

# Desktop Virtualisation and Security: Virtual 'Lock and Key'



**Desktop's virtualisation** is well on its **journey into the mainstream**. At the same time, it's ushering a host of **new considerations** for IT professionals – not least **security managers**.

A quiet revolution is currently underway in the desktop domain. The days of the traditional, monolithic desktop – where applications, the operating system and user data are all 'tied' to a specific piece of hardware – are numbered. The Client Virtualisation Imperative, 2011, a commissioned study conducted by Forrester Consulting on behalf of Dimension Data, confirms that organisations across all industries and geographies are prioritising their investment in desktop virtualisation. Overall, 40% of organisations view investing in and/or implementing desktop and application virtualisation as a 'high priority', while 12% deem this an area of 'critical priority' over the next 12 to 24 months. The study was conducted with 546 senior IT decision-makers in 16 countries.

Virtualisation breaks the traditional elements of the desktop into isolated multiple layers, enabling IT administrators to change, update and deploy each component independently. The advantages of this approach are plentiful and widely accepted. They include the ability for businesses to provide employees with the flexibility to work anytime, anywhere, on a range of devices, simplified application provisioning and management, and less labour-intensive Microsoft® Windows 7 deployments.

Enhanced security represents a further potential benefit of embracing desktop virtualisation. Indeed, the results of the Forrester study indicate that security ranks among the main drivers behind organisations' decision to pursue desktop virtualisation, with 59% of respondents citing it as a key motivating factor.

And with good reason. Many IT managers who have successfully deployed client virtualisation report dramatic improvements in their data security processes and patch management efficiencies. Why? Because the technology enables organisations to

remove all data from the user machines and instead host it in the data centre or public cloud. Now, the impact of a lost or stolen machine represents little more than the cost of the physical replacement, instead of the potential data security breach, the prospect of which used to keep IT professionals up at night. For many organisations, simply avoiding the cost of embarrassing and time-consuming disclosure procedures can make the case for client virtualisation.

### The 'but'

While the security boons associated with desktop virtualisation are compelling, it doesn't completely solve all traditional security risks. In fact, IT leaders need to be mindful that this approach also creates a new set of potential security hurdles.

"Desktop virtualisation creates a new paradigm for security managers, as it changes the ways that users interact with data and the network. Areas of the environment become more complex and additional attack surfaces are created,"

explains Stephen Mills, Dimension Data's Global Security Consulting Product Manager.

On the one hand, housing all your data in a central repository – as opposed to distributed widely among an array of physical devices – may be perceived to reduce business risk. However, it also amounts to 'placing all your eggs in one basket' if it's not carried out in a focused and thoughtful manner. Ensuring that the business' security posture is not compromised by the central model calls for organisations to implement processes to protect their data and maintain a robust security profile.

Let's take a closer look at some of the potential security risks that desktop virtualisation introduce and consider what businesses need to do to side-step them:

### Infrastructure vulnerabilities

All hardware and software have inherent security vulnerabilities of some kind. Effective security management is about designing your infrastructure estate in a manner that takes these risks into account. With desktop virtualisation, your infrastructure is highly Internet-facing, which inevitably translates into a plethora of new threats. You need to ensure you

### "Which features are driving your firms interest in application virtualisation?"

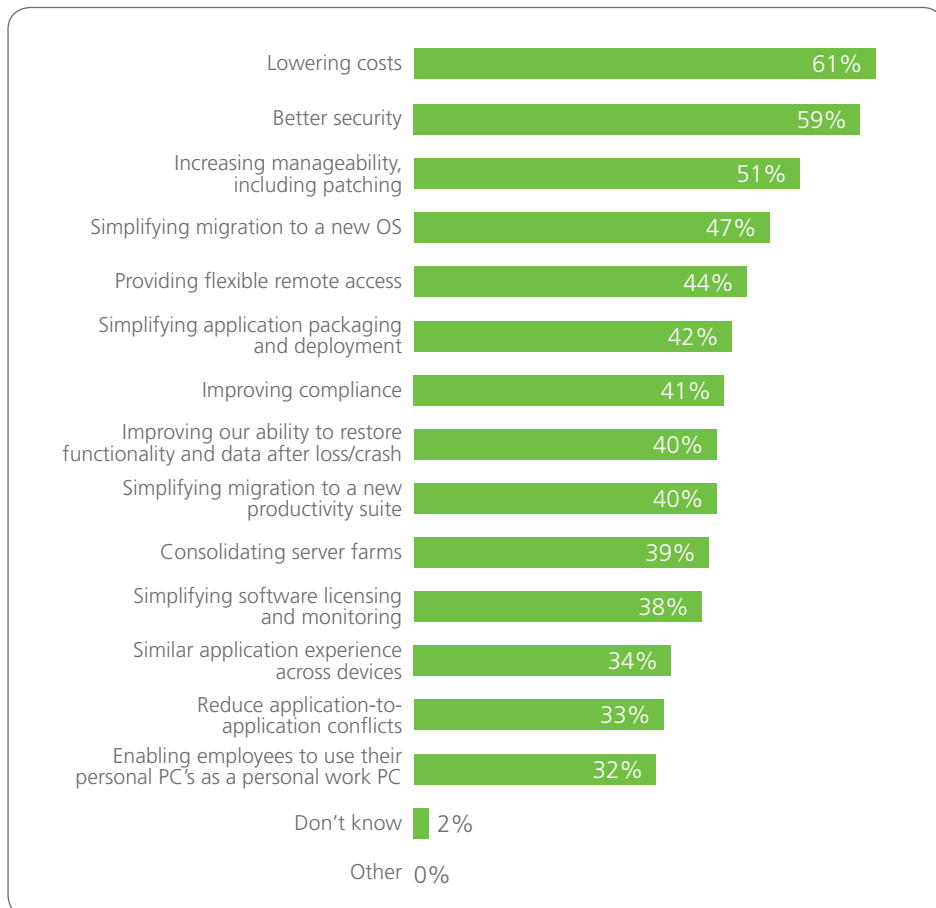


Figure 1 – Security, Cost and Manageability are the Main Drivers for Desktop Virtualisation.

have appropriate controls in place to patch issues as they arise and ensure ongoing proactive monitoring of your devices. Also adding to the risk are the many layers of infrastructure that make up a virtual desktop, when compared to the traditional model.

### **Virtual Desktop Infrastructure (VDI)-specific threats**

Once users log into a virtual desktop, they are immediately – and unknowingly – exposed to a number of threats to which they aren't subjected when using traditional desktops. For example, there have been instances of hackers exploiting the new network avenues that are opened up in a virtual desktop environment and effectively 'hijacking' the VDI. Other tactics include sending users an e-mail, the attachment to which contains malware that disables your ability to connect to the VDI.

To circumvent these threats, organisations should put in place and rigorously enforce a policy regarding what is permitted to connect to the VDI. For example, many will disallow the use of USB devices, which may easily be compromised. Others invest in technology that allows for USB devices to be automatically scanned before use. Your policy should also provide clarity regarding whether it's permissible to copy data from a laptop to a VDI and whether driver mapping is allowed.

### **Environmental threats**

Established and longstanding security hazards such as the disgruntled insider and opportunistic external third-party require as much, if not more focus, in the virtual desktop world. As mentioned earlier, if you're storing all your data and intellectual property in a central repository, you need to take additional steps to ensure its safety and integrity. With the centralised model, the potential consequences of administrator rights misuse or password abuse/weakness become amplified. Dormant virtual machines also pose a new risk, if they're not appropriately patched or upgraded.

Given the new slew of security considerations that desktop virtualisation brings to bear, what actions should IT security professionals consider to reinforce their businesses' defences?

"A structured and actionable plan on how these will be overcome should form part of any organisation's next-generation desktop strategy. Mills believes that there are two areas to consider: operations and technology."

"Effective operations involves ensuring that you put in place comprehensive security policies and procedures and that your systems are patched for desktop virtualisation-specific threats on a regular basis. Monitor your environment closely and should an event occur, be sure that an established process is in place to swiftly address it."

Technology has risen to the occasions and a host of mature tools are available in the marketplace to help organisations master the security challenges associated with desktop virtualisation.

Mills emphasises that from a technology perspective, IT teams need to pay close attention to the network architecture and how systems are designed.

"Before you step ahead in designing and deploying a desktop virtualisation infrastructure, you need to have undertaken a thorough assessment of all the new risks and vulnerabilities that you may be introducing within your environment,"

he cautions.

Ensuring information security and integrity can be challenging for even the most diligent organisation. Implementing a desktop virtualisation is an opportunity to tighten security, but it needs to be effected with a thorough appreciation of the potential new threats and vulnerabilities that this approach introduces. This will put you in a position to plug any gaps in your defences and harness the full advantages that a desktop virtualisation solution can bring to bear.

### **About the The Client Virtualisation Imperative Report, 2011:**

The Client Virtualisation Imperative, 2011, is a commissioned study conducted by Forrester Consulting on behalf of Dimension Data. In this study, Forrester conducted an online survey of 546 organisations, across all industries in Australia, Belgium and Luxembourg, Brazil, China, Czech Republic, Germany, Hong Kong, India, Kenya, Netherlands, New Zealand, Singapore, South Africa, the United Kingdom and the United States to evaluate the adoption of desktop and application virtualisation and the desktop transformation journey on which organisations are embarking. Survey participants included decision-makers in managerial roles and above for enterprise companies (1,000+ employees in developed economies and 500+ employees in developing economies). The study commenced in July 2011 and was completed in August 2011.

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • CONGO • BURUNDI  
DEMOCRATIC REPUBLIC OF THE CONGO  
GABON • GHANA • KENYA  
MALAWI • MAURITIUS • MOROCCO  
MOZAMBIQUE • NAMIBIA • NIGERIA  
RWANDA • 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