

White Paper

Understanding and Enhancing Virtual Desktop Security

By Jon Oltsik, Principal Analyst

June, 2010

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Contents.....	2
Executive Summary	3
PC Management Chaos.....	3
PC Problems are Driving Desktop Virtualization	5
Desktop Virtualization Offers Business Benefits	6
Desktop Virtualization Can Improve Endpoint Security	6
Endpoint Security Software Needs Virtualization Intelligence	7
Trend Micro OfficeScan: A Model Product for Desktop Virtualization	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..

Executive Summary

Desktop virtualization isn't a mere fad or industry hyperbole. ESG research indicates that large organizations are actively deploying desktop virtualization technology today or plan to do so in the next 12 to 18 months.

This brings up a plethora of questions. Why are enterprises jumping on the virtual desktop bandwagon? How are they measuring success? What about endpoint security? Many CISOs consider endpoint security a chaotic mess. Will desktop virtualization make this situation better or worse—and why? This paper concludes:

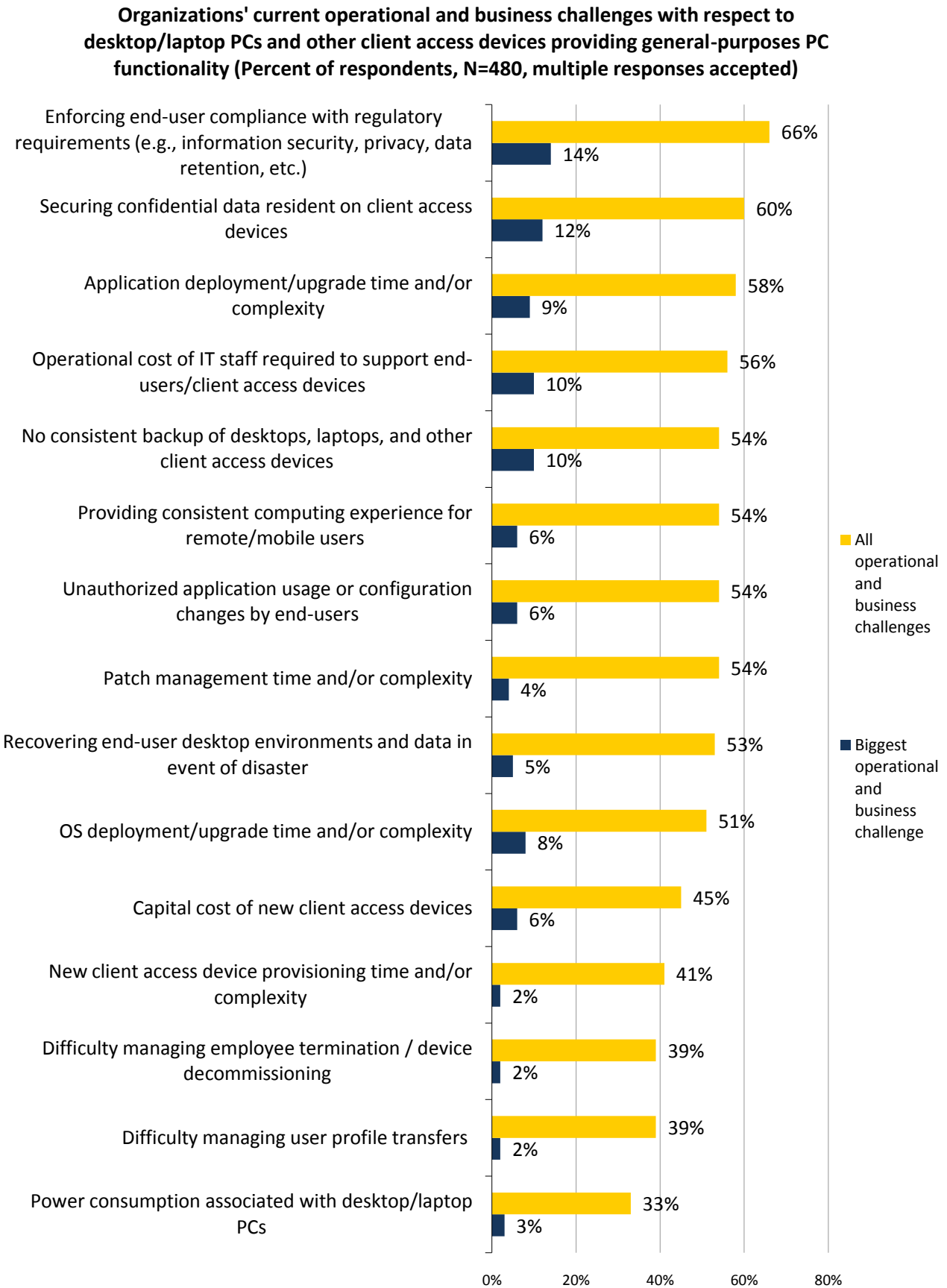
- **Like server virtualization, virtual desktops promise a steep payback.** Large organizations throw a lot of money at PC provisioning, configuration management, patch management, and support. Desktop virtualization has the potential to streamline these processes, reduce costs, and enable large organizations to greatly improve PC governance. This alone is driving a lot of virtual desktop interest and implementation.
- **Desktop virtualization can actually improve endpoint security.** By reducing the variation of PC configurations, simplifying patch management, adding white listing capabilities, and monitoring VM to VM traffic on servers, desktop virtualization can reduce endpoint security firefighting and thus reduce risks.
- **Endpoint security tools need virtual intelligence.** Today's endpoint security software was designed and developed to consume resources on physical PCs not shared servers and storage. This makes existing endpoint security obsolete at worst and a mismatch for virtual desktop infrastructure at best. Large organizations need new endpoint security tools that can distinguish between physical and virtual desktops, minimize resource consumption for system scanning and updates, offer common management for physical and virtual systems, and tightly integrate with virtual desktop infrastructure management and operations tools.

PC Management Chaos

Managing hundreds or thousands of PCs has never been more difficult than it is today. Historical problems with PC provisioning, configuration management, and software distribution have been exacerbated by more pressing concerns about patch management, data security, regulatory compliance, and malicious code attacks. According to ESG's research, large organizations believe that PCs present a constant challenge for IT, especially around compliance, security, and operating costs (see Figure 1).¹

¹ Source: ESG Research Report, [Virtual Desktop Infrastructure Market Trends](#), February 2009. All statistics are from this report unless otherwise cited.

Figure 1. Most Significant PC Challenges



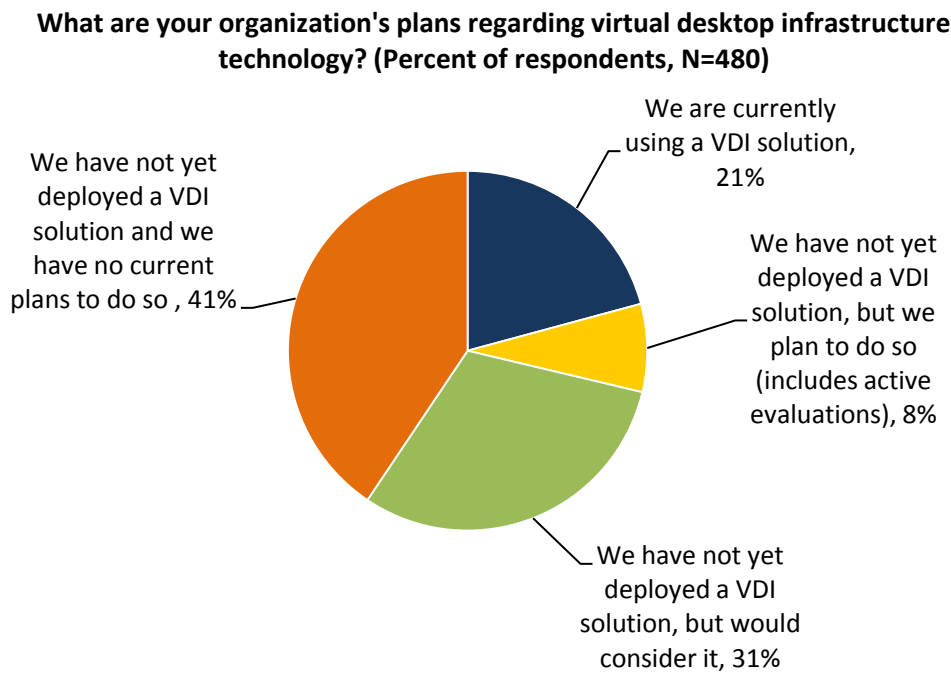
Source: Enterprise Strategy Group, 2009.

PC Problems are Driving Desktop Virtualization

PC chaos is nothing new—IT managers have tried to alleviate the time and costs associated with redundant, labor-intensive PC management tasks for years. How? With a parade of centralized management tools and security safeguards aimed at making PC management more cost effective, safer, and operationally efficient. CIOs deserve credit for their perseverance, but unfortunately, none of these solutions effectively tamed the PC beast. PC management and operations is as difficult as ever.

Given the measurable benefits of server virtualization, many organizations believe that desktop virtualization technology may represent their best hope to finally bring order to perpetual PC anarchy. In fact, a large number of enterprises are already engaged in virtual desktop research, testing, and deployment. ESG research indicates that 21% of large organizations (i.e. 1,000 or more employees) 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). Most desktop virtualization implementations are 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 will change dramatically as firms move virtual desktop infrastructure (VDI) projects from proof-of-concept to full production. Nearly half (45%) of VDI users expect to virtualize more than 50% of their client access devices over the next three years.

Figure 2. Adoption of Virtual Desktop Infrastructure Technology



Source: Enterprise Strategy Group, 2009.

Desktop Virtualization Offers Business Benefits

Beyond lower costs and simplified PC management, ESG sees additional drivers for desktop virtualization. PCs can take five minutes or more to boot up and buggy PCs often cause performance degradation, leading to problems with employee morale and productivity. Desktop virtualization promises a better user experience with instant access, consistent performance, and user personalization. Furthermore, desktop virtualization aligns with other network-centric technology trends such as Web 2.0 applications, interactive content, mobile device proliferation, and cloud computing. Because of these trends, desktop virtualization has become especially useful for specific industry requirements. For example:

- **Health care organizations look to desktop virtualization for improved productivity.** In many health care facilities, PCs are shared resources (a.k.a., “workstations on wheels”) that must provide customized services for physicians, residents, and nurses. Desktop virtualization offers a new type of solution to centralize the management of applications, allow for improved personalized services, and provide access control of patient records based upon worker identity and entitlements. 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 also helps hospitals comply with HIPAA privacy mandates by moving desktop images to a centralized data center.
- **Manufacturing companies want automation without PC operations overhead.** Many manufacturing companies run specialized applications for testing, measurement, or process automation. These applications tend to run on Windows PCs, but don’t need the functionality or operations burden associated with a fully-functional system. Since desktop virtualization reduces the need for PC maintenance and management, manufacturing companies can get the benefits of process automation while minimizing security vulnerabilities or IT management costs.
- **Public sector organizations are focused on reducing costs.** For state and local government agencies, PC management requires personnel, skills, and tasks that they can no longer afford. 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. States with broadband networks can now manage virtual PC images as a service for distributed agencies and local governments.

On a broader scale, large organizations are virtualizing Windows 7 instances on central servers and then delivering desktop virtual images over the network. In this case, desktop virtualization helps enterprise companies eliminate the cost and effort needed to upgrade physical PCs. Once the virtual desktop infrastructure is in place, Windows 7 is transformed from a PC upgrade to a network service.

Desktop Virtualization Can Improve Endpoint Security

Clearly, desktop virtualization has the potential to help organizations improve PC operations, reduce costs, and enable network-centric business processes, but what about security? After all, server virtualization delivers similar benefits, but moving physical server security zones to a virtual infrastructure isn’t easy. Are there similar security hurdles for desktop virtualization?

ESG believes that the opposite is true: with proper planning and deployment, desktop virtualization can actually improve endpoint security. Smart CIOs will use desktop virtualization as an opportunity to address today’s security issues by using:

- **Standard virtual images.** With thousands of physical PCs, many large organizations have generations of various systems with different configurations and applications. This creates a nightmare for help desk staff tasked with patching, securing, and supporting a potpourri of PCs for assorted users and groups. Many of these problems can be alleviated by creating a standard virtual desktop “golden image” with a common configuration and set of applications. This greatly reduces PC firefighting as changes made to a golden image are immediately integrated into each and every virtual desktop. Imagine how much time you’d get back if you could patch a single golden image instead of 10,000 PCs?

White listing. Employees tend to view their corporate PC as a personal device. Corporate data and applications commingle with social networking sites, iTunes libraries, and personal Web use, leaving sensitive data and corporate assets at risk. Desktop virtualization addresses this risk with a restricted corporate desktop image armed with white listing for policy enforcement. Employees can utilize their physical PC resources and Internet access only (i.e. Port 80) for personal use while their corporate tasks are executed on a tightly-managed and fixed virtual image. This is a win-win for enterprise organizations: employees can continue to use their PCs for personal use and entertainment, but since this activity is isolated from corporate use, overall security risks diminish.

- **Centralized storage for PC data.** Even with the best DLP tools, it is difficult to discover and classify sensitive data when it sits on thousands of PCs throughout the enterprise. Desktop virtualization centralizes all storage in the data center, making it easier to scan disks, discover and classify data, and enforce acceptable use policies.
- **VM to VM visibility.** In a virtual desktop environment, 25 to 60 desktop images will run as VMs on a single physical server. When one of these desktop images is compromised and begins scanning other systems, anomalous traffic spikes consume resources, setting off systems management tool alarms. By isolating this traffic on a single physical server, IT operations and security professionals will be able to detect anomalies, isolate issues, and remediate problems much more rapidly.

Endpoint Security Software Needs Virtualization Intelligence

Desktop virtualization has some inherent qualities that can help improve today's haphazard endpoint security, but it is still vulnerable to increasingly sophisticated malicious code and a growing global network of cybercriminals. Since virtual desktops simply emulate physical systems, these threats could be addressed by simply installing endpoint security software from an assortment of vendors on each virtual image. Wouldn't this work?

Yes and no. It would work in principle, but current endpoint security software was designed for the captive resources of physical PCs rather than shared CPU, memory, and network resources across a common server platform. It is not unusual for security software system scans to utilize between 40% and 60% of the CPU for a period of time. Given this, a single full system scan of a virtual desktop image could impede the performance of all other resident virtual machines while simultaneous scans of several virtual desktops collocated on the same server could make all other resident virtual desktops unusable. In spite of desktop virtualization benefits, the CEO will likely get extremely angry when her PC stops functioning when the scheduled security scans begin at 1pm.

To alleviate these issues, endpoint security software must be redesigned with deep virtual intelligence (see Table 1). This means: understanding the difference between virtual and physical desktops, and applying security policies and defenses accordingly.

Table 1. Requirements for Virtual Desktop Security

Requirement	Physical Desktop	What's Needed for Virtual Desktop Support
Resource utilization	Assumes captive resources. Generally consumes hundreds of megabytes of memory and GB of disk. Can consume 40% to 60% of CPU cycles for scanning.	Must assume shared resources and reduce resource consumption in all cases.
System scanning	IT typically configures systems to scan at the same time. Full system scans scan all files.	Must recognize virtual desktop and serialize scans to minimize resource utilization. Full system scans should only scan content that is incremental to the standard "golden image."
Provide common management of physical and virtual desktops	Assumes physical systems only.	Recognizes physical and virtual desktops. Provides common command-and-control and policy management. Adjust enforcement according to physical or virtual footprint.
Integration with virtual desktop management and operations	Assumes physical systems only.	Integration for virtual desktop provisioning, change management, and movement.

To support both physical and virtual desktops, endpoint security must:

- Decrease resource utilization.** Legacy endpoint security consumes hundreds of megabytes of memory, constant CPU cycles, and gigabytes of disk space for an ever-growing database of malware signatures. This makes no sense when virtual desktops share system and storage resources. To accommodate desktop virtualization, endpoint security must evolve from an application to an agent. This means calling for common resources and services (like a common anti-malware signature database) when needed rather than consuming captive resources at all times.
- Alter system scanning.** As previously mentioned, system scanning can have a profound impact on the performance of all virtual desktop images on a common server. To address this, system scanning must be throttled and serialized to use as little time and system resources as possible. Since virtual desktops share a common golden image, endpoint security can become more efficient by scanning the golden image once and then limiting individual virtual desktop scans to any additional applications or files only.
- Provide common management across physical and virtual assets.** Even the most aggressive organizations will increase the population of virtual desktops over time while continuing to support physical systems for power users and mobile road warriors. Since enterprises will have a mix of desktops for the foreseeable future, they will need endpoint security tools capable of managing physical systems, virtual images, or physical to virtual PC migrations.
- Integrate with virtual desktop management systems.** Using tools like [VMware's VMotion](#), virtual desktops will move from one physical server to another based upon server utilization metrics, maintenance requirements, and disaster recovery policies. Endpoint security tools must be aware of this movement in order to identify virtual desktop instances, alter scanning schedules, and apply policies.

To share malware signatures and address increasingly virulent malware, endpoint security will be supported by a new model commonly referred to as a hybrid cloud. Rather than "owning" their own malware signature database, virtual desktops will share a common database hosted on a virtual appliance. Just as in the current model, this database will receive regular signature updates, but in this case, one update will support all local images. Local signature databases will also rely on the cloud as a layered defense for zero-day anti-malware protection. When a virtual desktop is "checked out" for mobile use, users will rely solely on an up-to-date signature database in the cloud for protection.

Trend Micro OfficeScan: A Model Product for Desktop Virtualization

Many endpoint security vendors are reacting to the desktop virtualization trend and promise redesigned products offering virtual intelligence in the future. Alternatively, [Trend Micro](#), a leading provider of endpoint security software, anticipated the popularity of virtual desktop infrastructure and responded with OfficeScan 10.5. This new release marries Trend’s leading security protection with virtual intelligence as it:

- **Addresses resource limitations.** OfficeScan 10.5 adjusts typical system scanning tasks for virtual desktops running on common servers. For example, full system scans are serialized to minimize the impact of overall system (server) performance (see Table 2). Trend follows the same process with client updates, where it will only update a configurable number of virtual desktops per server at the same time. Finally, OfficeScan can pre-scan and white list the elements of a base “golden image” virtual desktop. Once this is done, OfficeScan performs only incremental scans of deviations from the base image.
- **Provides common management across virtual and physical systems.** As stated previously, this is critical: no enterprise organization wants multiple endpoint security management platforms. With OfficeScan, virtual and physical systems can be managed with common policies and configurable enforcement flexibility based upon whether desktops are physical or virtual.
- **Creates a roadmap for VDI management integration.** Future versions of OfficeScan will integrate with VDI management tools for vMotion support.

Table 2. OfficeScan Efficiencies for Virtual Desktop Infrastructure

	Physical Desktop Security Tools	OfficeScan 10.5	Difference
Scan Time	Approximately 15 minutes	Approximately 4 minutes	73% reduction in time needed for system scan
CPU utilization	Approximately 30%	Approximately 5%	83% reduction in CPU cycles
Disk space	Approximately 30 MB	Approximately 1 MB	96% reduction
Memory	Approximately 2 GB	Approximately 200 MB	90% reduction

Given its efficient use of resources with system scanning and updating each client, OfficeScan can enable a higher ratio of virtual desktops per physical server. ESG estimates that this level of scanning efficiency can increase the number of virtual desktops that can be run on each server for day-to-day use significantly, and even a relatively small increase can lead to large savings in capital and operating costs for a large enterprise. Early Trend Micro research indicates that using OfficeScan 10.5 can more than double the number of virtual machine scans possible on a single physical server.

Finally, OfficeScan is tightly integrated with the Trend Micro Smart Protection Network, a hybrid cloud architecture built to reduce its software client footprint, pool anti-malware databases, and back on-site protection with cloud-based resources.

With its overall virtual intelligence, reduced resource utilization, and hybrid cloud architecture, Trend Micro OfficeScan 10.5 should be on every CIO’s short list for virtual and physical desktop security.

The Bigger Truth

If implemented correctly, virtual desktops can look like physical systems while delivering better performance, security, and user experience. While this is true, it is important to remember that the underlying technology is vastly different and needs to be treated as such.

Today's endpoint security tools were designed for physical systems. As PC processors, memory, and storage increased, most endpoint security tools consumed more and more resources. This model won't work in a virtual desktop environment run on top of shared services. Clearly, new endpoint security with virtual intelligence is needed. As stated above, virtual desktop security demands more efficient resource utilization for scanning and client updates. Actual scans must be adjusted to accommodate the unique needs of virtual desktops running on shared servers. Endpoint security must also support virtual and physical footprints while integrating with virtual infrastructure tools like vMotion.

IT managers should also look to add to their layered defenses by backing endpoint security software and on-site appliances with a cloud-based layer of ubiquitous real-time protection.

A virtual desktop infrastructure, combined with endpoint security tools designed with virtual intelligence, can transform today's chaotic desktop security into a well-managed, policy-based architecture. Savvy CIOs will recognize this opportunity, partner with endpoint security leaders like Trend Micro, and get started on their virtual desktop journeys soon.



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