

# White Paper

---

## **Desktop Virtualization, Management, and Security**

*By Jon Oltsik, Principal Analyst  
and Mark Bowker, Senior Analyst*

**November, 2009**

---

## Contents

Contents.....	2
Executive Summary .....	3
PC Management – A Perpetual IT Problem .....	3
Desktop Virtualization to the Rescue? .....	5
VDI Use Cases in Vertical Industries .....	6
What about Security? .....	6
Security Must Have Virtual Intelligence and Integration .....	8
CIO To-Do List .....	9
The Bigger Truth .....	10

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188. This ESG White Paper was developed with the assistance and funding of RSA Security (The Security Division of EMC).

## Executive Summary

Desktop virtualization has received more than its fair share of publicity lately. But is it simply industry rhetoric or is this attention warranted? ESG believes that in this case, all of the interest in desktop virtualization is genuine. This technology can help large organizations gain some control over existing chaotic and complex desktop and laptop infrastructure AND improve desktop security at the same time. While this may be theoretically true, are users actually deploying desktop virtualization? And what about security? This paper concludes:

- **Large organizations are voting with their pocketbooks.** ESG's data indicates that many large organizations are already deploying, researching, testing, and planning desktop virtualization projects. Most are easing into technologies like VMware View today, but foresee more aggressive implementation over the next 3 years. This is especially true where desktop virtualization can help enable industry business processes. ESG has seen acute interest in the health care, higher education, and public sector markets in particular.
- **Virtualized desktop security remains elusive.** Desktop virtualization can help with basic configuration consistency and patch management, but specific problems around authentication, data security, and security/compliance management remain. If these issues are not addressed correctly, desktop virtualization will remain a niche technology at best.
- **Security must be tightly integrated into the desktop virtualization environment.** To overcome deficiencies, security must become an intermediary connecting users, data, and virtual desktop images in order to monitor and enforce security policies. Security tools must also bridge the virtual and physical worlds since physical desktops will continue to be the default platform for mobile and power users. If security intelligence is properly integrated into virtual desktop technology, it will address a conspicuous "weak link" in the enterprise security chain and lead to a marked improvement in overall enterprise security.

## PC Management – A Perpetual IT Problem

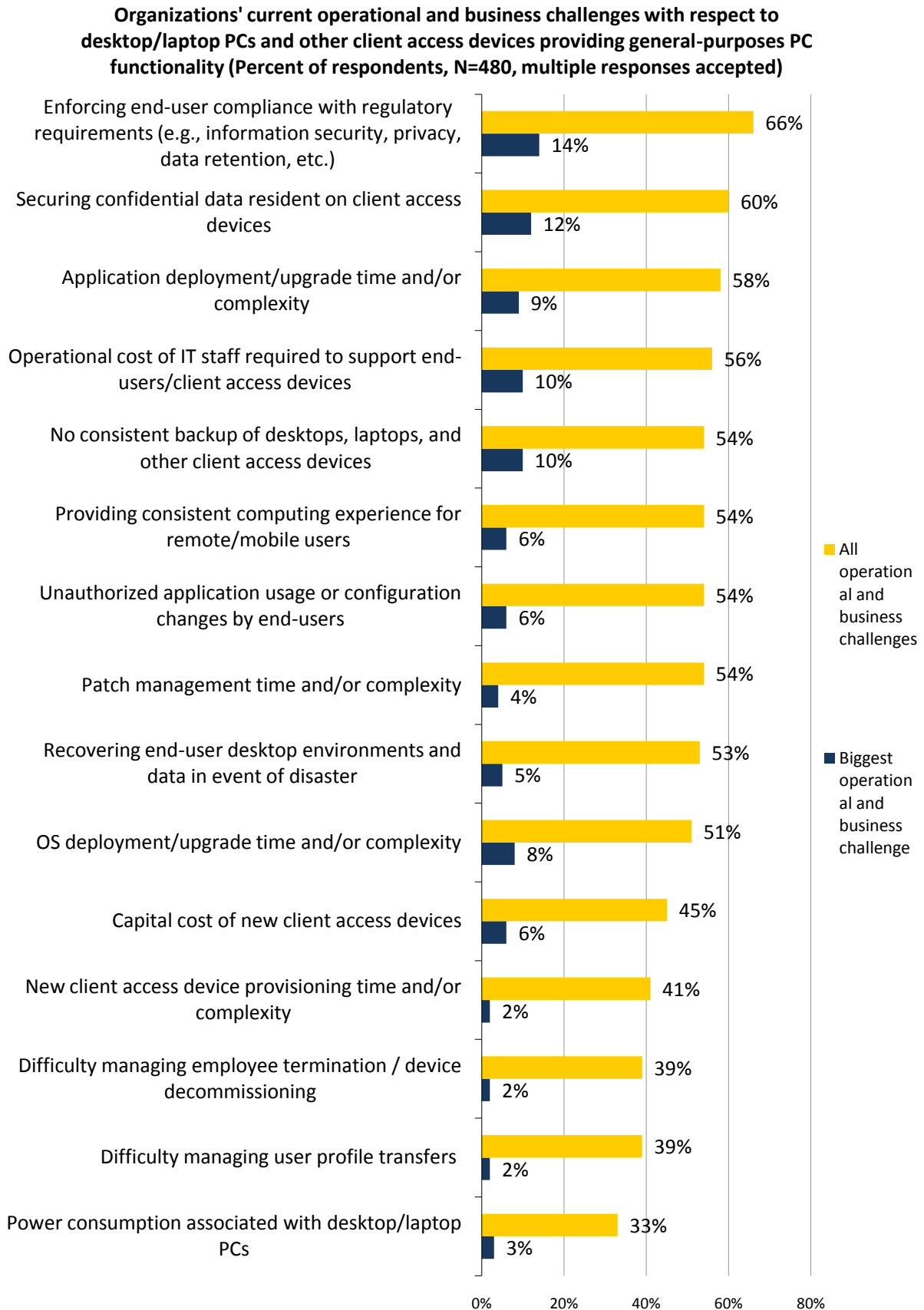
Once considered a rogue device, the PC has taken its rightful place alongside mainframes, Ethernet switches, and storage arrays as IT infrastructure staples. This being the case, why would large organizations even consider replacing venerable desktops and laptops with virtualization technologies? The answer can be summed up in a few words: management and control. Regardless of the IT environment, most enterprise organizations would characterize managing and securing an army of distributed desktops and laptops as a perpetual struggle. This thesis is supported by recent ESG research in which large organizations clearly indicate that PCs present a constant challenge for IT, especially with regard to areas such as regulatory compliance, security, and high operating costs (see Figure 1).<sup>1</sup>

ESG's data certainly makes a lot of sense considering that the PC world is in a constant state of chaos. Users download the latest browser plug-ins, add consumer hardware, and exchange confidential files as part of their everyday routines. To support this activity, IT scrambles with help desk support, software patch installations, and configuration changes. Given this stream of endless activity, regulatory compliance oversight can be a monumental task.

---

<sup>1</sup> Source: ESG Research Report, *Virtual Desktop Infrastructure Market Trends*, February 2009.

Figure 1. Most Significant PC Challenges



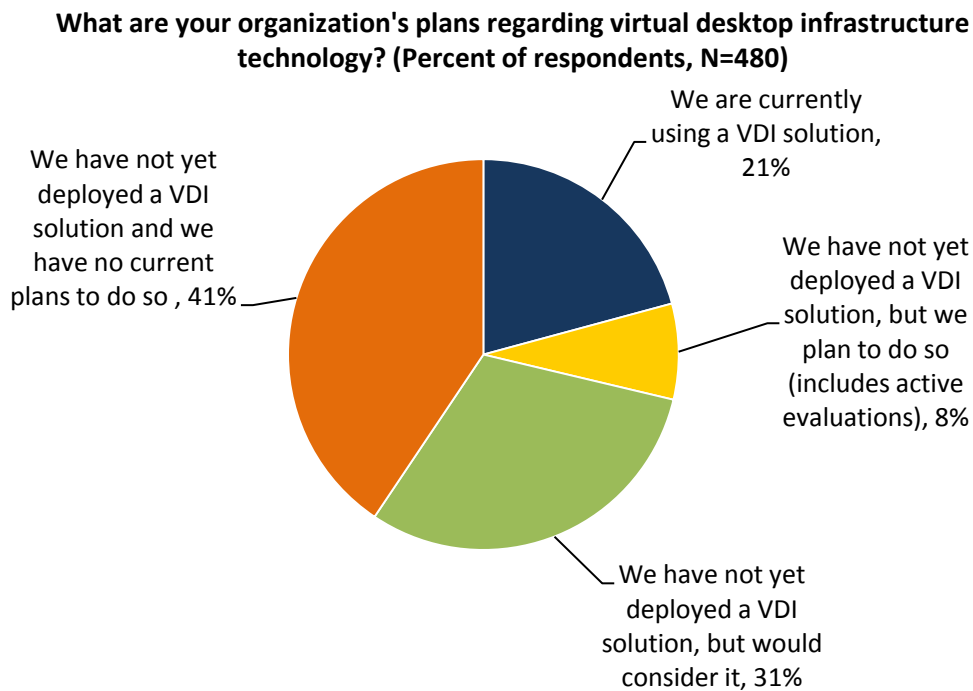
Source: Enterprise Strategy Group, 2009.

## Desktop Virtualization to the Rescue?

While many of the challenges surrounding traditional PCs are intensifying, these challenges in and of themselves are not necessarily new to IT staffs. Consequently, for years IT organizations have looked to alleviate the time and costs associated with redundant, labor-intensive PC management tasks by implementing various management environments so that PCs can be efficiently accessed, managed, and protected from a central location. Ideally, this can help organizations reduce operational costs, improve service levels, and satisfy compliance and information security requirements all while maintaining an identical—and in some cases, improved—end-user experience.

Given the proven benefits associated with server virtualization, many organizations see the same potential with desktop virtualization technology and have started preliminary research, testing, and even deployment efforts. In fact, ESG research indicates that 21% of large organizations have already implemented some type of desktop virtualization solution while an additional 39% are either planning to deploy a virtual desktop infrastructure or are interested in doing so (see Figure 2).<sup>2</sup> Most current desktop virtualization implementations are relatively restricted to limited production or test/development deployments, thus the majority of organizations have virtualized less than 10% of their PCs or other client devices to date. This scenario, however, is expected to change dramatically as firms move Virtual Desktop Infrastructure (VDI) projects from test/development to full production. ESG research indicates that nearly half (45%) of VDI users expect to have virtualized more than 50% of their client access devices over the next 3 years.<sup>3</sup>

Figure 2. Adoption of Virtual Desktop Infrastructure Technology



Source: Enterprise Strategy Group, 2009.

Desktop virtualization market drivers remain numerous and varied; however, several common themes emerge. In general, many firms are looking toward desktop virtualization as a way to reduce capital expenditures, streamline operations, and simplify OS deployment. Not surprisingly, desktop virtualization market drivers are a solutions-based mirror image of organizations' PC challenges cited in Figure 1.

<sup>2</sup> Source: Ibid.

<sup>3</sup> Source: Ibid.

## VDI Use Cases in Vertical Industries

Clearly, ESG's data indicates that universal challenges with PC management and security are driving growing interest in desktop virtualization technologies across enterprise organizations in all industries. That said, some industries also see desktop virtualization as an enabling technology for specific types of vertical industry business processes. Desktop virtualization can:

- **Facilitate efficient resource sharing for health care organizations.** Health care organizations face a unique PC challenge: oftentimes, PCs are shared resources (a.k.a., “workstations on wheels”) that must provide customized services for different health care professionals such as physicians, residents, and nurses. In this use case, desktop virtualization provides a new type of solution to centralize the management of applications, allow for improved personalized services, and provide access control for patient records based upon worker identity and entitlements. For example, VDI can support physicians with “follow me” capabilities that retain desktop state as physicians roam from patient to patient and workstation to workstation during their rounds. Desktop virtualization is also helping hospitals comply with HIPAA privacy rules by moving desktop images to a centralized data center, eliminating any data stored on endpoint devices and consolidating event logs for controls monitoring, oversight, and auditing.
- **Help educational institutions balance personal freedom and control.** Universities tend to give students the freedom to choose the PC they want and use Internet resources for academic and recreational purposes. Unfortunately, this philosophical model can also exacerbate security events, desktop support costs, and network traffic management headaches. Desktop virtualization is increasingly seen as a way to balance these diverse objectives. Rather than manage individual systems and users, universities can create a few virtual desktop image types used by faculty, staff, and students. Each group uses this image for academic or administrative purposes only, while maintaining a completely different desktop environment for personal use. This creates a “firewall” between institutional and recreational computing, helping to reduce security incidents, streamline PC configuration management, decrease help desk calls, and diminish IT operations costs.
- **Public sector organizations need scale and agility.** For large state and federal government agencies, PC management has become nearly impossible—many now report that this burden is impeding their organizational mission. In this case, desktop virtualization is being seen as a potential “game changing” technology that makes it much easier to support users, modernize IT infrastructure, and roll-out new common applications. This is especially important as state and federal agencies seek to deliver e-government applications that make it easier for citizens and private sector organizations to do business with the government.

## What About Security?

Desktop security is extremely difficult today and desktop virtualization is viewed as a potential solution. This makes sense since desktop virtualization can help large organizations control desktop configurations, manage vulnerable software, deploy patches, and limit user behavior. Yes, this can certainly address some of the challenges large organizations face today, but ESG believes this is just a start. While desktop virtualization can help lock down PC configuration and centralize data, several security challenges remain, such as:

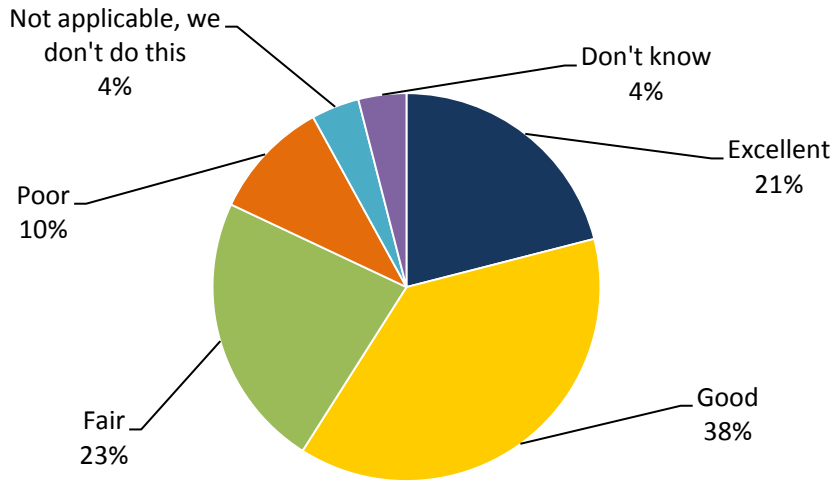
- **Data discovery and classification.** Whether it is stored on a laptop, USB flash drive, or enterprise file server residing in the data center, it is impossible to protect confidential data if no one knows it is there. The only way around standard guesswork is through data discovery and classification—unfortunately, this isn't always easy. According to ESG's research, one-third of security professionals believe that their organization is either “fair” or “poor” at classifying and tracking the movement and copying of confidential data (see Figure 3).<sup>4</sup> Desktop virtualization does little to rectify the obvious security vulnerability.

---

<sup>4</sup> Source: ESG Research Report, *Protecting Confidential Data Revisited*, April 2009.

Figure 3. Adoption of Virtual Desktop Infrastructure Technology

In your opinion, please rate your organization's performance in terms of classifying and tracking the movement and copying of confidential data.  
(Percentage of Responses, N = 308)



Source: Enterprise Strategy Group, 2009.

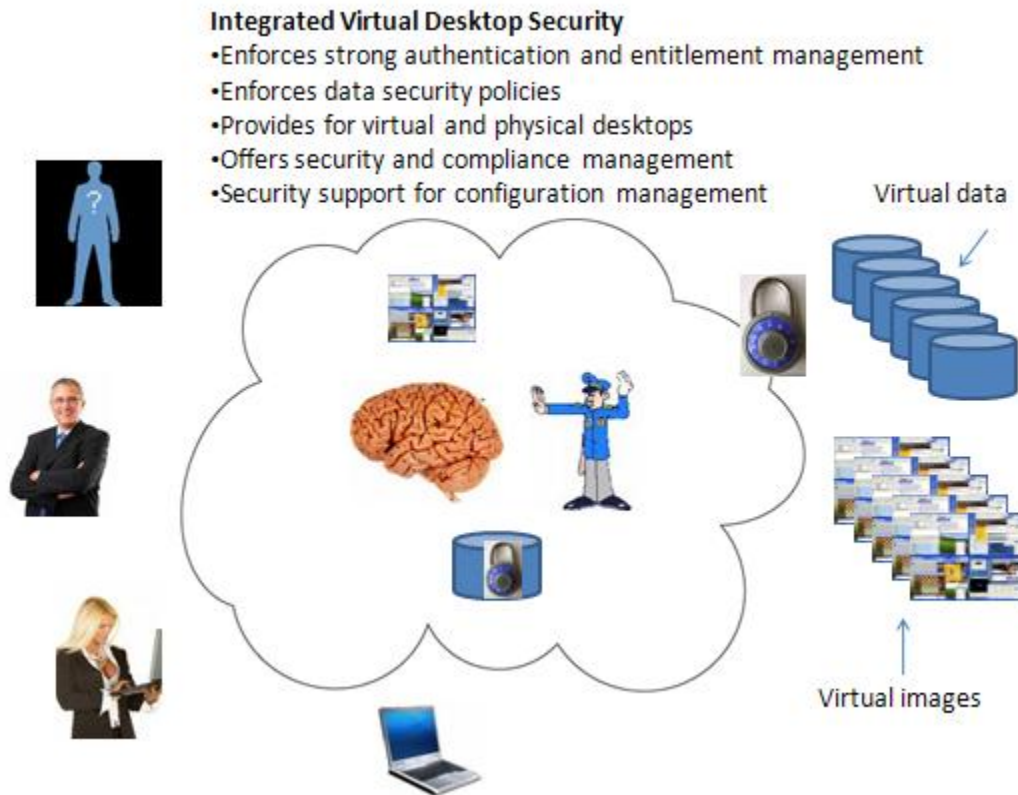
- **Strong authentication.** With users accessing their entire desktop over the network, weak authentication can give hackers and social engineers easy entrée to the “keys to the kingdom.” Additionally, industries like health care are looking to desktop virtualization as a way to personalize services and secure PCs while meeting compliance mandates and optimizing shared resources. This can only be accomplished if desktop virtualization is deployed with identity-based services and if strong authentication is designed into the final solution.
- **Log, event, and security management.** In a virtual desktop environment, dozens of user desktop images can share a common server platform. This is great for consolidation, but how will IT track user access and behavior? Without this visibility, it is hard to imagine how desktop virtualization can support regulatory compliance requirements.
- **Integrated configuration management.** Disparate users need different desktop images, software patches, and configuration management, regardless of whether they use a physical laptop or a virtual desktop image stored in the data center. Central configuration management for both physical and virtual desktops is essential here to reduce operations overhead, ease physical to virtual migrations, and standardize the user experience.

If security functionality like this is tightly integrated into the desktop virtualization environment, it can actually enhance overall enterprise security. How? By centralizing security policy creation, monitoring, and enforcement. This alone should persuade organizations to evaluate desktop virtualization technology soon.

## Security Must have Virtual Intelligence and Integration

Desktop virtualization has the potential to simplify PC support and management, but without the proper security controls, it can only be used as a niche solution for a small percentage of users. To overcome this issue, security tools must be tightly integrated with virtualization technology, acting as both a traffic cop and policy management brains between users, data, and virtual images in order to enforce security policies (see Figure 4).

Figure 4. Adoption of Virtual Desktop Infrastructure Technology



Source: Enterprise Strategy Group, 2009.

To accomplish this goal, integrated virtual desktop security must:

- **Track virtual desktop images.** Security tools must be able to see and track virtual desktop images as they are created, backed up, or moved from one server to another.
- **Control identity.** Security tools must be able to inspect user credentials and map them to virtual image access and application privileges.
- **Understand the data.** DLP functionality like data discovery, classification, and policy enforcement must understand the relationships between data, identity, and virtual infrastructure. When multiple user images are accessed from a single server, DLP must allow the Chief Legal Counsel to send confidential documents to an external attorney while preventing an HR administrator from e-mailing the employee database to a head hunter via her Hotmail account.
- **Follow virtual and physical activities in devices and applications.** Security management systems must be able to monitor and correlate user behavior, system activities, and application intelligence down to virtual images and VM movement across servers and networks.
- **Orchestrate configurations.** Desktop virtualization certainly eases this task, but it is still important to manage the creation and updating of virtual images. Security tools must play a role in configuring, distributing, and monitoring hardened virtual image configurations and patch management.

It is also important for security tools to provide comprehensive management coverage across virtual AND physical desktops. This is essential since most organizations will continue to have a mixed environment of virtual and physical devices with constant migration back-and-forth based on application needs and mobility requirements. A “single pane of glass” for security tasks will help improve both IT and security operations.

One vendor to consider for these requirements is RSA, the security division of EMC, since RSA is working with VMware to integrate security into VMware View environments for desktop virtualization. VMware describes View as “a universal client” that combines different devices, multiple platforms, and legacy and web-based applications. RSA enhances this personalized virtual desktop solution with tight integration of its DLP (RSA Data Loss Prevention Suite), security/compliance management (RSA enVision), and identity management (RSA SecurID). This integration enables the virtual intelligence requirements described above. In addition to the RSA pieces, parent company EMC also adds value to the mix. For example, EMC Ionix provides operations management tools for physical and virtual environments while EMC also provides indispensable enterprise products and service pieces needed to create a virtual desktop infrastructure in the data center. Given these many qualifications, RSA should be strongly considered as a vendor capable of providing the “security glue” for desktop virtualization deployment.

## CIO To-Do List

Desktop virtualization may help simplify desktop management and even improve security, but it is not a panacea by any means. To maximize the operational and security benefits of desktop virtualization, CIOs should:

- **Contemplate all potential cost implications of virtual desktops.** It is important to recognize that TCO and ROI calculations extend beyond the technology and IT infrastructure necessary to support desktop virtualization deployments and, as such, are not limited to a structured system for calculating “success metrics.” ESG has witnessed several initial desktop virtualization deployments judged largely on their abilities to solve bigger business issues and provide operational improvements. For instance, a financial institution was able to leverage desktop virtualization to support local developers without having to build a new overseas data center.

It is also important that all costs associated with various desktop virtualization solutions, in terms of additional investments and savings, are considered in the evaluation process. While, in some cases, data center infrastructure may need to be upgraded to accommodate centralized desktop computing, more often than not, existing technology assets can be leveraged to provide optimum efficiency. Users also recognized single image management as an improved method to maintain one instance and update all virtual desktops simultaneously. This not only reduces the workload of IT administrators, it also helps improve desktop security and user satisfaction.

- **Sell desktop virtualization internally.** Consistent with prior research on the topic of desktop virtualization, ESG discovered that the primary advocates of VDI adoption within organizations were typically high level IT managers and even CIOs. This is a great start, but ESG suggests that IT executives take this strategy to the next level and sell desktop virtualization internally to business and executive management. For example, health care CISOs should advocate desktop virtualization and strong authentication as a way to maximize IT investment in shared workstations while providing for personalized services for health care workers and easing regulatory compliance management. In this way, desktop virtualization can help enable business initiatives, not just cut IT costs.
- **Look for integrated solutions.** Virtual desktop infrastructure projects will fail if approached like science projects. Yes, VDI is an evolving technology, but it is important to look for comprehensive suites from enterprise-class vendors that provide technology and partner solutions for configuration, management, monitoring, and security. Remember that desktop virtualization may have many different flavors, so work with vendors that support flexible rather than draconian virtualization models. Make sure virtual desktop vendors have lots of partner support, existing references, and a visionary roadmap.

Finally, it is important to keep in mind that like any IT technology, VDI is ultimately a business solution. CIOs that build desktop virtualization solutions that fit with IT and business initiatives and support user demands for a high

performance personalized workspaces will ultimately make desktop virtualization a successful part of their IT and business strategies.

## **The Bigger Truth**

While server virtualization has lots of market momentum, desktop virtualization may become far more broadly implemented over time. Why? Today's users are mobile, Internet-savvy, and work with multiple devices. What's more, wired and wireless broadband networks are becoming more and more ubiquitous, providing near-global access to the Internet.

In this environment, users want their personalized desktops anywhere, anytime, and on any device. Central control and desktop virtualization have the most potential to deliver.

While the desktop virtualization future seems clear, ESG believes that there are still lessons to be learned. As the philosopher George Santayana said, "Those who cannot learn from history are doomed to repeat it." If security is an afterthought as it has been in the past, IT will find itself perpetually catching up to security problems in a dynamic, virtual world. However, if security is "baked into" desktop virtualization solutions from the start, it will be more effective and more manageable throughout the desktop virtualization lifecycle.



Enterprise Strategy Group | **Getting to the bigger truth.**