White Paper

VDI-Centric Endpoint Security Can Help Lower Costs and Increase ROI

By Jon Oltsik, Senior Principal Analyst

June 2012

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

Contents

Executive Summary

In August of 1981, IBM introduced its model 5150 personal computer complete with an Intel processor and operating system from a little-known Seattle-based software company named Microsoft. Henceforth, enterprise endpoint computing has been all but equated with Windows and Intel-based desktop and laptop PCs deployed across the network. Over the past few years, however, the endpoint computing model has begun to change in several ways. One visible new endpoint computing model is called Virtual Desktop Infrastructure (VDI). Instead of running the Windows operating system and applications and storing files locally on a physical PC device, VDI serves up desktop images as a managed service typically running on servers in data centers.

Is VDI gaining momentum or does it represent yet another empty threat to Wintel hegemony? VDI carries many benefits around business agility, but can be costly to deploy. Do the benefits outweigh the costs? Furthermore, what about endpoint security? Does VDI address or ignore the multitude of endpoint security challenges that organizations face and how does security impact VDI costs and ROI? This paper concludes:

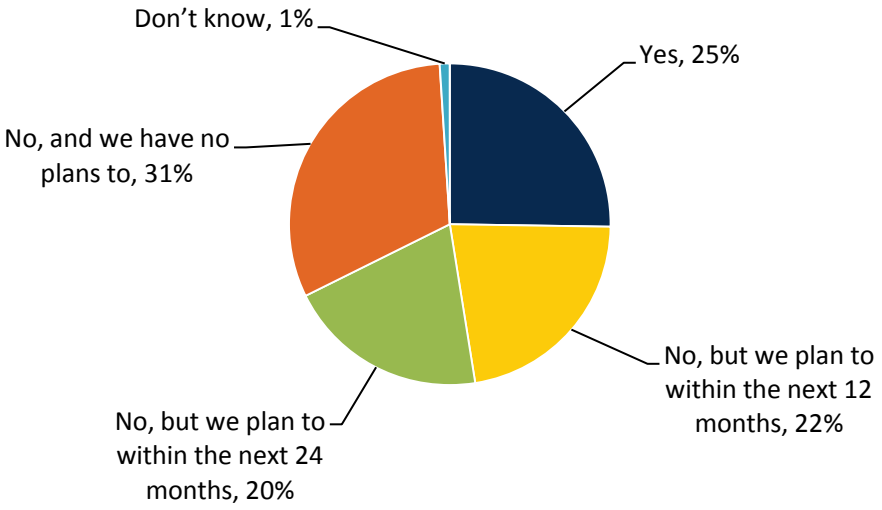
- **Many organizations are moving forward with VDI.** Over the past two years, ESG Research reveals that IT professionals have identified VDI as one of their top 10 IT priorities. CIOs are embracing VDI to establish better controls in areas such as PC deployment, configuration management, patch management, and data backup. VDI is also perceived as saving costs by reducing administration, and extending PC refresh cycles, etc., but projects usually carry startup investments associated with data center infrastructure, increased management and training, and other implementation expenditures. VDI projects tend to center on specific business functions like call centers while VDI adoption is most pronounced in industries such as health care, education, retail, and manufacturing. Small pilot projects often lead to wider deployment over time.
- **VDI security is a mixed bag.** On the one hand, VDI can help improve endpoint security by locking down PC configurations to specific "gold images," and replacing distributed vulnerability scanning and patching with more easily controlled central processes. Offsetting these benefits however, legacy endpoint security software remains antithetical to VDI design. Why? Legacy endpoint security software assumes a physical PC—not a virtual machine (VM) image—running on a shared server. Because of this misalignment, legacy endpoint security software must be installed on each virtual desktop, which consumes an inordinate amount of server resources. Furthermore, security scanning of multiple VMs collocated on a server can drastically impact server performance. Finally, organizations can easily deploy insecure or non-compliant VDI images outside of the purview of legacy endpoint security software. This increases IT risk and could lead to a successful malware attack, a compromised system, or a data breach. And the impacts of legacy endpoint security software on resources, performance, and VM densities can also increase the ongoing cost of VDI projects.
- **Organizations need VDI-centric endpoint security.** Legacy endpoint security software is a compromise at best. To maximize VDI benefits while addressing IT risk, enterprises need a VDI-centric security software designed for the unique properties of VDI. VDI-centric security tools should be integrated into hypervisor APIs to gain deep virtual intelligence. This changes the architecture in fundamental ways–instead of running security software on each VM, VDI-centric security operates as a virtual machine with visibility and oversight over all VDI images. In this way, VDI-centric security greatly reduces resource contention while improving overall VDI security with greater control and additional layers of defense. With lower resource usage, VDI-centric endpoint security can increase VM densities and improve the ROI of VDI projects, while still maintaining strong security.

VDI Benefits and Costs

While not as popular as server virtualization, VDI projects continue to make steady progress at many enterprise organizations. In fact, VDI was identified as a top 10 IT priority in ESG's annual IT spending intentions research survey in both 2011 (#6) and 2012 (#8). Early projects were focused on local users with high-speed LAN connections, but ESG research indicates that VDI is branching out beyond the corporate headquarters—25% of midmarket (i.e., 100 to 999 employees) and enterprise (i.e., more than 1,000 employees) organizations are already using VDI technology to support WAN-connected remote office/branch office workers while another 42% plan to use VDI technology to support WAN-connected remote office/branch office workers within the next two years (see Figure 1)[1].

Figure 1. Midmarket and Enterprise Organizations are Using VDI to Support ROBO-based Employees

Is your organization currently using desktop virtualization technology to replace ROBO employees' local desktop/laptop PCs with virtual desktops running in a central location, such as a corporate data center? (Percent of respondents, N=454)



Source: Enterprise Strategy Group, 2012.

VDI's success should come as no surprise since this technology can provide measurable benefits such as:

- **Improved IT service and support.** VDI brings distributed PC support to a central location—the data center. This centralization can help accelerate PC provisioning, improve patch management processes, and ease the cost of supporting an army of widely distributed PCs.
- **Lower PC hardware costs.** Since VDI execution is done on data center resident servers, PCs are relegated to the role of network terminals, rendering a VDI image over IP networks. This is a relatively easy technical chore allowing organizations to extend the useful life of PC hardware beyond today's 2 to 3 year replacement cycle.
- **Provide ubiquitous network access to business and specialized desktop images**. VDI disaggregates employee workspaces from physical boxes. As a result, workers are able to access their corporate desktop from any PC, anywhere, at any time. This also alleviates the need to back up distributed PCs over busy corporate LANs, or scramble to re-image a system when an employee's PC is lost or stolen. Given this network connectivity model, organizations can also use VDI to create images for specialized use cases like retail kiosks, shared health care workstations, or user self-service applications.

The key to VDI's success is really rooted in its ability to centralize and standardize PC management tasks. Upon each month's "Patch Tuesday," it is far easier to create a standard operating system "gold image" for 100 VDI users

[1] Source: ESG Research Report, *Remote Office/Branch Office Network Trends*, July 2011.

than to distribute patches and then configure and update 100 distributed PCs. In this way, VDI can help reduce PC maintenance, operations, and support costs.

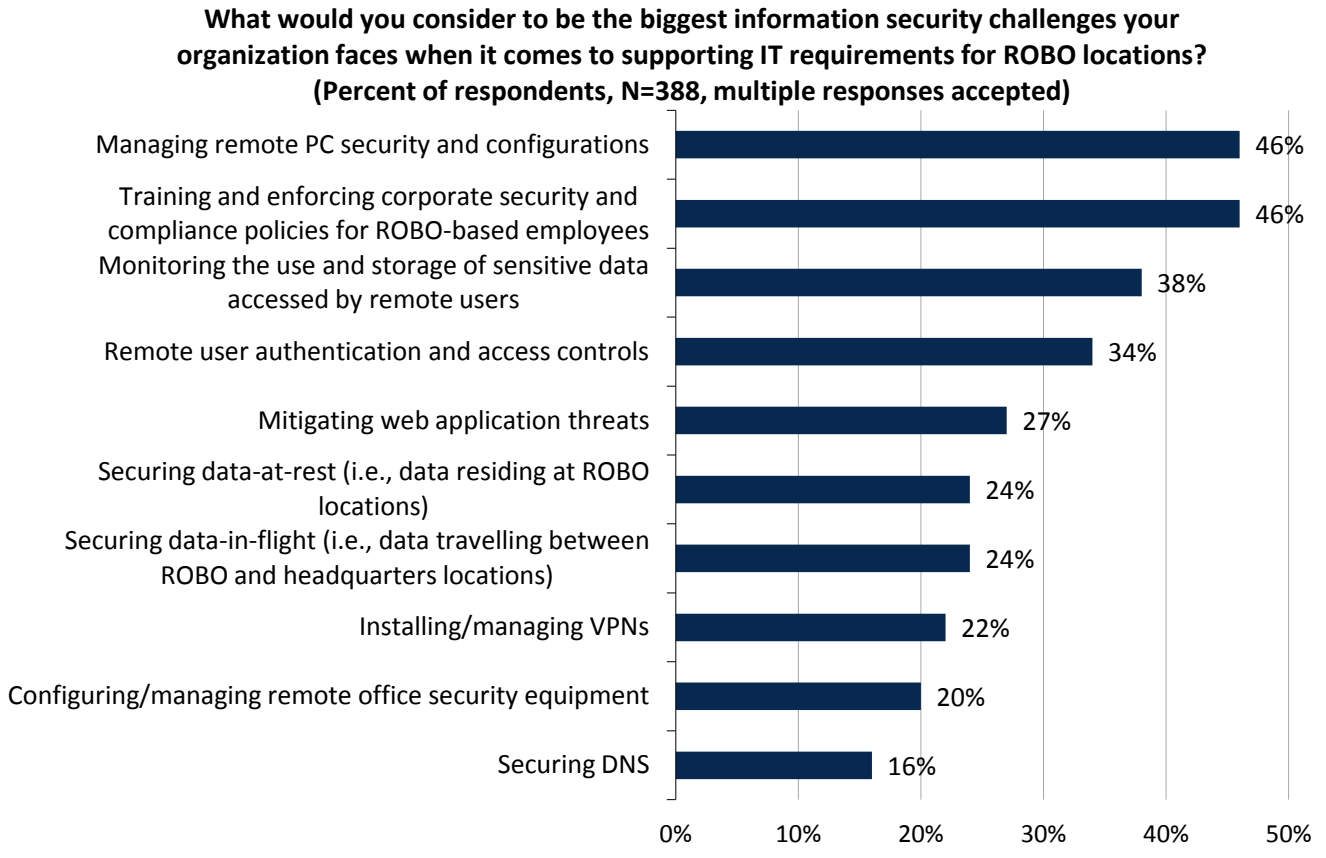
Before jumping into VDI however, organizations must also factor in additional costs. For example, VDI replaces individual PCs with shared servers, storage, and networks in the data center. LAN and WAN bandwidth requirements may also increase. VDI may place new demands on the IT staff as it deploys VDI infrastructure, supports pilot projects, and invests time in VDI training. Finally, operating system and PC application licensing fees can increase when deployed as VDI. These initial costs may eventually be offset by ongoing VDI efficiencies, but organizations should account for initial VDI costs in their implementation assessments.

Given these trade-offs, CIOs should do extensive research and planning in preparation for any VDI project. As a general rule ESG finds that VDI delivers strong ROI when it is applied to a sub-segment of the employee population working in areas such as call centers, order entry, new student "desktops," or health care patient services. Focused initial VDI projects often provide valuable experience that can accelerate ROI benefits as the VDI footprint expands over time.

What about Security?

Beyond PC lifecycle extension and help desk costs, bolstering endpoint security is often cited as a primary VDI driver. For example, ESG research illustrates that many organizations are adopting VDI to support remote office/branch office workers. One of the primary reasons behind this decision is that Windows PCs residing in ROBO locations create a number of security challenges leading to increased risk for the entire organization (see Figure 2)[2]. VDI can act as a solution to many of these challenges.

Figure 2. VDI Is Used To Address Security Challenges for ROBO Locations



Source: Enterprise Strategy Group, 2012.

[2] Ibid.

Through standardization and central control, VDI addresses a lot of the volatility that makes endpoint security so difficult. VDI "gold images" are easier to scan for vulnerabilities and patch. Application controls are centrally managed, and antivirus signature distribution takes place within the friendly confines of the data center.

Endpoint Security Software Remains an Achilles Heel

While central VDI management and operations can help improve PC security, it also introduces a new set of issues that center on legacy endpoint security software. Why? Legacy endpoint security software was designed to run on a physical PC with exclusive access to its resources (i.e., CPU, memory, and storage). Therefore, when legacy endpoint security software runs in a VM residing on a shared server, it can lead to problems because:

- **Each VM requires its own software agent.** Rather than take advantage of the common hypervisor, legacy endpoint security software must be deployed, configured, and managed on every VDI instance. Other than data center collocation, the security team gets none of the operational benefit associated with VDI centralization. Additionally, endpoint security agents consume a fair amount of server resources, limiting the ratio of VMs per physical server. This alone reduces VDI efficiency.
- **Legacy endpoint security tools can't keep up with VDI agility.** Whether it's for server virtualization or VDI, provisioning a new VM is as simple as a few mouse clicks. Unfortunately, this can lead to negative repercussions around endpoint security. A VDI image may not be configured properly. Critical software patches or the latest antivirus signatures may be missing. Dormant desktop images may be way out of compliance when reactivated. Without virtual intelligence, legacy endpoint security software can only see these issues if it is installed on each VM and centrally managed. In most cases, security operations teams are forced to manage endpoint security on a system-by-system basis, rely on manual processes, and hope for the best.
- **Simultaneous endpoint security scans can disrupt server performance.** Endpoint security scans consume a lot of CPU resources as they look for malware residing in PC operating systems, applications, and files. Typically organizations run a full-system scan at least once per week. VDI creates a bit of a dilemma since physical servers may contain dozens of VDI desktop images. Security scans of multiple collocated desktop images could easily utilize 80% of CPU capacity, leaving 20% or less for dozens of other endpoint images. Ironically, this could lead to an unintended denial-of-service condition caused by security endpoint best practices.

These legacy security issues can increase IT risk and impact the short-term efficiency and long-term ROI of VDI initiatives. Clearly, these shortcomings render legacy endpoint security software as a mismatch for VDI.

Organizations Need VDI-Centric Endpoint Security

Legacy endpoint security software was designed for the PC era of endpoint computing when each user was assigned a physical PC for their personal use. Given the transition to VDI, endpoint security must be redesigned for a modern VDI-centric use case. In other words, VDI-centric endpoint security software must be designed with virtual intelligence to provide VM-level (rather than system-level) protection and support the dynamic nature of VDI provisioning, cloning, change management, and mobility. To accomplish this, VDI-centric endpoint security must include:

- **Hypervisor-level integration.** VDI-centric endpoint security software must be integrated into APIs in the hypervisor in order to gain visibility into "guest" VMs. By doing so, VDI-centric endpoint security can communicate with each VM, customize and enforce security policies on a VM-by-VM basis, and maintain an audit trail of all VMs for regulatory compliance, corporate governance, and IT audits.
- **A security virtual appliance**. Legacy endpoint security tools consume an inordinate amount of resources because they require a software agent on every VM. VDI-centric endpoint security tools alleviate this contention by offloading security software functionality to an omnipresent virtual appliance. In this design,

the security virtual appliance oversees tasks like security scans and updates for all VMs and monitors VM status to ensure up-to-date data security for new or reactivated VMs. With the security virtual appliance taking on the real security work, VDI-centric endpoint security software eschews the need for software agents on individual VMs themselves as it moves resource-intensive security operations directly to the security virtual appliance. With this design, VDI-centric endpoint security software also eliminates the problem of "scan storms" (i.e., multiple simultaneous VM-level security scans on the same physical server) by delegating the coordination of staggered security scans to the security virtual appliance.

- **Multiple security services.** With hypervisor integration and visibility into each VM "guest," VDI-centric security software can go beyond antivirus protection alone. Leading VDI-centric security software will provide additional security services such as VM-level firewalls, host intrusion prevention, and Web application protections.

VDI-Centric Security Software Benefits

By eliminating the design restrictions of legacy endpoint security tools, VDI-centric security software can deliver multiple business and IT benefits, including greater virtualization efficiency, streamlined IT operations, lower IT risk, reduced VDI costs, and higher VDI ROI (see Table 1).

Table 1. Legacy Endpoint Security Software Versus VDI-Centric Endpoint Security

Legacy Endpoint Security Issue	Ramifications	VDI-centric endpoint security alternative	Benefits
Security agent required on each VM	Consumes server resources impacting VDI efficiency	Agentless design anchored by a security virtual appliance with visibility and oversight over all VMs	Lowers resource consumption and improves VDI efficiency—reducing costs and increasing ROI
Legacy endpoint security tools can't keep up with VDI agility	New or reimaged VDI-based endpoints can be configured and deployed without the proper settings, patch levels, or security signatures	Virtual security appliance with visibility and oversight over all VMs	Accelerates detection and remediation of out-of-compliance endpoints, lowering IT risk
Simultaneous security scans of collocated VDI images	Excess resource consumption can lead to performance problems or create a denial-of-service incident	Virtual security appliance with visibility and oversight over all VMs	Centralizes and staggers VM security scans to lower resource consumption and improve VDI efficiency—reducing costs and increasing ROI

Source: Enterprise Strategy Group, 2012.

VDI-Centric Security Software from Trend Micro

The problems described above are really market-driven since most vendors continue to sell misaligned legacy endpoint security tools for VDI implementations. One exception here is Trend Micro and its Trend Micro Deep Security offering. Deep Security is actually designed for physical, virtual, and cloud-based servers and endpoints.

Trend Micro supports the VDI-centric security software model requirements described above by integrating with VMware vShield APIs. This integration enables an agentless design where VM security is anchored by a security

virtual appliance for security services such as antivirus, firewall, intrusion prevention, and web application protection, etc. Deep Security also has hypervisor-level oversight providing immediate protection for new VMs as they are provisioned, changed, or reactivated.

With its VDI-centric design, Trend Micro Deep Security can help improve VDI efficiency, lower IT risk, streamline endpoint operations, reduce VDI costs, and improve the overall ROI of VDI initiatives. Given this, CIOs may want to evaluate Deep Security as they begin new VDI projects or look to maximize ROI on existing ones.

The Bigger Truth

As the old saying goes, "if the only tool you have is a hammer, everything looks like a nail." This colorful analogy is certainly applicable to legacy endpoint security software. In this case, everything looks like a physical PC in spite of the fact that VDI virtualizes endpoints and delivers them over the network—a completely different technical architecture. Using legacy endpoint security software for VDI does not leverage the efficiencies of this environment to deliver security. Instead it negatively impacts resources and performance. This approach increases VDI costs due to the increase in infrastructure required to support VDI instances.

ESG believes a different colloquialism is more appropriate here—"choose the right tool for the right job." Legacy endpoint security is still useful for protecting Windows and physical PCs, but VDI requires another toolset. ESG suggests VDI-centric security tools with hypervisor integration, VM-level visibility, and customized and coordinated VM policy enforcement. The best VDI-centric security software will also include multiple security services for defense-in-depth protection. By leveraging the virtual environment for security, organizations receive better protection, less administrative complexity, and increased performance. VDI-centric security consumes fewer resources and increases VM densities for better ROI while delivering protection designed for VDI security challenges.

Trend Micro obviously anticipated the need for VDI-centric security by partnering with VMware, integrating with the vShield APIs, and extending its endpoint security portfolio with specific VDI support. This gives Trend Micro a great head start, making it a strong endpoint security candidate for enterprise VDI deployment. When planning VDI projects, organizations should consider evaluating Trend Micro VDI-centric security to see if it can help bolster VDI ROI and security.

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

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com