



Client Virtualization for Government

Improved security and long-term cost savings on hardware and staff are a few of the benefits of virtualizing clients

TABLE OF CONTENTS

- 2** Why Client Virtualization?
- 2** How Client Virtualization Works
- 4** How Thin Clients Work
- 5** Benefits and ROI
- 6** Factoring in Support Needs
- 7** Best Practices

Executive Summary

Faced with mounting IT costs and security concerns, federal, state and local government agencies are increasingly looking to client virtualization as a worthwhile infrastructure model. This approach uses innovative technology to move data processing and storage to a server in a data center, which connects to users' desktop devices.

Users typically see little difference in their computing experience. But IT departments benefit from improvements in the ease of managing and maintaining computers, including sharp reductions in the frequency of desk-side service calls.

Often, users' desktop and notebook systems can also be replaced with thin clients — inexpensive and simplified devices that retain no information when a session ends — resulting in a more secure data posture because files reside on central storage devices.

This is an infrastructure model that aligns well with the far-flung organizational structures common to government enterprises, particularly in federal and large local government organizations, but even in many small municipalities too.

As agencies explore this technology, many are already realizing benefits. Users, including agencies with several thousand staff members, can be set up with new desktop devices and applications quickly and easily because installation and configuration is done once, at the server, and duplicated as needed. Users can log onto their own virtual desktops from any device on the network.

Switching to client virtualization requires an upfront investment, but agencies will see the real value in the cost savings accruing a few years later. Implementation should be done in stages, providing an opportunity for testing new systems and giving IT staff time for training. For many organizations, the new technology can bring significant improvements worth the necessary investment and infrastructure planning.



Why Client Virtualization?

Rapid advances in IT are allowing organizations to run operations and deliver services in entirely new ways. At the same time, organizations everywhere are struggling to contain IT costs and counter ever-more-sophisticated security threats to their systems and the data they contain. Client virtualization provides a technological approach to address many of these concerns.

Client virtualization refers to a computing architecture in which the functions of a desktop computer (running and storing software, data and personal settings) are done on servers in an organization's data center. Each desktop device is connected to one of these servers. For users, the experience remains essentially unchanged from how they worked on their traditional desktop computer.

There are compelling reasons for government agencies to choose the desktop virtualization option, including lower cost, easier management and support, and better security.

The pared-down design and features of thin clients, which often replace traditional desktop computers, cost less to adopt and run. They are more energy efficient, resulting in lower electricity bills, and they have the intangible public-relations benefit of being green technology.

But a much bigger source of potential savings is in operation and maintenance. When staff work on traditional PCs, the IT team often must install and update applications on each computer. Troubleshooting must be done separately for each computer, necessitating a desk-side visit from tech support.

The research firm IDC estimates that the total cost of managing a PC can run up to \$1,000 per year or more. In even a small government office, it's easy to see how support can eat up as much as 80 percent of the IT budget.

Virtualization can lower maintenance costs by 40 percent, according to research by IDC and VMware. Since operating systems and software reside on a central server, any updates and patches can be installed once and then appear immediately to all users on the network. In this scenario, IT can much more effectively monitor, quarantine and combat viruses, malware and other attacks.

Should problems occur, machines can be fixed, rebooted or taken offline remotely, requiring far fewer hands-on visits by IT support staff. In large agency environments with multiple locations and buildings, the move to a virtualized desktop can also lead to a drop in travel expenses for major application rollouts and upgrades.

New users, even groups of users, can be set up with computer access and services in minutes, not days. Because user files reside centrally, backups can be set to take place automatically, minimizing the risk of data loss from failed hard drives or inadvertent user errors. This also allows for a quicker recovery point objective (RPO) should a disaster strike.

With the network perimeter now extending beyond the edge of the organization's property, IT security has become a more pressing priority. Mobile users, combined with the very public location of systems in many agencies, only serve to heighten the security demands.

Security is greatly enhanced by moving to virtual clients because the devices that users work on do not store data. The files remain secure in data centers. Lost or stolen devices cannot jeopardize sensitive information.

Because of this combination of lower maintenance costs, improved user portability and increased security, desktop virtualization is catching on in a big way. Research firm Gartner has predicted that the worldwide market for hosted virtual desktops will expand from \$1.5 billion in 2009 to more than \$65 billion in 2013.

Wyse Technology, one of the biggest suppliers of thin clients and desktop virtualization technology, says its most rapid adoption has been in the public sector, especially among government agencies.

A Cloud Precursor

Client virtualization may benefit government agencies' long-term networking goals in another way — serving as a preparatory move toward cloud computing. Also known as software as a service, cloud computing is the delivery of scalable IT applications, services and infrastructure over the Internet. This service is typically offered by a third party, saving the agency time, money and technical resources.

Whereas client virtualization pushes out desktop resources from an internal server, cloud computing provides an array of resources that are delivered by a third party via the Internet. Working out the bugs of a client virtualization arrangement can go a long way toward preparing an agency for cloud computing.

How Client Virtualization Works

Client virtualization is a technology that allows data and computing to be located some place away from the desktop user, usually in a secure data center. There, multiple virtual desktop computers run simultaneously on one or several central servers.

Manufacturer Options

The desktop and application virtualization software field is dominated by three manufacturers: Citrix Systems, Microsoft and VMware.

HP and Wyse Technology are the leading providers of thin clients and now have begun promoting their zero clients — even simpler devices than thin clients because they house neither a CPU nor an operating system.

Other manufacturers providing thin clients and other devices, such as PC blades, include: ClearCube, IGEL Technology, Lenovo, NComputing, Planar Systems and Sun Microsystems.

Each virtual machine has its own operating system, applications, stored data and personal settings, and is encapsulated in an isolated environment. A failure or problem in one virtual machine does not affect the others.

For the user connecting from inside the office or remotely over the Internet, the experience will have a look and feel that's almost identical to working on a traditional PC. Users can access their virtual desktops from a thin client or a standard PC.

This allows for a certain degree of mobility, as users can connect to their personal desktop environment from any networked client device. This mobility is a boon for government agencies, where staff are logging on from office workstations, telecommuting from home and connecting from agency-related remote locations. This also allows staff to share workstations but still have a personalized desktop to themselves.

Several different technologies can be used with a client virtualization solution. The original and still most widely used form of thin client computing, called shared services, runs applications on the server and sends out a regularly updated user interface to individual users. This approach enables users to execute only a limited number of tasks.

A more recent approach, called streaming, sends the entire computing environment, including the operating system and applications, to the desktop device incrementally, as it is needed. There, it runs locally on the desktop's CPU. This technology combines the centralized management of applications and data with performance similar to a PC.

Another approach that is generating a great deal of interest is called desktop virtualization, or Virtual Desktop Infrastructure. With VDI, a thin layer of virtualization software, known as a hypervisor, sits between the server hardware and its operating system. This allows the server to host multiple virtual computers, each with its own operating system and applications, in a tightly isolated environment.

The desktop experience is delivered to each user — and their keystrokes and mouse clicks are returned to the server — via a connection protocol. Several different protocols are available; for example, one is included free with Microsoft Windows operating systems.

This is a powerful technology. If various users in an organization require different operating systems, such as Windows, Linux, Novell Network or Solaris, they can all run on the same physical server at the same time. And a user who needs to run more than one virtual machine can do so from a single desktop device.

If staff need access to sophisticated multimedia applications, such as computer-based training and video conferencing, VDI is an effective technology to deliver these increasingly sophisticated applications while providing a secure, reliable and easier-to-maintain network.

VDI typically includes application virtualization, which can be used with both standard PCs and virtual desktops. Application virtualization is a technology in which an application is run from the server and then streamed into an isolated environment on the target device where it will execute.

The application is essentially tricked into believing that it is directly interfacing with the user's operating system and all the resources managed by it, when in reality it is not.

The purpose of this technical ruse is to avoid incompatibilities among applications. A virtual application doesn't "see" the other applications that may be running alongside it but "thinks" it is executing alone on an operating system. This avoids the need for time-consuming regression testing and allows users to run different versions of the same apps simultaneously.

Application virtualization can help IT managers keep track of application usage and stay in compliance with license requirements. But there is one caveat to application virtualization: While many applications can be virtualized, not all work well in a virtualized environment. So evaluation and pretesting will be necessary before migrating an app to this environment.

Client Virtualization in Government Agencies

- 75%:** The percentage of federal IT managers who see value in virtualization
- 20%:** The percentage of Feds who think their agencies have used it to its full potential
- 79%:** The percentage of agencies that have implemented some form of virtualization
- 49%:** The percentage of agencies that have introduced client virtualization

SOURCE: CDW•G survey of 377 federal IT managers

How Thin Clients Work

As touched on previously, thin clients are pared-down desktop devices that give users the experience of working on a PC, while actually connecting them with a physically remote server where the processing takes place. Thin clients are growing in popularity as increased server processing power and network capacities facilitate improved remote performance.

Advances in thin client technologies themselves are making the devices better able to simulate a full PC experience, while offering an organization important benefits including central control of software and data, improved security and reduced energy consumption.

Thin clients are certainly not a new concept. For decades, task-based workers, such as airline ticket agents and bank tellers, have used them, but often for text entry only and with minimal or no graphical interface. Today, when organizations consider installing thin clients, they are generally thinking about devices that are far more sophisticated than those simple early terminals.

By definition, thin clients have neither hard drives nor other peripherals, such as CD or DVD drives. Today's devices typically have a processor, RAM and flash memory. They also have a light operating system, such as Microsoft Windows CE, Microsoft XP Embedded, Linux or a custom OS.

Thin clients transmit keyboard strokes and mouse clicks back to the server, and the results show up on the user's monitor. With no drives, cooling fans or other moving parts, the devices are more reliable than PCs and tend to last about twice as long (typically six to seven years,

twice the functional lifespan most manufacturers recommend for PCs).

If a thin client does break down, it can be replaced with a new device — with no need to configure it or install software and minimal downtime. Because users' personal settings and files reside on the server, users can log on from any device and access their own desktop. Thin clients are cheaper than traditional desktops, use considerably less electricity and are quieter (since they have no fan or hard disk).

Other devices can often be used in place of a thin client, such as full PCs (running their own programs locally and connecting to a virtual machine at the same time) and mobile devices. Today, zero clients are also available. These machines have no operating system, CPU or memory of their own, but instead rely on the server for all operations and, consequently, require greater bandwidth.

There are four different thin client architectures:

- **SHARED SERVICES:** This traditional thin client form factor runs applications on the server and sends out the user interface, updated in real time, to individual users. This approach is suited for users who work regularly on a small number of applications, including common ones such as Microsoft Office. Users can execute only a limited number of tasks and do not have the same flexibility and functionality they might have with a standard PC. This is still the most widely deployed thin client technology.
- **STREAMING:** In this infrastructure, the server sends the entire computing environment, including the operating system and applications, to the desktop device as needed. There, it runs locally on the client's CPU.
- **BLADE PCs:** Each user is assigned a physical PC (in the form of a thin modular circuit board and hard drive), which is stacked in the data center and accessed via a thin client device.
- **DESKTOP VIRTUALIZATION INFRASTRUCTURE (VDI):** In this infrastructure, a server hosts multiple virtual computers. They all share the server's resources, such as processor and memory, but each is strictly isolated so that any failure of one will not affect the others. This technology is drawing the most interest today.

Where users need web browsing and graphics-intensive programs, streaming, blade PCs and VDI are preferable. Each of these environments has the advantage over a traditional client-server topology of allowing the IT staff to centrally manage applications and data.

Benefits and ROI

For some time now, government agencies have been virtualizing their servers, reducing server sprawl and increasing the use of each physical server's capacity by managing them together as one virtual device.

That first wave of virtualization has been followed by a second — client virtualization — in which computing and data storage are separated from the desktop computer and moved to centralized servers. The first wave brought consolidation of server hardware; the second is bringing easier management of desktops.

When organizations adopt client virtualization, they often switch users to thin clients. As these devices have no hard disks, they cost considerably less than PCs (basic models sell for around \$150). But the biggest savings come from the reduced costs of managing the infrastructure over time.

With traditional desktop computing, one of the biggest drains on IT budgets is the frequent need to update operating systems and applications on each piece of hardware.

With client virtualization, however, multiple virtual desktops run simultaneously and independently on a single physical server. This allows centralized maintenance of the machines and the applications. IT departments install new applications and updates directly on the servers.

The technology is also inherently scalable. All components of a virtual desktop, including operating system and applications, are stored as files, allowing multiple virtual desktops to be updated swiftly and easily.

This eliminates the need for many service visits to individual users. Most problems, including the reinstallation of corrupted programs, can be handled on the server. Users, individually or as groups, can be assigned their own virtual computers very quickly as well.

With no hard drives, fans or other moving parts, thin clients break down less frequently than PCs, so they tend to have longer periods between refreshes. But if one should fail, it can simply be discarded and replaced by a new, inexpensive device. Because the user's desktop image, the virtual machine, resides on the server, there is no downtime needed to reconfigure a new desktop.

IT departments are also freed from most regression testing, the time-consuming task of determining whether new applications (or new versions of existing ones) will conflict with other programs. When installing apps virtually, they interact with their operating system in an isolated bubble, eliminating most conflicts.

Security Gains

Virtualized computer systems are more secure for several obvious reasons: Users can't install unauthorized programs or disable antivirus software. If a user accidentally downloads a virus or spyware from the Internet, it will not propagate. Instead, it will disappear when the session ends. Even if a user connects from a standard PC, the virtual machine remains isolated from locally installed software, risking no application conflicts or virus infection.

Because data is stored centrally and not on the physical device, organizations no longer risk losing sensitive data if a notebook is lost or stolen. Moreover, data and user profiles automatically back up centrally. This provides greater data security and faster disaster recovery.

This also makes compliance with laws, mandates and regulations more straightforward. Government agencies, for example, must comply with the Health Insurance Portability and Accountability Act (HIPAA) legislation on healthcare records, and all organizations must assure privacy of Social Security records.

In a virtualized, thin client infrastructure, all such files remain behind the firewall and can be centrally managed — protected from easy access yet available for easy monitoring or searches. (Keep in mind, other security precautions are still needed for robust protection of these files.)

A Commonwealth Client

The Pennsylvania Attorney General's Office is a strong believer in virtualization.

It has already applied the technologies to its servers and storage systems, resulting in significant benefits. Now it has begun a desktop virtualization pilot. The office envisions a hybrid solution for its 850 staff members. "We believe we can get a third, if not 50 percent, of the devices moved to virtual desktops," says PAG CIO George White.

The office's IT department is evaluating how to best virtualize and support necessary and mission-specific applications. For instance, some of the case management apps do not appear suited to a virtual environment. Even for apps that do work well on a virtual desktop, it's still crucial to think through each app's use process and determine what services, such as printing, will be needed, White says.

Thin clients also use considerably less power than PCs and have to be replaced less often. In fact, client virtualization can bring a real reduction in the total cost of owning and operating computer systems.

But an IT department might have to detail how those savings will accrue over time. This is because of the upfront costs tied to adopting the technology. Thin clients may be inexpensive relative to even the least expensive desktop systems, but buying new servers and upgrading storage and network capacity can drive up initial costs. The cost of training IT staff on the use of these technologies must also be added to this expense.

Factoring in Support Needs

The advantages client virtualization can bring to the management, cost and security of computer systems are what make the technology so alluring to government agencies. But to optimize the benefits that the technology can provide, careful thought must be given to the entire infrastructure supporting client virtualization.

Infrastructure Support

The typical computer infrastructure is composed of several distinct parts, with staff desktops (thin clients, PCs, mobile devices, etc.) at one end of the spectrum and the servers in the data center at the other end. Servers were the first piece of the infrastructure to benefit from virtualization, and many organizations have already adopted this technology to some degree.

Server virtualization involves the consolidation of an organization's server resources onto a much smaller number of physical devices. Software enables each remaining physical server to host numerous virtual servers. Adoption of this technology has been driven by the proliferation of servers — each for a different task, application or physical location.

Typically, less than 15 percent of each server's capacity is used before virtualization. Consolidation through virtualization immediately drives up utilization capacity. With virtualization, utilization often rises to 60 percent, and can go as high as 80 percent of capacity. The results are clear cost savings on hardware, power and cooling, physical space and server management.

Data storage resides close to the data center on the infrastructure spectrum. Government agencies continue to face rapid growth in data, both to support administrative and core operations and often to stay in compliance with various mandates, regulations and laws, such as HIPAA.

Virtualization can improve management and efficiency of data storage. The concept is to have multiple storage devices act like one virtual device, making it easier to centrally manage and back up data.

Other storage-related concerns are rock-solid backup, disaster recovery and archiving. Luckily, many of the technologies that support data storage management are also helpful with disaster recovery.

Storage virtualization can be combined with several other technologies to improve data-access efficiency. These include thin provisioning (reducing the storage space allocated to users in a flexible manner, based on minimum requirements of each), data deduplication (eliminating multiple copies of data beyond needed backups) and data tiering (moving data from high-price/high-performance storage to low-price/low-performance storage as the data's value and access needs decrease over time).

The network is the indispensable web connecting the items along the infrastructure spectrum. As servers are consolidated and storage devices become more interconnected, systems rely more heavily on network connections.

Not only is upgrading to higher bandwidths often needed, but redundancy of cables and switches is required too, just as is common with processors and storage. Organizations may want to also consider WAN and LAN optimization solutions as well.

Device Support

In many organizations, a thin client may be the appropriate access device for most users. As mentioned, these devices have the advantage of low cost and low power consumption.

But agencies can often save money by using their aging stock of standard desktops instead. And with staff or other users increasingly logging on from remote locations, the infrastructure must support capacity for notebooks, netbooks, tablet PCs, smartphones and other mobile devices. IT managers must also address the use of peripherals, including printers.

Device security should be closely examined and planned for. In some environments, critical security issues may require the use of stricter authentication methods, such as smart-card readers, biometric scanners and two-factor authentication tokens.

Basic issues of system requirements will generally be decided not by IT managers but by an agency's senior management, ideally with input from various departments. This would include issues such as which applications and data need the highest availability, what level of redundancy applies to specific data sets and where does the reliability of the network fall versus the cost.

Best Practices

Any transition from standard desktop PCs to client virtualization must be carefully thought out and planned to avoid ineffective choices and user resistance — and, most crucial, to optimize potential benefits. The most fundamental task is evaluating whether a migration makes sense for all or some of an agency's users.

By managing software and data from a central data center, client virtualization can reduce costs (technicians no longer have to update and maintain numerous individual PCs). It can also keep data secure on an organization's servers instead of on individual desktop or notebook systems that can be lost, stolen or illegally accessed.

But as with any technology, thin clients do not suit the work demands of all users. Client virtualization works best for users who access a limited number of standardized applications.

Although server software and thin client devices are improving rapidly, the technology may not work well for certain staff who need a larger variety of programs or intense computing power. The fit may not be ideal, as well, for legacy or graphics-heavy applications used within graphic design departments.

Once the extent (and type) of virtualization is decided, IT managers must assess existing infrastructure and then most likely plan an expansion. Systems engineers typically recommend developing as cohesive and holistic a strategy as possible to minimize system complexity and to capture maximum synergistic benefits.

Speed Up Turnaround

Government agencies are increasingly turning to server, storage, desktop and application virtualization to simplify management and increase security of IT systems.

A key benefit of such a move is greater agility, says Andi Mann, vice president of research for Enterprise Management Associates in Boulder, Colo. Improvements in the time it takes to start using new software can be dramatic, he says.

“Turnaround for new applications decreases from an average of up to 90 days to two to four hours, which gives government IT organizations a real boost in responding quickly to ever-changing requirements,” Mann says.

Because computing and storage will transfer from individual PCs to the data center, some government agencies may need to significantly increase capacity for their network bandwidth, servers and storage.

Plans must include sufficient redundancy to reliably ensure availability of applications, data and services in case of hardware breakdowns, as well as to provide for adequate disaster recovery and continuity of operations. The data center may also need additional power and cooling or a change in how the cooling is engineered.

IT departments can consider several techniques to safely reduce needed capacity, such as automatic storage tiering (moving older and less frequently used data from higher-cost, more-available storage devices to lower-cost, less-available ones), data deduplication and WAN optimization.

In conjunction with the numerous security gains of client virtualization, certain departments working with classified or sensitive data may want to take extra security precautions. One recommended measure is to reserve a separate server for virtual machines that handle sensitive data.

This separation reduces the potential damage caused by a jailbreak, whereby someone with access to one virtual machine manipulates the server hypervisor software (which controls desktop virtualization) to compromise other virtual machines on the same server.

While IT managers map out the client virtualization architecture, decisions about system requirements will likely be made by an organization's senior management, ideally with input from all departments and user groups. This would include reviewing related issues such as which core applications, for example, e-mail and mission-essential data, require high availability.

Government agencies should not undertake a fast and comprehensive migration. Rather, deploy slowly. Often a pilot deployment in a non-mission-critical area makes sense.

An incremental rollout provides an opportunity for the IT team to become acquainted with the new technology and to identify and address problems that arise. Although users should find little changed in their desktop experience after a switch to virtualization, IT staff will likely need some training to maintain new virtual systems.

Users may need some guidance on the new systems too. Ideally, they will have input into design as well. A key to successful change management is getting users to buy into the new system.

Systemic changes can be difficult from some users. A typical reason is that users are uncomfortable with the sense of having less control over their computing environment. Management will need to stress the advantages, such as the ability to access one's desktop and applications from any location.

Finally, government agencies should recognize that some users, or groups of users, may have job functions or learning needs that require more personalized or distinct desktop experiences, even if they are performing tasks similar to a larger group. IT departments should have some flexibility to customize the experience of those users.

At the same time, clear user and device policies may be needed to avoid improper customizations and to prevent the connection of incompatible peripherals or the installation of undesired applications.

With the right vision, investment strategy and deployment plan, client virtualization offers an infrastructure-altering way to truly do more with less.

Securing Virtual Environments

Federal IT managers, responding to an 1105 Government Information Group's 2009 Cybersecurity Survey, recommend four steps to improve security no matter the type of virtual environment:

- Deploy security monitoring tools to check communications among virtual machines on the same or different physical servers.
- Make access rules consistent across physical servers and guest operating systems.
- Establish policies to audit configuration and deployment of virtual systems and applications.
- Group together servers that require a similar level of security, so that high-security virtual servers are not on the same physical server as less secure ones.