A Smart Guide published by

FREEFORM DYNAMICS

Desktop Virtualization

Aligning options with user and business requirements

Microsoft®

With Compliments

Technology needs context

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

An innovative research methodology allows us to gather feedback directly from those involved in IT strategy, planning, procurement and implementation.

Our output is grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics research service, visit our website or contact us at **info@freeformdynamics.com**

freeformdynamics.com

Desktop Virtualization

Aligning options with user and business requirements

Contents

Introduction

Welcome to the Freeform Dynamics Smart Guide to Desktop Virtualization. Our aim is to bring you up to speed on the most important principles, technologies and techniques in this highly important area. Along the way, we'll also provide you with some guidance on where desktop virtualization might fit into your organization, and how to prepare for a successful implementation.

Who is this book for?

This book is intended as a general primer for anyone interested in the topic, but will be particularly useful for:

- IT managers responsible for end user computing strategy.
- IT professionals charged with operating and supporting the organization's desktop computing environment.
- Anyone involved in a desktop modernization initiative.
- Business managers interested in how IT can be better used to support new ways of working.

Why is this topic important?

Desktop virtualization can be used to create a more robust, flexible, secure and easier-to-operate desktop computing environment. This is significant for a number of reasons.

Devices that present users with a personal electronic desktop or workspace are integral to IT service delivery. Whether it's a desktop

PC, laptop, ultrabook, tablet or other type of device such as a 'thin client' terminal, the 'desktop client' represents the primary point of access for users into business systems and information. How well it performs and the experience it delivers has a big impact on user productivity, as well as significantly influencing business user perception of how well IT is being managed.

Modernizing the desktop computing environment can, therefore, be a good way of enhancing business performance and user satisfaction. Conversely, allowing your infrastructure to drift out of date leads to escalating cost and risk as older desktop hardware and software are more expensive to maintain, more prone to failure, more hassle to support and more difficult to secure.

Beyond these general considerations, the traditional ways in which desktops have been implemented and managed are being challenged by broader trends and developments that are changing needs and expectations. Increasingly pervasive connectivity and a growing richness of device choice/capability is enabling ever more flexible working, e.g. from home, hot-desks, conference rooms, hotels, airports, client sites, and so on.

Put this together with a trend towards users employing multiple devices for work purposes, including personally owned equipment (the 'consumerization' phenomenon), and the result is a need for a rethink of how end user computing is enabled and managed from an IT perspective. In particular, the model in which all software is installed and managed locally on each physical desktop or device is looking increasingly less likely to cope with future needs.

An alternative approach

While the traditional desktop computing model is still relevant for dealing with certain scenarios and requirements, desktop virtualization provides a number of additional options for handling emerging needs more effectively and efficiently.

The overall aims of desktop virtualization include:

- Providing users with the flexibility to work almost anywhere, but in a consistent and well-coordinated manner. Key to this is effective access to their applications and data regardless of device and form factor (desktop, laptop, ultrabook, tablet, etc.), with their personal 'preferences' as well as preferred 'look and feel' preserved wherever possible across devices.
- Enhancing business continuity by minimizing the impact of malfunctioning PCs, power outages, natural disasters and other disruptive events. Key to this is reducing the user's dependency on a specific work location and/or specific devices to perform their duties effectively.
- Ensuring that business requirements around security and compliance (where relevant) are met. Key here is the centralization of management, application execution and/or data storage in a way that enhances visibility and control, but without undermining the user experience or unduly constraining user flexibility.
- Reducing the overhead on IT staff and enhancing their ability to maximize the quality of service to users. Important keys here are

the simplification of application development, deployment and maintenance, and the efficiency gains that stem from a more centralized and streamlined management approach.

If you are skeptical about whether a single solution can deliver against all this, don't worry. The reality is that desktop virtualization is actually based on a family of techniques and approaches, with a simple 'model' underpinning each that's relatively easy to understand. We'll be covering these models shortly, and discussing how they are combined to meet the needs of different types of user, but before getting into this, let's review some important foundation principles.

What is desktop virtualization?

Many readers will be aware of virtualization in the context of x86 servers, where it has been used as the basis for consolidating server estates, streamlining operations and increasing flexibility. An enabling component is the 'hypervisor', which allows multiple 'virtual machines' (VMs) to run on a single physical computer, breaking the traditional tight coupling between software and hardware. This basic idea of 'uncoupling' previously dependent components can also be applied to desktop computing, but here it is extended to provide even greater flexibility.

In the traditional desktop model, the desktop computer runs an operating system upon which applications are executed, with their user interface displayed on the computer screen. By introducing virtualization into this mix, we break the bindings between physical hardware, operating systems, applications and displays, meaning

that some or all of the software components can be run or managed from a remote server instead of locally (Figure 1):

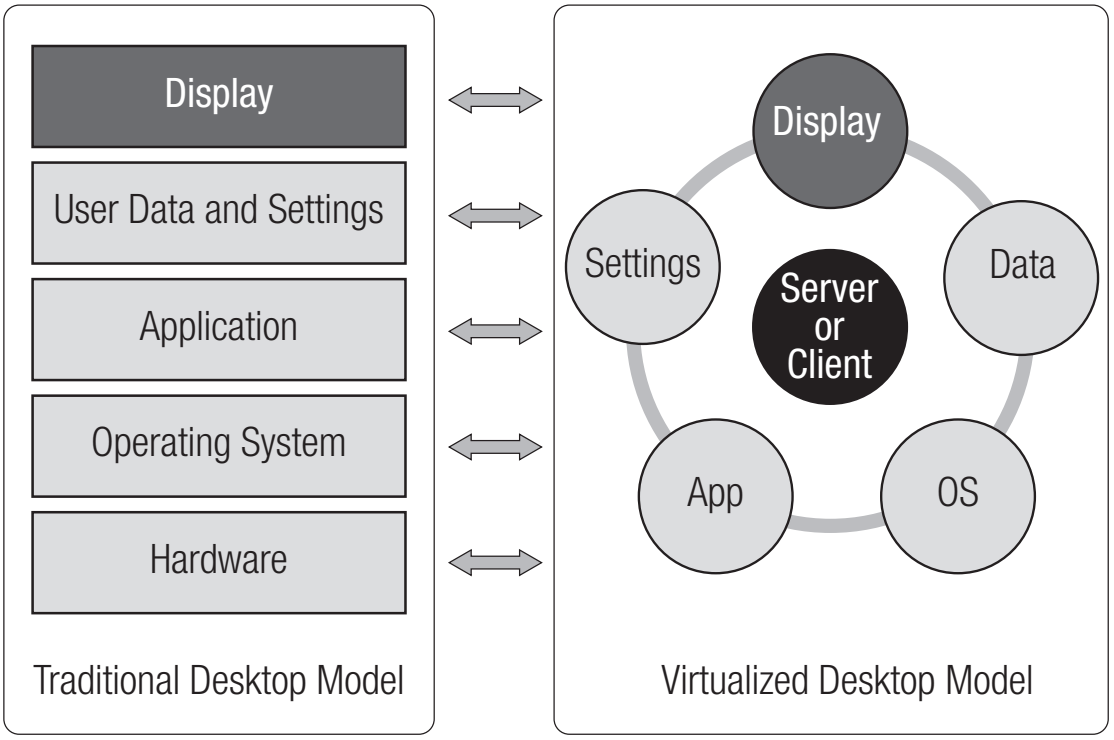

Figure 1: Breaking the traditional bindings between layers.

As shown in this graphic, in addition to having a choice about where the operating system and individual applications reside, we can also choose whether user information such as application data and configuration settings are stored locally or on the server.

The latest generation of desktop virtualization solutions allows all of these options (and more) to be freely mixed and matched, according to what's going on at any particular moment in time. The way the operating system and applications are served up to a user may be different, for example, depending on whether they are logging in from their desk PC over the corporate network, from their laptop over a hotel WiFi service, or from their home PC over a domestic broadband connection.

Fortunately, it's not necessary to work through all these options from first principles as a number of 'deployment models' have emerged to cater for frequently occurring requirements and objectives. These are relatively easy to understand, and the best way of appreciating what fits where is to consider each of the three important layers in turn – the desktop operating system (OS), the applications that run on it, and the settings and data accessed by those applications.

OS deployment models

One of the challenges with getting up to speed on desktop virtualization is working through the jargon, which is often used imprecisely or inconsistently. This is particularly problematic when exploring OS deployment models. Experts and IT vendors, for example, sometimes use the term 'virtual machine' (VM) to describe an executable image sitting on disk, but they often also use it when talking about a live 'instance' of the OS running in machine memory. There is then the question of what's included in a particular person's notion of a virtual machine – does it contain just the OS, the OS plus other platform software, or all of the platform layer plus the applications? You often don't know.

For this reason, we are going to introduce a couple of more precise working terms for the purposes of our discussion in this Smart Guide - 'OS image' and 'OS instance'. The first refers to the software on disk, from which a desktop operating system is booted, and the second refers to an actively running desktop, i.e. the collection of processes executing in machine memory at runtime. These two terms may not be in general use, but it is important to

distinguish between the concepts they reflect when considering what's behind another piece of commonly used jargon, 'VDI'.

Virtual Desktop Infrastructure (VDI)

The term 'Virtual Desktop Infrastructure' (VDI), is generally used to describe infrastructure which allows the desktop OS to run on the server. In reality, however, it encompasses three different models:

- Session-based VDI.
- VM-based VDI (shared image).
- VM-based VDI (personal image).

Let's walk through these one at a time.

Session-based VDI

This model has its roots in the 'terminal services' architecture that gained popularity in the 90s. Multiple users log onto a single 'multi-user' instance of the operating system executing on the server.

Pretty much all server resources are shared between users dynamically, but a 'session' is created for each user to keep their activity separate from everyone else's (very similar to traditional multi-user operating systems such as Unix).

The client can be 'thin' because it only needs to handle the display and the input; indeed 'zero clients' can contain just a network port and graphics card. However, session-based VDI can also be implemented using software-based thin clients, which, being relatively undemanding, can run on low spec equipment (an approach often used to extend the life of old PCs).

VM-based VDI (shared image)

Desktops are again executed on the server side of the network, but rather than multiple users sharing the same operating system instance (as they do in the session-based model), each one has their own dedicated OS instance, which we might refer to in this context as a discrete virtual machine or VM. Resources such as memory and CPU are dedicated to the VM while it is running (which has performance benefits), though most modern systems allow on-demand memory allocation so VMs only take control of what they actually need when they need it.

In this shared image model, users with the same or similar OS-related requirements are grouped into 'pools', and all of their desktops are booted from the same OS image, sometimes referred to as a 'golden image'. Where requirements vary significantly between groups, a separate golden image is created for each.

VM-based VDI (personal image)

From a runtime execution perspective, this model is identical to the one we have just been discussing, i.e. each user has a discrete OS instance running on the server with dedicated resources.

The difference, however, is that every user's desktop is booted from a separate OS image. This provides more user flexibility as each desktop can be uniquely set up and even tailored by the user (subject to policy). However, with each user's image being stored separately on disk, a lot more storage is required to implement this model, and management overhead is likely to be higher.

Niche OS deployment models

In addition to VDI, there are two other OS deployment models you may come across, though both of these are targeted at niche areas rather than commonly occurring mainstream scenarios.

Desktop on a blade

It is possible to implement a VDI-like model using dedicated hardware, with each user's OS instance running on a separate dedicated 'server blade' with its own CPU and memory. As shared resource VDI solutions have become more efficient, flexible and performant, however, the relatively expensive 'desktop on a blade' alternative has become associated with a small number of very exceptional scenarios, so we won't be discussing it further.

Client-hosted virtual machine

In this model multiple VMs are run on a single physical desktop (rather than on the server). It is mostly used by IT professionals to create multiple OS installations so that different development, testing and troubleshooting activities can be carried out on the same machine. This has obvious productivity benefits as well as maximizing return on investment in high spec equipment. The model is often also employed by Apple Mac users to run Windows as a guest OS in order to access corporate applications.

Application deployment models

Applications may, of course, be installed onto physical or virtual desktops in the traditional manner, but desktop virtualization solutions provide a couple of alternatives. Let's explore the options.

Direct installation of applications

Applications can be installed in the familiar way following OS deployment, or pre-installed as part of a standard OS image to form a foundation for a pool of users with similar core requirements.

Direct installation in either a session-based environment or in the pooled user VDI model will, by definition, make an application available to any user in the relevant pool served by a particular image, so this is something that would normally be controlled by IT.

Where personal desktop (image per user) based VDI is used, or desktops are running as client-hosted VMs, different mixes of applications may be installed on each individual desktop by either IT or the user (depending on permissions).

As with traditional desktops, applications get woven into the local operating environment when they are directly installed, sharing things like runtime libraries, the registry, and other local resources. The usual caveats therefore apply regarding application conflicts.

Alternatives to direct installation

Virtual application streaming

In the virtual application streaming model, individual applications are bundled up with the resources and settings they need to operate (library modules, specific registry entries, and so on), then deployed (even 'streamed' on demand) from a central server in the form of a self-contained package to the target desktop (which may be physical or based on any kind of virtual OS deployment model).

From there they execute as if they were directly installed, but in their own 'protected' environment. Application requests to the

operating system for settings or resources are intercepted and fulfilled using the contents of the package if possible, and only passed to the OS if nothing relevant is found. This avoids the conflict and compatibility issues associated with direct installation.

To the user, virtual applications look no different to directly installed software. They can still make use of local data and interoperate with both each other and traditionally installed applications through 'cut and paste', dynamic links, etc.

In terms of deployment, virtual application availability is normally tied to the user rather than a specific device or virtual desktop. This means users can invoke a virtual application from any compatible device or virtual OS environment. If it has not previously been used on that desktop, it will be streamed (downloaded) from the source server, and subsequently updated when the user connects to the network, keeping everything current.

Remote application execution

As the name suggests, in this model the application executes on a remote server, which may be different from the one running the virtual OS. In essence, the application may appear to be running on the target desktop (which again may be physical or virtual), but in reality it is not; it's just presenting the user interface and interaction part of the application.

Nevertheless, in the latest generation of desktop virtualization solutions, remote applications look to the user as if they were natively installed, so they can run alongside and interact with both software that has been directly installed, and virtual applications that have been streamed as described above. Remote applications

can also make use of all of the resources available to the desktop, including printers, storage, network drives and so on.

Summary of app deployment models

The two things that matter the most are where the application executes and where it looks for the specific settings and other resources (e.g. shared libraries) that it needs (Table 1):

Model	Executes on	Settings/resources
Direct installation	User's physical or virtual desktop	User's physical or virtual desktop
Virtual applications	User's physical or virtual desktop	Within application deployment package
Remote applications	Independent server, separate to desktop	Remote server environment

Table 1: Application deployment models.

As a reminder, any or all of these application models can be used in conjunction with any type of physical or virtual desktop, and can even be combined with each other to meet particular needs.

Combining application models

To illustrate how the different application deployment models work together, it is possible, for example, to have a word processor directly installed onto the desktop, an image processing tool streamed as a virtual application, and a business intelligence (BI)

tool running remotely. Each of these would be launched in the same way by the user, e.g. from the OS menu or desktop icons.

The user may then generate a chart in the BI tool, copy it to the clipboard, then task-switch to the image processing tool, where it is pasted for enhancement. Once the user is happy with the chart, they copy it to the clipboard again, switch to the word processor, and paste it into their monthly report. Three different application deployment models all working together seamlessly, regardless of whether the user's desktop is physical, session-based or VDI -based.

User settings and data

Personalization is an important part of desktop computing, but with the advent of virtual desktops and the use of multiple devices by a single user becoming more popular, traditional approaches to managing user settings and data are often no longer adequate. The user virtualization model has therefore emerged to fill the gap.

User virtualization

This model is concerned with providing users with a consistent experience across devices. Rather than user settings (e.g. OS and application preferences) being stored in the user's desktop environment, they are held on a server and pulled down over the network when required.

In practice, user OS and application preferences along with other settings can be synchronized between any of the user's desktops and the server. Such synchronization occurs at log

on time, when an application is launched or closed, and/or when significant changes or events occur (e.g. reconfiguration, application installation, etc.). Changes are then propagated to all other compatible desktops accessed by the user, which is how the consistent experience is maintained.

User virtualization can work across any mix of desktops that support the facility, whether they are physical, virtual or even temporary (e.g. a hot-desk device). Furthermore, preferences and settings captured and synchronized through this model can be used to manage the configuration of natively installed software, streamed virtual applications, or remote applications, providing a personalization management overlay across the whole physical and virtual desktop landscape.

Data virtualization

Keeping track of where user data is stored can be hard in a virtual multi-device environment. An answer is to make the 'Documents' folder and other work areas virtual too. When the user accesses one of the virtual locations, which may appear to represent local storage, their action is redirected behind the scenes to where the data really resides, e.g. a folder somewhere on the network.

Synchronization is used when a mobile user needs to access their data while they are disconnected from the corporate network. Data from the main folder (e.g. on the network) is locally cached, then any changes made to either the master location or local store are synchronized when the device is next online.

Models versus solutions

The above models have been described in a 'logical' sense, i.e. we have focused on the functionality of each rather than the enabling technology. When you start to look at specific offerings you will quickly discover that any given model will translate to a whole dedicated solution for one vendor, yet be regarded as simply a feature of a broader offering by another, or even be implemented via capability embedded in an OS or management suite.

The trick to avoiding confusion is to keep the logical models we have been discussing in mind when reviewing specific solutions.

Benefits and practicalities

Two common threads run through all of the models we have been discussing: centralized management and the minimization of dependencies between components and activities. Let's take a look at the benefits that arise from these, then go on to consider the individual pros and cons of each specific desktop virtualization model.

Benefits of centralized management

From an IT perspective, central control can simplify operational challenges such as asset management, patch management and license management, as well as enabling desktop policies to be defined and implemented more straightforwardly; a welcome benefit for often overstretched IT professionals.

Better central control is also the basis for improved security and compliance. It helps to ensure user environments are as up to date (and therefore secure) as possible, and offers an opportunity to lock down elements of the desktop to prevent user mishaps, misuse and abuse. The centralization of storage can then facilitate enhanced data protection.

The other big benefit is improved support. Flexibility for the user is enabled in a more controlled and consistent manner, with enhanced visibility of what has been deployed and how it is being used. This makes troubleshooting and remedial work much easier, further reducing IT overheads, as well as providing a better service to users.

Benefits of minimizing dependencies

Breaking the bond between hardware components, software components and user data underpins many of the benefits to do with flexibility. Users can access applications and data wherever it's most convenient, including running the work environment on a home PC or an internet kiosk. They can receive new and updated applications more quickly, and can even benefit from self-service application provisioning.

Separating applications from each other minimizes conflicts, which means fewer interruptions because of crashes and machine instability. Business continuity and flexible working practices in general are also enhanced, e.g. if a local desktop or even the entire office becomes unavailable, users can access their work from other (appropriately configured) machines, including from home.

Benefits and constraints of specific models

Beyond the generic benefits, each desktop virtualization model has its own unique set of capabilities and constraints. These dictate where the model can add most value, and as importantly, where it might not be either practical or appropriate. Let's take a look.

Session-based VDI

- ☑ The main benefits of this model stem from the centralization of control and data storage, and standardization of the desktop environment. IT overheads are reduced, security and compliance are enhanced, and desktops are easier to maintain and support, which benefits both IT and users.
- ✎ Desktops delivered though this model are relatively fixed, i.e. the user has little control over the core configuration. The impact of this can be reduced through the use of application and user virtualization, but the model is not really suitable for users requiring a lot of freedom and flexibility. The dynamic sharing of (and competition for) resources can also make this model unsuitable for more demanding users.
- ✗ Dependency on a good network connection means this model is unsuitable for mobile users who need offline access to their corporate resources.

VM-based VDI (shared image)

- ☑ Management is simplified and overheads reduced through the use of shared images. Dedicating resources to VMs allows support of users who need a reasonable level of performance.
- ✎ Even with shared images, more server resources are required compared to session-based virtualization. Image sharing also

translates to less flexibility, which can be alleviated to a degree through the use of application and user virtualization, but still represents a constraint for users needing a lot of flexibility.

- ✗ Dependency on a good network connection means this model is unsuitable for mobile users who need offline access to their corporate resources.

VM-based VDI (personal image)

- ✓ Again, centralization of control and storage can reduce IT overheads and improve security and compliance. A high degree of user flexibility, along with dedicated resources per VM, allows support for more demanding users.
- ! VDI requires more server resources than session-based virtualization and when personal images are used, a significant amount of network-based storage is also required, both of which can elevate implementation costs.
- ✗ Dependency on a good network connection means this model is unsuitable for mobile users who need offline access to their corporate resources.

Virtual application streaming

- ✓ All users see increased stability, and those using multiple devices enjoy broad, flexible access to their applications from any compatible physical or virtual desktop. IT sees a reduction in time spent on testing, rollout, maintenance and support, and where vendor terms permit, licensing costs may be reduced through on-demand software deployment. Local execution of

applications (once streamed) means this model is suitable for all users, including mobile ones.

- Virtual applications are generally OS-specific.
- No significant downsides.

Remote application execution

- Users can access applications immediately from any compatible machine with the necessary connectivity, greatly increasing flexibility in an office or campus setting. Central execution in a highly controlled environment enhances stability and security, and reduces IT complexity and overhead.
- Good for applications that need to interact natively with the desktop, but can be overkill for deploying the desktop component of client-server systems such as ERP, where it is often better to switch to a browser-based interface.
- Dependency on a good network connection means this model is unsuitable for mobile users who need offline access to the application concerned.

User and data virtualization

- Relevant in almost any environment to preserve user settings and preferences and make user data easily accessible when multiple desktops are used. Supports flexible and productive working, even when no other form of desktop virtualization is in place, but also adds an element of personalization to virtualization options that would otherwise be more rigid from a user experience perspective.

- Some solutions in this space only support a limited range of operating systems. This isn't necessarily a big drawback (as settings and preferences are often handled quite differently between OSs, so synchronization of them may not make sense), but it is something to consider when reviewing options.
- No significant downsides.

The above models are the ones that are generally most appropriate for use in a mainstream end user environment, but as we have seen, each has limitations as well as potential benefits. It is therefore essential to have a clear understanding of your requirements and constraints before attempting an implementation.

Analyzing your requirements

The best way of analyzing requirements is through a user profiling exercise. The aim is to build a picture of which applications are being used, how and by whom, and to identify groups or segments with the same or similar requirements. Needs in terms of the required application mix are important here, as are constraints and considerations to do with performance, access and security.

In practice, profiling exercises aren't as onerous as you might imagine, as you can focus initially on a subset of users in a specific department and/or use automated discovery tools that interrogate machines over the network to speed up data gathering.

However you go about your profiling, it's important to identify all applications currently installed, exactly as you would in preparation for a traditional desktop migration project. Categorize applications

according to their importance, and if rationalization or consolidation is appropriate, do this before getting into any virtualization activity.

As part of the requirements analysis, you should also think about emerging and future needs, such as better enablement of flexible working, support for the safe and cost-effective use of personal equipment, or laying the foundations for new collaborative or mobile productivity applications.

With all this in mind, questions to consider when analyzing needs and grouping users include:

- Which applications are important today, and which are likely to become key in the future?
- Are the application needs relatively static or likely to change on a frequent or continuous basis?
- What is the level of need for applications that are particularly demanding in terms of compute power or graphics capability?
- What is the mix of devices likely to be used, and will the use of personal equipment be supported?
- How much need exists for applications to be configured or managed by users as opposed to by the IT department?
- What are the requirements for operating over slow or less reliable networks, or even running applications in disconnected mode?
- Are there any special security or compliance concerns?

Segmenting users

One possible outcome of your segmentation exercise might be a set of groupings based on role, such as:

- Managers and executives.
- General administration staff.
- Finance and accounting staff.
- Sales and marketing professionals.
- Customer services representatives.
- Engineers and technicians.

However, where the workforce is more complex, or where a lot of 'exceptions' to normal requirements exist, it can sometimes be better to segment users based on key characteristics or behaviors such as in the table overleaf (Table 2):

User type	Characteristics
Task/process worker	Works from a fixed location, always connected to the LAN, often through a hot-desk terminal (e.g. in a call center), limited set of applications (e.g. CRM or ERP access).
Admin worker (regulated)	Works from a fixed location, always connected to the LAN via a dedicated workstation, fixed set of applications, but often working with sensitive data or on highly regulated activities.
Admin worker (normal)	Works from a fixed location, always connected to the LAN via a dedicated workstation, fixed set of applications, but not involved with particularly sensitive or highly regulated data.
Office-based professional	Usually desk-based, well connected, one or two devices, more variable or demanding application requirements.
Roaming professional	Works from different locations, intermittent or variable connectivity, multiple devices, variable or demanding app requirements.
Home office worker	Works from fixed desk at home, reasonably well connected over broadband, single device, fixed set of applications.
Guest/BYOD worker	Needs to connect personal or non-company device to corporate network, limited access to small number of specific applications.

Table 2: Example segments based on characteristics/behavior.

Please note that the purpose of Table 2 is to show how requirements can vary between groups – it is not intended to be exhaustive.

Mapping options to needs

Mapping is all about identifying the most appropriate option, or blend of options, for each category of user to get the balance right between cost, performance, security, flexibility and control.

If you work through all of the needs and practicalities, and bear in mind the economics (e.g. use the less costly session-based model rather than VDI for users with fixed application needs and modest performance requirements), then you may end up with a mapping that looks something like this for OS deployment options (Figure 2):

Centralized ⟷ Localized

	Session-based VDI	VM-based VDI (shared)	VM-based VDI (personal)	Local physical desktop
Task/process worker	●	○	✘	✘
Admin worker (regulated)	⊙	●	○	✘
Admin worker (normal)	○	⊙	○	●
Office-based professional	✘	○	⊙	●
Roaming professional	✘	✘	✘	●
Home office worker	⊙	⊙	✘	●
Guest/BYOD worker	●	⊙	○	✘

● Preferred/primary option
⊙ Option, depending on practicalities
○ Generally only for exceptional needs
✘ Generally not appropriate

Figure 2: Typical mapping of deployment options to user types.

The figure on the previous page was put together bearing in mind the limitations of current solutions, the typical constraints of most existing enterprise infrastructures, and the common limitations of networks in terms of coverage, performance and reliability. It would, in theory, be possible to be more aggressive with regard to centralization, but it's important to be realistic rather than idealistic.

Once the OS deployment model is selected, you can turn your attention to the deployment of applications that have not been pre-loaded into the OS image. Virtual application streaming is likely to be used for frequently updated software, with limited or transient use requirements met through remote applications. User and data virtualization may then be layered across everything.

As you work through your options, it is useful to bear a couple of general principles in mind when making choices in situations where more than one model is technically viable:

- Always opt for the cheapest viable option that meets the users' requirements when it comes to the core desktop OS. When you take the cost of software, server hardware, storage and operations into account, the order of preference is session-based VDI, VM-based VDI (shared image), VM-based VDI (personal image), then local desktop. It just so happens that this order also reflects the level of control in terms of management, security and compliance, which is quite useful.
- Always opt for the most centralized application deployment model viable, with the order of preference being remote applications (where connectivity is assured), virtual (streamed) applications (where connectivity is variable), then directly installed apps. If the latter is selected in relation to server-based desktops, embed the applications into standard images wherever

possible so image refresh can be used to keep everything up to date.

So having done your mapping, are you ready to get on with procuring what you need and starting your implementation? Well no, there is still some planning to be done.

Desktop virtualization software

The first and most obvious consideration from an enabling perspective is the software required to implement your desktop virtualization environment.

As we have mentioned, the chances are that you will end up using a number of the models we have discussed, perhaps even all of them, which translates to a lot of functionality in software terms – server operating systems, hypervisors, connectivity components, monitoring and management tools, and so on.

It is beyond the scope of this Smart Guide to go into any level of detail on software vendor and solution evaluation and selection. Suffice it to say that you are likely to be faced with choosing between a collection of specialist solutions, each working together to deal with different aspects of your virtualized setup, or one or two broader 'suites' that take care of most of what you need within an integrated framework. This kind of choice will be familiar to those in IT, and the criteria you apply should be determined by your needs.

A specific and critical part of any desktop virtualization environment is the management piece, so it's worth paying special attention to making sure you understand the implications in this area before embarking on an initiative.

Management considerations

Desktop management isn't straightforward at the best of times, and while desktop virtualization will usually help with many operational requirements, explicit and proactive management is still required.

Indeed, some aspects of management become more challenging as virtualized environments provide users with greater flexibility to work in new ways, exploiting multiple devices enabled through a different mix of models and connecting over multiple network types. It's not that such behavior doesn't take place in more traditional setups, but in the virtual world there will be more of an expectation for everything to work together in a coordinated, robust and well-performing manner.

To ensure routine operational management is effective it is essential to consider key elements up-front, such as:

- **Asset management:** Desktop virtualization does not dispense with the need to maintain an accurate view of devices, users, software deployments, usage, etc.
- **License management:** It's important to ensure that the licensing regimes and agreements with software vendors are appropriate for your virtualized environment.
- **Software distribution and patch management:** Both of these should be more straightforward, but operational processes will need to be adapted.
- **Health and performance monitoring:** With centralization, a failure or performance issue is likely to impact a lot more users, so effective operational monitoring becomes critical.

- **Backup and recovery:** User data as well as application and configuration settings need appropriate backup and recovery, as, of course, does the server and storage infrastructure.
- **Security and compliance:** Centralization can help with these, but the increased flexibility potentially provides more scope for issues to arise, so a reappraisal of policies, processes and supporting tools in this area is advisable.
- **Help-desk:** As well as expecting a larger than usual influx of calls during the transition period, you must make sure that your support processes are geared up to the specifics of virtualized desktops and applications and that your help-desk staff have been trained with the new solutions in mind.

In addition to changes in these routine aspects of management, desktop virtualization brings with it a number of other management considerations:

- **Image management:** Tools and best practices are required to minimize the number of images you need to support, and to maintain the images that exist, including tracking, patching, upgrading, provisioning and de-provisioning.
- **Application packaging and maintenance:** For virtual applications in particular, tools and processes are required to manage the packaging, testing, provisioning and de-provisioning of software.
- **Policy-based deployment and access:** Delivering the kind of anytime, almost anywhere access with a seamless user experience that we mentioned at the beginning of this Smart Guide can only be achieved with policy-driven automation. If

> IT needs to be involved every time a user wants to log in from a new device or over a different kind of network, the promise of flexibility is undermined. User/scenario-based automation of application delivery and access is, therefore, key to success.

Lastly, you probably won't end up with an entirely virtualized desktop estate – you'll be managing both physical and virtual machines in parallel. By considering the management and operation of both physical and virtual resources from the start, you avoid the possibility of fragmented and disjointed operations that inevitably lead to escalating cost, risk and overhead.

Impact on physical infrastructure

Beyond the enabling software, success with desktop virtualization is also hugely dependent on having an underlying server, storage and networking infrastructure in place that is up to the job.

It's important not to underestimate how much network bandwidth is required for remote displays in the case of session virtualization, or to misjudge how many users can work in parallel on a single server in the case of VDI. Making sure that central storage platforms can meet expected peak demands without impacting user response times, e.g. as virtual machines are booted at the beginning of the day, is something else that must be considered.

Suppliers can often help with analysis and sizing exercises if you are not comfortable working out the infrastructure requirements yourself. Either way, in order to maximize the chances of success, it is always advisable to test the proposed configuration in a way that is relevant to the real world. Piloting with selected groups of

users to ensure that the setup is going to deliver against required or expected service levels is a good way of doing this.

Tips for success

We have taken you pretty much as far as we can without coming along and working beside you. Hopefully, the material we have covered has provided you with a good starting point for understanding the potential represented by desktop virtualization, crystalizing your needs, and creating a first cut plan of action.

Before we finish, however, let's pull out some tips, tricks and traps to keep in mind as you take it from here:

- **Put the users first:** This doesn't mean 'giving people what they want', but it does mean giving people what they need to do their jobs in a productive and motivated manner. Getting this right has a collateral benefit of increasing user satisfaction with virtualization solutions, so it is essential to manage users' expectations in advance and to communicate effectively.
- **Remember the alternatives:** Desktop virtualization provides a lot of options as we have seen, so don't get drawn into focusing on one deployment model, as some suppliers may encourage you to do. Perform your analysis, determine your needs, and select the right mix of solutions to meet them.
- **Focus on subsets of users with clear needs:** Defining user segments or groups, then prioritizing based on the level of potential benefit weighed up against the cost and risk of delivering it, will help with phasing development, testing, piloting and rollout, and with securing early success.

- **Take the opportunity to clean up:** Now is a great opportunity to update, consolidate and rationalize your application portfolio.
- **Get the configuration right:** Too many desktop virtualization initiatives are hamstrung by inadequate specification of the hardware and software required to work at scale, notably around storage and networking, especially to cope with peak demands. Get help from suppliers on this if you need it.
- **Consider management up-front:** It's important to appreciate that desktop virtualization technologies have their own administration requirements. The investment and effort needed to put the necessary tools, processes and training into place must be planned into the implementation project.
- **Build in continuity, data protection and security:** It's critical to make sure that the risk management element is an integral part of your up-front analysis, ensuring that needs associated with protecting user data and countering security threats are understood.
- **Be inclusive when considering the cost:** Implementing desktop virtualization will almost certainly require investment in server hardware, software, management tools and implementation effort. Upgrades to your network and storage infrastructure may also be required. It's no good getting part way through an implementation then figuring out you need more funding than you budgeted for.
- **Be inclusive when considering the benefit:** Some benefits may translate to direct, quantifiable savings, e.g. prolonging the life of desktop hardware, streamlining the application lifecycle,

and reducing support and operational overhead. Other benefits may be less quantifiable, such as the removal of downtime, the boosting of user productivity, or the enablement of new ways of working.

- **User training:** While the differences in user experience between the old and the new may appear to be small, appropriate training can ease the transition and also identify any last-minute gotchas, such as missing applications.

Closing advice

We have talked about some very compelling ideas and technologies, but as we highlighted at the beginning of our discussion, changes to the desktop will have a direct impact on employee productivity and the relationship between IT and the business. It's a highly sensitive area.

Given this, we cannot stress the importance of analysis and planning enough. It needn't take long, especially in a smaller scale environment, but it needs to be done, and properly. Neglect this advice, and you are likely to run into problems with both users and business stakeholders. Get it right, though, and you and your users could start to unlock the potential of desktop virtualization and flexible working in a relatively short space of time.

With that, we hope this Smart Guide has helped you to appreciate some of the theory and practice, and we wish you the best of luck with your desktop virtualization initiative.

Further reading

User Virtualization (Smart Guide Mini-Book)

Beyond device-centric computing

The Consumerization of IT (Research Report)

A question of freedom versus control

Applied Desktop Virtualization (Research Report)

Perceptions, reality and practicality

These may be downloaded from www.freeformdynamics.com

About Microsoft

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

See here for more information on Microsoft desktop virtualization solutions: www.microsoft.com/DV

This book was written independently by Freeform Dynamics and sponsored by Microsoft.

A Smart Guide published by

FREEFORM DYNAMICS

Desktop virtualization has progressed from a niche way of handling exceptional user requirements to a mainstream IT delivery approach. Technology has matured to provide options ranging from terminal services through application and user virtualization to a full-blown virtual desktop infrastructure.

All in all, there have never been more ways to optimize desktop service delivery. But where do you start and what's the best way forward? With these questions in mind, and against the backdrop of increasing workforce mobility and consumerization, this Smart Guide walks you through the options available and how to blend them optimally to meet different user needs.

The rewards for IT and the business are better cost and risk management, while for users, it's all about enabling flexible and efficient working.

Get it right, and everyone benefits!