

April 9, 2008

# Demystifying Client Virtualization

by Natalie Lambert

for IT Infrastructure & Operations Professionals



April 9, 2008

## Demystifying Client Virtualization

Desktop And Application Virtualization Increase Security And Streamline Ops

by **Natalie Lambert**

with Robert Whiteley and Rachel Batiacila

### EXECUTIVE SUMMARY

To virtualize or not to virtualize? That is no longer the question. The new question that desktop managers should ask is, “What desktop environment strikes the balance between productive users and IT’s need for increased manageability and security?” Emerging client virtualization technologies have the answer: Cost-effectively deliver a desktop tailored to each user scenario. This means that the traditional desktop model — inherently insecure, inflexible, and hard-to-manage — is a thing of the past. Organizations will instead identify their users by criteria like task-based, knowledge, or power users and will deliver dynamic desktops accordingly. After speaking to organizations looking at desktop and application virtualization, we know that client virtualization is not just an emerging trend, it’s the future of the corporate PC.

### TABLE OF CONTENTS

#### 2 **The Desktop Dilemma: New Mandates, Old Technologies, And Too Many Users**

Today’s Technologies Do Not Address Desktop Operations’ Top Five Headaches

Today’s Users Fall Into Three Basic Categories: Task-based, Knowledge, And Power

#### 5 **Client Virtualization Addresses Security, Management, And Flexibility Needs**

Desktop Virtualization: Delivering Desktops Independent Of Hardware Configuration

Application Virtualization: Delivering Applications Independent Of OS Configuration

Two Other Client Virtualization Technologies Will Further Simplify Desktop Management

#### 9 **The Dawn Of Scenario-Based Computing: New, Flexible Desktop Models**

#### 12 **Mainstream Enterprises Use Client Virtualization**

#### RECOMMENDATIONS

#### 13 **Don’t Succumb To The Hype: Build A Targeted Business Case**

#### 14 **Supplemental Material**

### NOTES & RESOURCES

Forrester spoke with more than 100 user companies and 15 vendors, including Citrix, Dell, HP, Microsoft, Sun Microsystems, Symantec, and VMware.

#### **Related Research Documents**

[“Virtualization On The Client . . . Finally!”](#)

November 21, 2007

[“The Virtualization Imperative”](#)

November 8, 2007

[“The Forrester Wave™: Client Management Suites, Q3 2007”](#)

July 24, 2007

[“Client Management 2.0”](#)

March 29, 2007

## THE DESKTOP DILEMMA: NEW MANDATES, OLD TECHNOLOGIES, AND TOO MANY USERS

As any desktop operations professional at a large organization will tell you, his job is getting harder by the day. Employees are more mobile; malicious code (spyware and Trojans) is more targeted; applications are larger and harder to deploy in a timely manner; patch management is a nightmare; and managing dozens of corporate PC images is all but impossible. And let's not even discuss upcoming Windows Vista migrations. Users will tell you that their machines are simply "too slow" and that IT is not responsive to their needs.

As a result, today's PC environment feels like a zero-sum game. As soon as IT fixes one problem, such as deploying a productivity application to a user, another pops up, such as a user needing a PC re-imaged due to a virus. IT operations and support costs are on the rise, and organizations are looking for a way to curtail their spending. However, today's desktop managers can't overcome the numerous challenges that exist when using the traditional PC environment.

### Today's Technologies Don't Address Desktop Operations' Top Five Headaches

IT managers are handcuffed by all of the processes they must follow as workers become more mobile and compliance requirements more difficult to enforce. Specifically, the desktop operations group is responsible for the productivity of its users while making sure that their PCs are locked down to the required spec. However, current client management and security tools tackle only part of their problem; for example, tools can assure that users have access to necessary applications but can't guarantee that machines are healthy enough to perform sufficiently.<sup>1</sup> From our conversations with clients, this adds up to five universal challenges:

- **Reining in the costs of PC management.** Managing the day-to-day operations associated with supporting a PC environment is no easy assignment. IT departments are working overtime to deploy additional applications to users on a one-off basis and at the same time making sure all machines and applications are patched in a timely manner. All of this hurts IT's bottom line while only keeping machines at a bare minimum of acceptable standards.
- **Securing devices and data regardless of location.** An OS will always require patching, but increasingly the challenge is securing the data. More than three-quarters of North American and European enterprises stated that protecting customer data and intellectual property are top business objectives in 2008.<sup>2</sup> To do this, however, they are forced to deploy multiple technologies, such as antimalware, host intrusion prevention, information leak prevention, and encryption in silos, making it difficult for IT to keep up with the latest threats.<sup>3</sup>
- **Remaining compliant with regulations and mandates.** In today's world, IT must be able to ensure that machines are compliant with the necessary regulatory and corporate requirements, such as the Office of Management and Budget (OMB) mandate to have all PCs configured with 300 specific settings.<sup>4</sup> Whether the requirement is around energy efficiency or data protection, organizations must have full control and visibility into their PCs and at the snap of the finger be able to prove to pesky auditors that they are compliant.

- **Supporting a changing workforce.** The number of typical nine-to-five office-bound workers decreases every year. In the wake of this, IT faces a two-fold challenge: 1) the increasing number of mobile and remote employees, and 2) a younger, more demanding generation of workers. And IT must still provide a consistent level of service to these users that now require anytime, anywhere access to data and applications.
- **Planning for disasters or workforce disruption.** Another top priority for today's enterprises is protecting the organization's information assets from the next 9/11, Hurricane Katrina, or even a simple laptop theft.<sup>5</sup> The traditional computing environment is not equipped to handle such disasters, however, so IT must find a way to ensure workforce continuity in the event of a disruption.

### Today's Users Fall Into Three Basic Categories: Task-Based, Knowledge, And Power

We know that today's workers have high expectations from IT. They demand that their PCs have sufficient computing power to accomplish their tasks in a timely manner. But not all users are created equal, and IT must balance users' expectations with the organization's security and manageability requirements. To better understand different user requirements, Forrester defines three buckets of employee types: task-based workers, knowledge workers, and power users. Each of these groups has its own set of challenges that IT must address:

- **Task-based workers: limited apps and limited performance requirements.** Task-based workers use a computer to perform a limited set of tasks. These workers typically run no more than five applications, which aren't particularly performance heavy. But what they lack in applications, these workers make up for in numbers. You'll find thousands of task-based workers as call center employees, receptionists, and bank tellers.

*What's it mean for desktop managers?* Task-based workers are the easiest user group for IT to manage. They use a very specific set of applications, need only limited customization, and can generally use a computer with limited performance. But these workers carry out many business-critical processes, like customer service in your call center, so outage time is unacceptable.

- **Knowledge workers: standard office apps and medium performance requirements.** Knowledge workers use their computers for almost all aspects of their job — and increasingly their personal lives. These workers can run upwards of 25 productivity applications, with more than five open and in use at one time. They require a fully functioning PC environment that will allow them to make changes to their PC settings as necessary. Examples of workers in this category are consultants, lawyers, accountants, and sales employees.

*What's it mean for desktop managers?* Knowledge workers are more difficult for IT to manage. System and application conflicts are common because these workers need to access multiple applications at a time. In addition, knowledge workers need control over their PCs to: 1) install additional software to complete specific work; 2) change configurations to fix a conflict; 3) personalize the machine for optimal efficiency; and 4) postpone systems scans to allow all available resources to be dedicated to the job at hand. Such requirements make managing these PCs difficult, which results in a high percentage of help desk requests and support calls.

- **Power users: compute-intensive apps and high performance requirements.** Power users not only require advanced PC features but also use more advanced tools and applications that require intimate knowledge of a given task. These users expect the highest level of performance and customization from their machines. Examples of workers in this category are engineers, developers, graphic designers, and financial traders.

*What's it mean for desktop managers?* Power users are the most difficult users for IT to manage. They pose the same challenges as knowledge workers: They access multiple applications simultaneously, and they need control over their PCs. However, power users also need the most high-performing machines. Their applications, like GCAD and Adobe Photoshop, are among the most intensive, which means they always need the latest and greatest hardware to meet the demands of their applications.

This taxonomy is a helpful way of thinking about the various high-level user categories in your environment. And although all computing employees fit into one of these user groups, there are secondary attributes that you'll want to consider as well. These attributes define yet another set of challenges that desktop managers must address. The companies we interviewed took additional steps to classify users as:

- **Mobile.** These users are away from their desks more than 30% of the time and use laptops or mobile devices to complete their work. They typically have limited or no Internet connectivity, making it difficult for IT to manage and update these machines; for example, it's difficult for IT to complete a software update or a machine backup that takes more than an hour.
- **Remote.** These employees generally work at home or in a branch office and use either laptops or desktop computers to complete their work. They typically have persistent Internet connection; however, connection speed and quality are not guaranteed.
- **Third-party.** Also known as "untrusted" or "unmanaged" users, third-party workers often use their own PCs. These machines are not provisioned by the hiring organization and can't be controlled by IT without undertaking considerable liability.

## CLIENT VIRTUALIZATION ADDRESSES SECURITY, MANAGEMENT, AND FLEXIBILITY NEEDS

IT has overcome the challenges of today's diverse set of users and machines with predominantly manual workarounds, which is both costly and nonscalable. Over the past few years, many IT organizations have succumbed to the fact that they will always be in a reactive state. However, an emerging set of technologies — which Forrester collectively refers to as client virtualization — shows promise for getting desktop managers out of this reactive rut.

Client virtualization encompasses four different technologies: 1) local desktop virtualization; 2) hosted desktop virtualization; 3) local application virtualization; and 4) hosted application virtualization. Each addresses a subset of IT's most complex desktop challenges, but together they streamline the corporate computing environment and eliminate the issues that keep IT staffers up at night.

### Desktop Virtualization: Delivering Desktops Independent Of Hardware Configuration

A virtual desktop is the idea that the traditional desktop environment is not installed on or coupled to the device the user is interacting with. More generally, desktop virtualization is defined as:

*A computing environment, consisting of an operating system, applications, and associated data, that is abstracted from the user's PC.<sup>6</sup>*

Desktop virtualization comes in two flavors (see Figure 1):

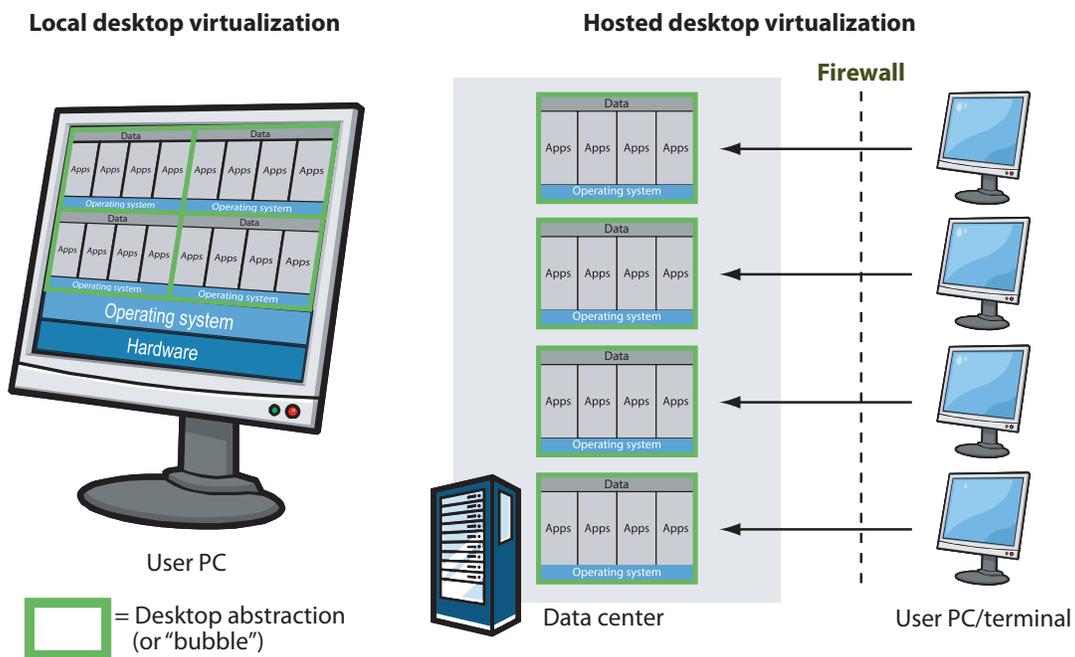
- **Local desktop virtualization.** For local desktop virtualization, the entire desktop environment executes in a protected environment on the user's PC. This "bubble" runs on top of the underlying hardware and host operating system platform. Virtual machines run like any other application directly on top of an installed OS but are still independent from any software that has been deployed. Vendors in this market include Microsoft, MokaFive, Parallels, and VMware.

*Benefits to desktop managers:* Local desktop virtualization enables desktop managers to provision virtual desktops as large files rather than as individual, physical PCs. Imagine being able to simply give a user a file that contains the entire corporate computing environment yet can run from any machine.<sup>7</sup> This desktop is fully managed and secured by the same policies that govern physical PCs. Because a virtual desktop has all the attributes of a file — albeit a very large file — it can be encrypted and backed up, helping streamline regulatory compliance and business continuity initiatives.

- **Hosted desktop virtualization.** Hosted desktop virtualization is where the desktop environment executes in a protected environment on data center servers.<sup>8</sup> The virtual machine bubble runs directly on a data center server alongside other VM instances, allowing multiple users to remotely connect to their desktops simultaneously. Vendors in this market include Citrix, Deskton, Microsoft, and VMware, as well as solutions providers HP and Sun Microsystems.<sup>9</sup>

*Benefits to desktop managers:* Hosted desktop virtualization brings the desktop environment into the secure data center, where data and applications aren't as susceptible to theft or loss as they would be on traditional PCs. These desktops are always on and users can access their environment from anywhere. Similarly, IT can access these machines across high-speed data center links for better maintenance, support, and patching. Hosted desktop virtualization also has native business continuity and disaster recovery capabilities; virtual machines can be easily backed up and transferred to alternative servers or data centers in the case of an outage. Finally, PC refresh cycles can be extended thanks to application processing occurring on the server.

**Figure 1** Local And Hosted Desktop Virtualization Abstract The OS, Applications, And Data



41495

Source: Forrester Research, Inc.

## Application Virtualization: Delivering Applications Independent Of OS Configuration

A virtual application runs in isolation in its own contained environment. A virtual app is not installed in the traditional sense, even though a user will interact with the application as if it is. More generally, application virtualization is defined as:

*An application that is abstracted from the user's OS and runs in isolation from other applications.*

Like desktop virtualization, application virtualization has two forms (see Figure 2):

- **Local application virtualization.** Local application virtualization is the next generation of application packaging. Applications are packaged as self-contained executables that run independent of any other application on the machine. They run in an isolated bubble on the user's OS, unable to interact with other applications without explicit permission.<sup>10</sup> Vendors in this market include Citrix, Microsoft (with acquisition of Softricity), Symantec (with acquisition of Altiris), and VMware (with acquisition of Thinstall).

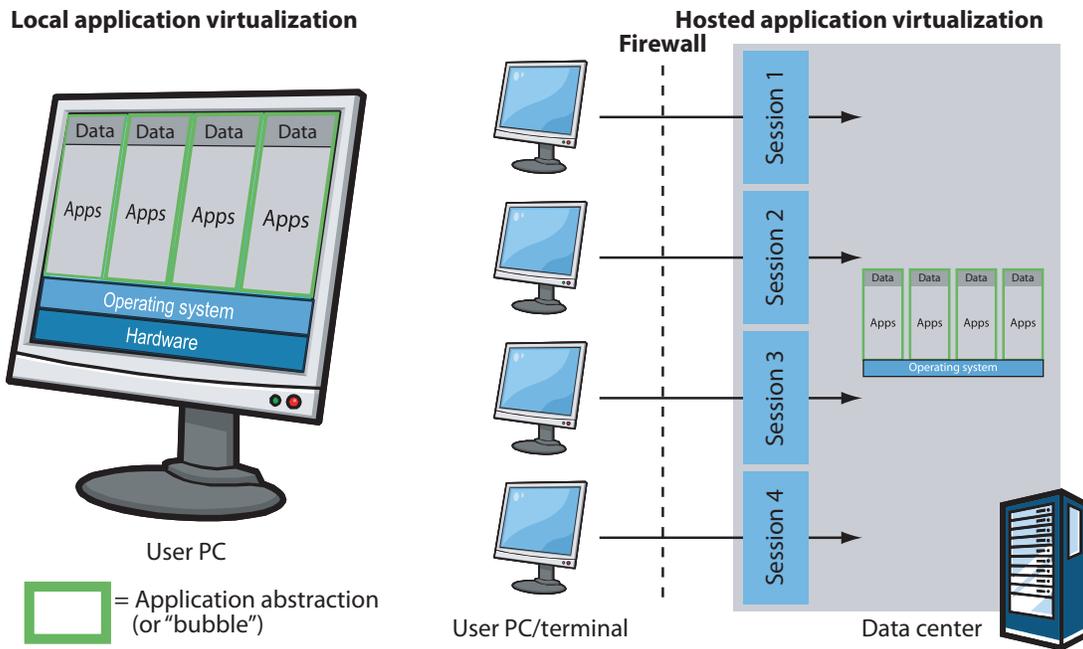
*Benefits to desktop managers:* Local application virtualization is the future of software deployment. Within the next five years every single application on a PC will run virtually. Why? Because it solves many of today's problems that would otherwise not get solved, like the much-needed ability to run both Microsoft Excel 2003 and Excel 2007 on the same machine. When applications are isolated and packaged in a bubble, there are two immediate benefits: 1) They can't see other applications on the machine, which eliminates conflicts, and 2) they decrease management and support costs by allowing IT to reset an application back to a good state. Finally, local application virtualization can be used in conjunction with other types of client virtualization: It's not uncommon to see enterprises running virtual apps inside of virtual desktops.

- **Hosted application virtualization.** Hosted application virtualization is a new spin on an old theme: server-based computing. Applications are run in bubbles hosted on data center servers, and users access these applications over the network.<sup>11</sup> This is transparent from the user's perspective; the application appears to be running on her machine via a set of shortcuts on her desktop. Vendors in this market include Citrix, Microsoft, and Sun Microsystems.

*Benefits to desktop managers:* Hosted application virtualization has the same centralization and consolidation benefits as hosted desktop virtualization. Both types of virtualization keep applications and data centralized on data center servers, but that's where the similarities end. In hosted app virtualization, only selected applications are centralized, and there is still the threat of users storing sensitive data associated with the remaining applications on a PC. However, for the apps that are hosted, it provides secure remote access and data security, and it decreases support costs for applications.

Although we describe these four types of client virtualization separately, enterprises are deploying them in tandem to get combined benefits (see Figure 3).

**Figure 2** Local And Hosted Application Virtualization Abstract The Applications From The OS



41495

Source: Forrester Research, Inc.

**Figure 3** How Client Virtualization Addresses The Headaches Of Desktop Managers

Strength in addressing desktop operation headaches:

● Very strong ◐ ◑ ◒ ◓ ◔ ◕ ◖ ◗ ◘ ◙ ◚ ◛ ◜ ◝ ◞ ◟ ◠ ◡ ◢ ◣ ◤ ◥ ◦ Does not address

Client virtualization	Management	Security	Compliance	Changing workforce	Business continuity	Ideal for:
Hosted application virtualization	◐	◑	◒	●	◐	Problem and legacy applications
Hosted desktop virtualization	●	●	●	◐	●	Data security
Local application virtualization	◐	◑	◒	◓	◔	Application conflicts
Local desktop virtualization	◐	◑	◒	◓	◔	Unmanaged workers

41495

Source: Forrester Research, Inc.

## Two Other Client Virtualization Technologies Will Further Simplify Desktop Management

There are two more client virtualization technologies that help address persistent desktop woes: OS streaming and workspace virtualization. These technologies have many of the same attributes as the desktop virtualization; however, there are subtle differences worth mentioning:

- **OS streaming.** OS streaming is a delivery mechanism that enables IT to deliver, or stream, a virtual desktop environment to a server, PC, or thin client over the network. Using this model, IT can provide users with PC environments on demand. Vendors in this market include Akamai Technologies, Citrix, and solutions provider Dell.<sup>12</sup>
- **Workspace virtualization.** Workspace virtualization is the newest option to arrive on the client virtualization scene. It's similar to local desktop virtualization in that both technologies bundle the applications and data into a virtual bubble, but workspace virtualization only bundles the OS settings, not the full OS, and therefore reconfigures whatever is installed on the PC. The most prominent vendor in this market is RingCube Technologies.

There is no one silver bullet for virtualization technology. When investigating the various flavors of client virtualization, it's important to look at the current challenges in your environment that map to the benefits each technology brings to the table. Combining technologies ensures that you will address all of your concerns in aggregate.

## THE DAWN OF SCENARIO-BASED COMPUTING: NEW, FLEXIBLE DESKTOP MODELS

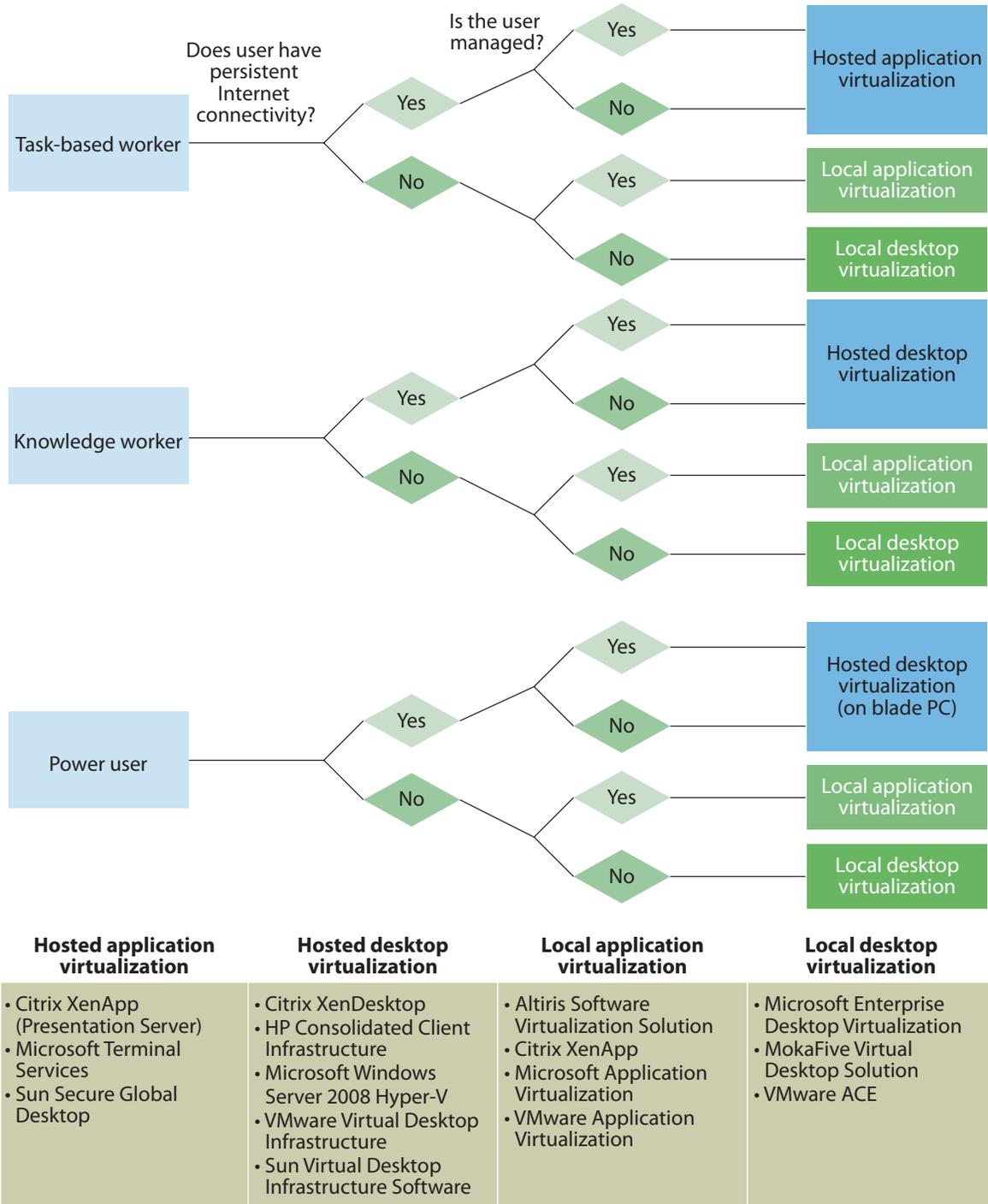
For desktop managers, the debate is no longer simply a thick- or thin-client device. With the dawn of client virtualization, the hardware and software are decoupled. As a result, IT can dynamically create multiple desktop scenarios by pairing the right virtualization technologies with the computing needs appropriate to each user. To get started, put your users into their respective worker group (task, knowledge, and power) and answer the following questions:

1. **Does this user have a persistent, fast network connection at all times?** This question determines if a hosted model will work for these users. Networks connect the remote user to the desktops and applications stored centrally in a data center. Many connections, such as local area networks (LANs) and fixed Internet links like DSL, are sufficient for virtualization. However, a 2.5G mobile connection, for example, doesn't provide the reliability and throughput to keep a worker productively connected to his desktop at all times.
2. **Does IT have control over his physical device?** Determining if the user accessing your environment is a managed worker helps establish: 1) how much control, if any, you have over his device, and 2) the level of risk he poses. For example, local application virtualization doesn't make sense for an unmanaged worker, as IT has no control over his machine to push updates or fix applications. Instead, hosted application virtualization allows IT to provide application access while keeping control over corporate data.

These questions help map your user base to the most appropriate virtualization technology (see Figure 4). While there is no secret formula to determining the right set of technologies for each user, here are four recommended scenarios that illuminate how client virtualization can be used today:

- **A home-sourced call center agent: tasked-based worker with Internet and managed by IT.** Home-sourcing is a popular way to tap into a population of well-educated adults who typically can't commute or who require flexible working hours. In this scenario, the best solution is a hosted application virtualization technology where the employee can use low-cost DSL for reliable access to a handful of centralized contact center applications and associated data.
- **A contracted accountant: knowledge worker without network and not managed by IT.** Contracted accountants are mobile and have multiple clients that they visit regularly. They use the machine provisioned by their accounting firm yet need temporary access to sensitive applications and financial data at the organizations that hired them. For companies that use contractors, this scenario is ideal for the combination of local desktop virtualization, which turns the accountant into a managed worker, and local app virtualization for easy provisioning of critical applications.
- **An outsourced application developer: power user with Internet and not managed by IT.** Outsourcing IT services, like application development, is a key cost-cutting measure for many enterprises. However, enterprises struggle with outsourcing these functions for fear of lost or exploited intellectual property. We recommend hosted desktop virtualization to ensure that each developer has his own dedicated desktop environment — or even blade PC — while also securing the intellectual property on premise.
- **Employees migrating to Windows Vista: any user with any network and managed by IT.** Not all scenarios need to be narrowly defined. Take, for example, the impending move to Windows Vista that will eventually impact all users. Most companies will find Vista creeping in on new laptop PCs, but they will immediately remove it for fear that dozens of custom applications will be incompatible. Instead, we recommend local desktop virtualization where Windows XP and any thorny apps are run as a virtual machine on top of the new Windows Vista PC.

**Figure 4** Scenario-Based Computing: Finding The Right Virtualization Model For Your Users



41495

Source: Forrester Research, Inc.

## MAINSTREAM ENTERPRISES USE CLIENT VIRTUALIZATION

Client virtualization may be an emerging set of technologies, but it's still ready for the enterprise. We've spoken with dozens of companies that are deploying client virtualization in production environments. Typically the business case started with data security, but increasingly companies are mentioning operational efficiency and savings as the key benefit. Here are four examples of enterprises that were able to streamline IT operations:

- **A large financial institution cut application packaging and delivery time in half.** When it comes to trading environments, any delays for the users, such as system downtime and application incompatibilities, can cost millions of dollars. Consequently, a global financial institution found that its application packaging process, which was costly and time-consuming, was an ideal candidate for streamlining. This firm used local application virtualization, specifically Altiris Software Virtualization Solution, and cut in half its time to package and deliver applications to users. In addition, it cited that both application testing times and support costs dropped dramatically because applications can simply be reset when they break.
- **A utilities company gained 10% productivity from its virtual machine users.** A North American power utility, constrained by multiple security regulations, needed to maintain separate networks to run its grid. These private networks held critical data and applications that the majority of the user base didn't have clearance to use. To make matters worse, the company maintained entirely separate images — including different OSes, client security tools, policies, and applications — for the machines accessing the restricted zones. Before turning to virtualization, “highly classified” users kept two or more PCs on their office desk, each managed by a different IT department. Using VMware ACE, a local desktop virtualization solution, this organization virtualized the “classified” desktop environment and placed it as a VM (or multiple VMs) on each user's corporate machine. Now a single machine can act as both a corporate machine and a secure machine, which the company cited as providing a 10% productivity gain.
- **A medical institution decreased power consumption and support costs with hosted desktops.** A midsize hospital — with 5,300 employees and hundreds of doctors' offices and hospitals — was growing fast in a highly regulated industry. The IT department was tasked with finding a way to streamline management of the PC environment while increasing compliance with corporate and regulatory requirements. In essence, it needed much tighter controls over its data. VMware's Virtual Desktop Infrastructure (VDI) did the trick. It lowered support costs by removing the need to send technicians on-site for tech support. In addition, the introduction of thin-client devices led to a 72% decrease in power consumption and overall reduced desktop provisioning time. However, the most important benefit was that its HIPAA-governed data was now maintained on virtual desktops on highly secured data center servers.
- **A government agency secured its data and migrated to Windows Vista in one easy step.** In situations of national defense, data security is of utmost importance. Take for example an

Australian government agency tasked with managing 4,800 users and 5,800 devices, all across 93 different locations. Its goal? To find a solution that allowed users to access data and apps from anywhere yet guaranteed the safe housing of national security data in the event a device was lost or stolen. This agency turned to hosted application virtualization, using Citrix XenApp (formerly Presentation Server) to connect users to centrally hosted servers. This way, national security data never left the four walls of the data center. Furthermore, managers quickly recognized that removing applications from the desktop accelerated their Windows Vista migration because they no longer worried about application incompatibilities.

## RECOMMENDATIONS

### DON'T SUCCUMB TO THE HYPE: BUILD A TARGETED BUSINESS CASE

There is no one-size-fits-all client virtualization technology — nor is every user a fit for virtualization. Desktop environments are almost always unique, so more than with other technologies, your mileage will vary. Make sure you build a tailored business case that prioritizes your organization's scenarios. Forrester recommends that you take this three-step approach:

- **Step 1: Build a business case around security and manageability, not cost savings.** As with any new technology, you must build a business case. Refrain from building this business case around the cost savings that your preferred vendor is hyping. Focus your argument on data and endpoint security, improved desktop manageability, and flexible remote access. Our clients that cite cost savings are having a hard time proving it to management because of the additional server hardware, storage, and bandwidth needed. Those that focus on hard IT support costs combined with softer benefits are proving value from day one.
- **Step 2: Define your scenarios and classify your users.** Many of you have already gone through this exercise as part of your traditional PC management process. For the rest, use a two-step classification method: 1) Based on performance needs, put users in task-based, knowledge, and power user groups, and 2) further segment your users based on whether they are mobile, remote, or third party.<sup>13</sup> The remaining users who can't find a home in this classification should remain on a traditional PC — for now.
- **Step 3: Pick a problem scenario to start with — build out from there.** Take a look at your user population. Are there groups that have specific needs — such as access to highly confidential customer data or the ability to use a nonmanaged device — which the traditional PC model doesn't accommodate well? These are great starting points for a client virtualization pilot. Use the success of the pilot to build your case for new user groups and technologies. This will eventually lead to a wide-scale deployment that delivers customized environments that meet the needs of your different users — however, this can take upwards of five years to complete.

## SUPPLEMENTAL MATERIAL

### Companies Interviewed For This Document

Citrix	RingCube
Dell	Sun Microsystems
DeskTone	Symantec
HP	VMware
Microsoft	

## ENDNOTES

- <sup>1</sup> Client and network securities are evolving. Why? Because today's technologies do not support the requirements that businesses face, such as providing secure access to corporate resources independent of user location. So, how can security and IT operations heads protect their firms? Look for emerging software tools — which we call proactive endpoint risk management (PERM). See the March 29, 2007, "[Client Management 2.0](#)" report.
- <sup>2</sup> The top three business objective to IT security decision-makers are protecting customer data, developing business continuity and disaster recovery plans, and protecting intellectual property. Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2007.
- <sup>3</sup> Thirty-nine percent of North American and European enterprises told us that they have already adopted host intrusion prevention technologies, 27% adopted full disk encryption, and 24% adopted information leak prevention. Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2007.
- <sup>4</sup> The Office of Management and Budget requires that all federal agencies standardize the configuration of approximately 300 settings on each of their Windows XP and Vista machines to improve IT security. Source: The White House (<http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf>).
- <sup>5</sup> Seventy-eight percent of North American and European enterprises told us that business continuity and disaster recovery plans are top issues for 2008. See the February 27, 2008, "[The State Of Enterprise IT Security Adoption: 2007](#)" report.
- <sup>6</sup> Here, PC refers to the device which the user is interfacing with. This can be a traditional desktop or laptop, thin client, diskless PC, or mobile device.
- <sup>7</sup> According to VMware's product specifications, local desktop virtualization requires a 500MHz or faster processor with recommended 256MB of memory. Our own experience shows that PCs must be faster and have more RAM to work efficiently.
- <sup>8</sup> Regardless of which hosted desktop virtualization solution you choose, a Microsoft Vista Enterprise Centralized Desktop license is required. This is the Microsoft license that allows users to deliver an OS over the network.

- <sup>9</sup> HP and Sun Microsystems offer customers full hosted desktop virtualization solutions — hardware and software — based on VMware technology. Both vendors OEM VMware software and sell it to customers as an end-to-end solution.
- <sup>10</sup> We continue to use the bubble metaphor, although the distinction is subtle. In desktop virtualization, the bubble refers to a fully wrapped desktop environment (OS, applications, and data) that runs in isolation; for application virtualization, only the app and a minimum number of associated components like DLLs are wrapped and run in isolation.
- <sup>11</sup> Using hosted application virtualization technology, organizations can also deliver fully locked-down desktops to users.
- <sup>12</sup> Dell partners with Citrix to offer customers a full end-to-end OS streaming solution.
- <sup>13</sup> Although creating user scenarios around performance needs and mobility will help determine the primary virtualization technology that should be used, there are exceptions. Organizations that handle very sensitive information may forgo all user classification and create a desktop environment based on the need to centralize data. These organizations should use either hosted desktop or application virtualization to assure that data doesn't live out on machines.



# FORRESTER®

Making Leaders Successful Every Day

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617.613.6000  
Fax: +1 617.613.5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations, visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or [resourcecenter@forrester.com](mailto:resourcecenter@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit [www.forrester.com](http://www.forrester.com).