktop itself. Aside from occupying a dramatically smaller footprint, thin clients also run cooler and quieter than conventional PCs, contributing to a better, more sustainable working environment.

Thin clients (and zero clients, which are similar but do not include an embedded operating system) also support higher system availability. And they usually return to service faster in the event of equipment failure. Thin client hardware does not require the same frequency of software and OS patching that conventional desktop PCs require. And they are not considered to be at risk for malware attacks, further reducing the possibility of disruption due to emergency patching.

Even in the event of total system failure, it's possible to return the end user to a previously saved configuration with greater assurance and in less time than with a traditional desktop PC using conventional backup and recovery methods. This is especially relevant in distributed-computing environments that do not have onsite IT support services.

Government organizations can stock up on low-cost thin clients, requiring minimal or no configuration, or order replacements via overnight delivery. Minimally trained staff can swap out failed thin clients, eliminating the wait for tech support.

It's important to note that client virtualization does not require thin clients on the desktop. Desktop PCs and notebooks that are managed using client virtualization systems can be easily managed and replaced, although a small amount of data loss may occur.

Regardless of technology, support activities that previously required onsite, deskside assistance can be delivered remotely and on demand through client virtualization. Activities that might previously have resulted in significant disruption, such as reimaging a desktop, installing new software or recovering damaged or deleted files, can be performed remotely in minutes. In every case, client virtualization delivers improved IT services at a lower cost than conventional desktop technology.

Considering Client Virtualization

When considering client virtualization, it's better to determine which architecture is best suited to a particular use case than to formulate a use case to fit an architecture. Most client virtualization products support multiple independent architectures in a single solution, providing a combination of VDI, presentation virtualization and distributed client virtualization solutions in a single product.

Client virtualization for the sake of client virtualization may prove challenging to deploy. So government agencies and their IT staffs should be on the lookout for computing challenges that might trigger (or lend themselves better to) a client virtualization transition strategy.

For many government organizations, one of the most obvious triggers for initiating client virtualization today is the transition from Windows XP to Windows 7. With less than two years to go before Microsoft ceases to support one of the most successful and widely used operating systems, there has never been a better time to consider client virtualization. Virtualizing the computing environment now will make migrating later to a new OS throughout the agency a far simpler proposition.

The other prominent trigger for launching a client virtualization project is the introduction of mobile initiatives to the organization. It's not just that notebooks and tablets have become more critical to government operations.

Teleworking and increasing support for bring-your-own-device (BYOD) policies (which encourage agency workers to use their own smartphones, tablets and mobile PCs to perform their jobs) have also increased the need to present a unified, centrally managed client environment to a growing number of endpoints. The more devices the IT group must account for, the more sense client virtualization makes.

Client Virtualization, Consumerization and Mobility

Now more than ever, it is the consumerization of technology that informs expectations of its use in the workspace. At a time when consumer technology is often more advanced than what's available in the office, many IT users in government expect to be able to use the same technology at work that they use at home. The popularity of iPads and Android tablets has forced IT departments to answer complex questions within the context of current IT services delivery.

Client virtualization technologies provide an effective means of securely extending the reach of Windows applications to tablets and smartphones. All major presentation virtualization and VDI platforms provide native client software for commonly used mobile-device operating systems. They also offer enhanced usability features to provide the best possible integration with the mobile-device platforms.

In many circumstances, client virtualization may be considered the de facto standard for personal computing environments. But keep in mind, some environments are better suited to adopting client virtualization than others. The best candidates are those computing environments that are highly homogenous and well understood, such as a call center with a large number of identically configured workstations.

That being said, implementing client virtualization in this type of limited environment tends to be of little value unless it's carried out in conjunction with other IT initiatives, such as unified communications. Nevertheless, if an agency is looking for an area within which to pilot client virtualization (to test both the technologies and implementation processes), such a homogenous environment makes perfect sense.

Where should an agency *not* launch its first client virtualization project? Generally, environments with complex requirements are ill-suited to client virtualization launches.

These include highly diverse environments (for instance, a department of power users who have long-held expectations of being able to install their own applications) as well as environments in which elevated privileges are required (such as computing environments for developers and engineers, which often require elevated IT privileges allowing workers to install and test software). Client virtualization can support these environments, but even with mature technology it is often best to wait until less complex implementations have been successfully deployed.

Regardless of where a client virtualization project begins, it is important to conduct a comprehensive assessment prior to starting work. The assessment process details all applications and user communities across the organization in order to identify which are best suited to client virtualization.

Agencies should pay particular attention to not only application compatibility issues (identifying those applications that might present compatibility problems and require remediation during virtualization), but also to those installed applications that are no longer in use. This is important for avoiding unnecessary application remediation activities, and it also helps agencies reconcile software licenses.

Preparing the Data Center

Client virtualization, particularly VDI, can place unique demands on a data center. Government IT staffs must take these demands into consideration during implementation planning, then constantly monitor them during deployment to ensure all systems are performing in line with expectations.

Data centers are not generally designed with end-user computing in mind. So changes may be required to ensure appropriate availability of supporting infrastructure services.

Mainframe and midrange systems are unlikely to have issues and may actually benefit from implementing VDI or presentation virtualization. In moving the desktop environment to the data center, client-server applications may see significant performance improvement. This can be especially true with those applications that are particularly "chatty," as the reduction in round-trip latency boosts overall application response times.

But agencies will need to assess other services for performance and availability prior to implementation. In large deployments, the IT team may need to install additional Active Directory domain controllers in the data center.

This is sometimes needed to address additional authentication requests that might previously have been performed by servers outside the data center. Similarly, file and print services that might have been deployed outside the data center may need to be relocated when moving to VDI or presentation virtualization.

The challenge of delivering thousands of desktop environments from data center to end user is significantly different than delivering hundreds of servers. The existing storage and virtualization infrastructures will need careful assessment to ensure that they are capable of supporting a VDI implementation. In fact, it may be appropriate to implement separate storage and virtual infrastructures to support VDI.

When implementing a VDI system in particular, extra attention must be paid to storage considerations. The primary challenge is not capacity, but rather throughput. Conventional data center storage area network (SAN) storage is ill-equipped for the I/O demands that the simultaneous boot-up of hundreds of virtual desktops places on disk storage.

Poorly specified data center storage can be a significant bottleneck for VDI deployments, resulting in poor performance and desktop logon times measured in minutes rather than seconds. However, scaling out storage in order to deliver the required random read/write input/output operations per second (IOPS) isn't always economically feasible.

Storage costs of $1,000 or more per desktop are not uncommon. Fortunately, alternative solutions have come to market, including dedicated VDI appliances with onboard solid-state disks, high-performance caching disk controllers that use flash memory, and in-hypervisor disk-image caching.

Data center storage for supporting client virtualization is a rapidly advancing area, with new developments announced on an almost weekly basis. Ensuring access to up-to-date advice is essential to managing VDI storage costs.

For client virtualization to be effective, the entire network infrastructure must ensure appropriate bandwidth to accommodate the different network traffic patterns seen in presentation virtualization or VDI. The adoption of quality of service (QoS) measures and WAN optimization controllers to prioritize, compress and cache network traffic applies to all forms of client virtualization technology, not just presentation virtualization and VDI.

Moreover, in agencies that make extensive use of unified communications, including voice over IP (VoIP) and video conferencing, the IT department may need to ensure that the network can accommodate hairpinning, the process of routing a call request from an endpoint to a server and back out to another endpoint, without degrading performance.

The IT group should also review its internal data center network services in preparation for client virtualization. The availability of advanced application delivery controllers to provide load-balancing services can be essential to

maintaining end-to-end system availability of client virtualization components.

Plus, agencies should consider their physical and logical network architectures to support presentation virtualization and VDI deployments. For example, appropriate network zone segmentation must be implemented to isolate virtual desktops from critical infrastructure services.

What's at Stake in Green IT Initiatives

IT services are responsible for approximately 2 percent of overall U.S. energy consumption. This fact places pressure on government agencies to adopt a greener approach to delivering IT services. Adoption of client virtualization can not only reduce overall power consumption and carbon dioxide emissions, it can also deliver multiple secondary advantages that may be considered part of an overall green IT initiative.

The use of thin clients as part of a presentation virtualization or VDI deployment leads to a direct and measurable reduction in CO^2 emissions. Overall, the use of low-power thin clients coupled with energy-efficient shared servers can reduce overall power consumption by between 50 percent and 80 percent, which may translate into an equivalent reduction in CO^2 emissions.

At the same time, using thin clients can assist government agencies in complying with sustainability initiatives, such as the federal *Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance*, which sets sustainability goals for the federal government in a number of areas, including electronics stewardship, or New York's *Executive Order No. 4*, which established and requires reporting on statewide green procurement and agency sustainability programs.

Thin clients have a considerably longer working life than conventional desktop PCs. Although the conventionally recommended PC replacement timeframe tends to be every three or four years, the operational life of a thin client is usually at least six years, with most devices used eight or more years. (Data center servers are also renewed less frequently than desktop PCs, although they tend to be replaced more frequently than thin client devices.)

And because they're smaller and have fewer parts than traditional PCs, thin clients consume far fewer resources in manufacturing and shipping. Together, the longer operational life of thin clients and smaller device footprint lead to considerable e-waste reduction, in support of the government's goals.

Appropriate consideration must also be given to high availability, disaster recovery and continuity of operations planning (COOP) services. This is especially important in presentation virtualization or VDI environments where failure of key infrastructure components can result in loss of service for many or all users.

Depending on requirements, government agencies, departments or workgroups may want a full-fledged COOP environment built in a separate data center. They might also take advantage of cloud services to mitigate the effect of any downtime at their primary data center.

Finally, the physical data center itself should be taken into consideration. Presentation virtualization and VDI workloads can be particularly demanding in terms of power and cooling requirements.

For example, current-generation, high-density blade systems are ideally suited for a client virtualization workload, but data center infrastructure services must be equipped to support them. With a typical heat load of 300 watts per square foot, blade systems can cause a temperature rise of 25 degrees Fahrenheit in less than a minute when powered on. Starting up a large number of blades at the beginning of the workday may present a challenge to cooling systems designed for load levels that fluctuate more slowly.

Addressing Security

For many organizations, the Common Criteria for Information Technology Security Evaluation, an international standard for computer security certification, is an important requirement when procuring IT products and systems.

To this end, all leading client virtualization solutions have either obtained or are in the process of obtaining Common Criteria certification. Regardless of their status, all client virtualization solutions can provide enhanced security compared with conventionally managed, distributed-desktop environments.

By ensuring that all desktops are managed through a single, central point of control, client virtualization solutions can inherently improve security, regardless of where the endpoints are located. At the same time, by offering a user-centric management approach, client virtualization application delivery can ensure that users get the applications they need, when they need them, without requiring any special or elevated privileges.

Presentation virtualization and VDI solutions provide heightened security by physically isolating the virtual desktop in a secure data center and passing along to the end user only the desktop image and the keyboard/mouse movement. All files remain secure in the data center.

To secure the remote display protocol between the data center and endpoint (and to secure data in transit), the right client virtualization solutions support government cipher suites using RSA key exchange and Triple Data Encryption Standard (DES) encryption, as well as the Federal Information Processing Standard (FIPS) Publication 197, Advanced Encryption Standard (AES) 256 encryption. Support for multifactor authentication technologies, such as the Defense Department's Common Access Card, is also common.

Presentation virtualization and VDI solutions also simplify the introduction of both perimeter and enclave-boundary firewall deployment. Appropriate device-level access control lists ensure that only authorized applications and virtual desktops can gain access to secure server resources.

In contrast, distributed desktop environments access resources from a broadly distributed range of network locations. Centralized solutions share a common IP address range, making access control lists easy to manage and vastly simplifying segmentation of network traffic types to only the appropriate range of IP addresses.

Today's more distributed client virtualization solutions — those that might support a highly mobile workforce — adopt a layered security approach based on granular role-based access control and full-disk AES 256 encryption to secure data on the client hard drive.

In the event that a device is lost or stolen, or even if a device does not reconnect to the network after a predefined time, remote access revocation and remote lock/wipe capabilities can be used to secure or destroy all data. The IT group can employ additional measures, including built-in antivirus scanning, to monitor for key logging or screen scraping software, as well as tamper protection to secure data if an attempt is made to directly copy or edit a virtual disk.

When it comes to client virtualization, regardless of the level of security offered by individual products, IT departments should follow an appropriate layered-security model. All computers must be kept up to date with security patches and effective antivirus software, but staff should also enforce appropriate physical controls. With client virtualization, the benefits of a single, central point of control — regardless of endpoint location — can simplify the implementation and maintenance of effective security controls.