

Taming the Tablet, Finding Your Strategy



For most IT departments it's an all too familiar story: Executives discover the latest technical gadgets, start using them at home and bring them to work, expecting to access corporate applications, e-mail and data instantly. Then there are the employees who have already worked out how to access corporate data using their tablet devices, and are carrying sensitive e-mails around with them, unwittingly placing the organisation at risk.

Tablets, specifically, are becoming ever-more popular both for personal and professional use, and the adoption rate of Apple iPads has overtaken that of the Apple iPhone in 2007 and DVD player in 1997.

Double-edged sword

As employees at all levels drive the requirement for secure access to business information from mobile devices, IT departments find themselves in the inevitable predicament of having neither the right capabilities nor infrastructure to support these new devices. Managing mobility is a challenge as it represents largely uncharted waters and right now, there is no one-size-fits-all solution or approach.

On the one hand, employee-owned tablets are powerful from a computing perspective, and organisations recognise the value of making sure these devices can access corporate networks, applications and data, to make it easy for employees to maximise work time, wherever they are. Indeed, Gartner Research predicts that 90% of organisations will support corporate applications on devices owned by end users by 2014².

However, while mobile devices are ushering in an age of improved productivity; organisations are still somewhat 'at sea' when it comes to integrating them, from a security and manageability perspective. Meanwhile, users expect a seamless transition between personal and business use and aren't concerned about operating system issues – rather they want a solution, and they want it now.

One thing is clear: achieving buy-in for a **desktop virtualisation** solution can't be based on promises of lower upfront costs. Rather, the approach should be to focus on the feature, **functionality and business issues that are addressed through these solutions.**

As IT teams seek ways to support the growing variety of client computing devices, they have to iron out compatibility issues and need a strategy to manage these new client environments. For mobile devices, this means managing them in a similar way to other corporate IT assets through smart usage management, configuration and security.

How desktop virtualisation can help

Effectively controlling and managing end-user devices, whether they are fixed or mobile and whether they are owned by your organisation or by your employees, involves finding a means to abstract the user experience from the device, the underlying operating system, the applications involved, and the corporate data. For these reasons, some organisations are moving away from the traditional model of the monolithic desktop in search of a fundamentally better way to operate their end-user environments. Many are investigating desktop virtualisation with the aim of storing their data centrally. This core manageability over data provides the key to ensuring users can log on to corporate networks using their chosen device and access data, while meeting mobile requirements and protecting corporate data assets.

Desktop virtualisation has the potential to enhance device security and simplifies IT management. With it, your IT team can provide a well-provisioned desktop in the data centre and can centrally manage and deliver corporate applications and desktops on employee-owned devices. It also enables users to switch between devices easily, removing the need for individual management – and it's viable now with tablet devices.

But what about the issues around compliance (licensing), architectures (your network), security and governance? And as with all new innovations, any changes have to be justified in terms of cost.

Cost and complexity

All devices have to be supported by a back end infrastructure. While thin client and tablet devices like iPads have a lower unit cost at first, the investment required to support them is as large (if not larger) than with traditional PCs. For organisations seeking to provide access to applications via tablet devices, it means they need to be connected to a server-based computing (SBC) or Server Hosted Virtual desktop (HVD) infrastructure. It may also require re-development of applications to work on specific platforms, especially if offline access is required. One thing is clear: achieving buy-in for a desktop virtualisation solution can't be based on promises of lower upfront costs. Rather, the approach should be to focus on the feature, functionality and business issues that are addressed through these solutions.



Are you covered?

How do you make provision for Microsoft and other third party business applications that aren't native to tablet devices, but have to be supported somehow? Providing tablet access to corporate applications means working out the impact on licensing of Microsoft products. Achieving compliance can result in a large unbudgeted expense, so organisations would do well to address three main usage scenarios for tablets such as iPads accessing Microsoft software and servers which include:

- Running e-mail from the Exchange server using built-in e-mail and calendaring clients;
- Accessing an HVD using secure access clients; and
- Using server-based Microsoft applications, such as Office using Microsoft Remote Desktop Services (RDS)

Many, if not most, tablet users will need to use Windows applications that are not available natively on their device and there are separate licensing issues to consider, regardless of who owns it, such as:

- Rights to access e-mail, RDS or other servers running Windows Server OS
- Rights to run Windows XP or Windows 7 desktop OS
- Rights to access Microsoft applications (including Office)

The fact is: When it comes to alternative or user-owned devices, Microsoft licensing requirements are complex and still not well defined. While the default licence position up until now has been device-based client access licences (CALs), it becomes more complicated when employees use their PC and tablet device at the same time, making user-based CALs the better option.

One thing's for sure: Current licensing issues are expected to evolve as new usage scenarios become commonplace, which is why businesses should seek the advice and guidance of their relevant Microsoft Large Account Reseller. Seasoned licensing specialists can assist with complex usage setups and ensure organisations are getting the most out of their licensing agreements.

Access to the network

Desktop and application virtualisation removes the need for siloed hardware resources and locally installed applications. At the same time, organisations need to understand the strain this technology can place on their data centre infrastructure, networks and operations – especially when thousands of employees use this platform type.

While HVD or SBC infrastructures can provide access, the range of available devices will depend on your organisation and end-user requirements. It may also be dictated by performance factors such as environmental, power consumption, form factor (or footprint), useful life and cost – and each will be weighted according to business priorities.

There is no universal approach. Rather, organisations should assess existing infrastructures before segmenting their user base and providing groups of users with desktops that are tailored to their requirements. If they don't need a desktop, give them a device like an iPad – something simpler and thinner which means less in terms of manageability. Finally, remember that some users may need both!

Securing your assets

Part of your user segmentation exercise should include a review of user groups against the categories of information being accessed. Security goes beyond virtualisation and should limit the type, use and flow of information that can be downloaded to unsecured devices like iPads.

For most business and corporate users, tablet devices offer fairly good security – with Apple’s mobile operating system (iOS), which is used in iPads supporting PIN and other good-to-have options such as Secure Socket Layer (SSL) encryption of messages in transit (a native capability of iOS). Google’s Android tablet devices can also be set to require a PIN and can support password and remote wipe and in-transit encryption.

Those organisations that have already worked out how to support tablet devices like iPads have addressed their security issues through blending four broad categories of access that include:

1. Routine business information – where PINs are important, as are other security and management capabilities like password expiration, remote wipe, in-transit SSL encryption of e-mail and other data and complex password requirements
2. Important business information – where the potential for economic and public relations damage requires complex password management including password expiration, remote wipe, in transit SSL and other good-to-haves such as VPN and on-device encryption
3. Sensitive business information – where essentials include complex password management, expiration, in-transit SSL, VPN and on-device encryption plus ideally the ability to control access to specific networks
4. Top secret information – where essentials include complex passwords, password expiration, remote wipe, in-transit military grade encryption, VPN access to sensitive information and data stores, physical second factor authentication support, on-device encryption and discrete lock down controls to name a few.

The tools for the job

The most secure and cost-effective way of providing access to corporate applications via tablet devices is to give users access to server-based computing capabilities – either server-based applications or hosted desktops.

Successful virtualisation of user desktops allows you to maintain desktop images that remain separate from computing devices. The result is better security, and improved performance availability that is achieved through well integrated system policies. But how exactly do you do that?

Depending on the infrastructure, there are a few options for Microsoft users – both out of the box and through third party VMware and Citrix technologies. A new environment with a VDI solution through Windows server can create desktops under your existing licence agreement.

If your business has complex networks and a branch environment for example, it may be worth looking at deploying a Citrix layer on top of an existing RDS layer for virtual communication into data centres, with an optimised desktop that enhances the user experience. This ability to offer a centralised desktop through a VDI suite means you can look after the desktop image centrally and patch it automatically. And because it’s a confined environment, you can manage the system easily and reduce risk.

Providing enhanced support for mobile clients includes minimising disruption to the user experience, and enabling users to tailor their work environment to suit their needs. Mobile management platforms allow IT managers to create separate profiles for employee- and company-owned devices, to separate personal and corporate data, and to remotely configure VPN, WiFi and other critical settings.

This means users can access the same applications from multiple devices, with full synchronisation across the devices – and can choose the one that is most convenient at the moment, or best suited to a particular task. Where users want more intense computing capabilities, they will be able to work on multiple devices at the same time.

Where users choose to work with their smartphones for example, vendors are leading the charge with new technologies – where VMware’s mobile virtualisation software allows users to have two completely separate virtual phone instances on the same phone hardware.

The challenge for IT professionals is how to integrate new and old technologies (and devices) and implement solutions that will complement what their organisations have in place today. To deliver what users need, when they need it, there has to be synergy between all technologies.

The certainty of change

Whatever the device or client computing option, organisations require a strategy to manage these new client environments. This in turn has to be backed up by expertise, processes and management tools.

The growing number of available client architectures means organisations are likely to use several platforms to meet the varied computing needs of their users. While we don’t expect one to prevail, each of these new technologies comes with its own management requirements and technology capabilities, putting organisations at risk of creating new technical and organisational silos and making them dependent on



technical skills. At the same time, while these user architectures offer the promise of improved user productivity, there is still an underlying requirement to reduce the total cost of ownership.

Organisations should bear in mind that creating separate groups based on platforms is more likely to lead to inconsistent decision making, and may add operational complexity from a support and maintenance perspective, as well as an overall disintegration of standards.

With users having as many as three devices or needing to access their environment from different locations, they may have to be enabled by multiple different platforms.

Developing a cohesive strategy for users, instead of individual platforms, will ensure consistent and secure access. It is also why it is worth having a single client computing service group in place that is responsible for understanding business objectives and delivering client computing capabilities to support them.

With no single suite available to manage all of these platforms, organisations would do well to implement a consistent policy and process, while keeping their long term desire for single management across all user platforms in mind. Getting this right will give users the access they need, and will ensure IT teams are geared for the certainty of more change.

With **users** having as many as three devices or needing to access their environment from **different locations**, they may have to be enabled by multiple different platforms.

So where do you start? How do you decide on the right technologies, roadmaps, delivery mechanisms and policies for your organisational needs and tame the tablet? Dimension Data recommends looking beyond the operating system at user profiles, business applications and working requirements when defining your desktop strategy. The knowledge gained from our desktop deployment experience, systems management and integration capabilities have been rolled into our Next Generation Desktop Assessment.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • CONGO
DEMOCRATIC REPUBLIC OF THE CONGO
GABON • GHANA • KENYA
MADAGASCAR • MALAWI
MAURITIUS • MOROCCO • NAMIBIA
NIGERIA • SAUDI ARABIA
SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES • ZAMBIA

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES