



F R O S T & S U L L I V A N

50 Years of Growth, Innovation and Leadership

How the Right Security Can Help Justify and Accelerate
Your VDI Investments:
Using Solutions from VMware and Trend Micro to Secure VDI Deployments

A Frost & Sullivan
White Paper

Rob Ayoub,
CISSP and
Global Director
of Information Security
and
Michael Suby,
Vice President of Stratecast

www.frost.com



Executive Summary	4
Introduction	4
Advantages Offered by a VDI Deployment	5
Security Challenges Related to VDI	6
<i>Performance Degradation from Resource Contention</i>	6
<i>Zero-Day Threat Environment Poses Increased Risk for VDI</i>	7
<i>Lower than Expected ROI from Poor VDI Deployments</i>	8
Common but Inappropriate Responses to these Challenges	8
<i>Randomization/Disabling of Updates</i>	9
<i>Reliance on Physical Network Infrastructure Products (IDS/IPS and Firewalls)</i>	9
How VMware and Trend Micro’s Agentless Architecture Approach Solves VDI Security and ROI Challenges	9
<i>VMware vShield Endpoint Provides the Foundation</i>	9
<i>Trend Micro Deep Security Integrates with vShield to Provide Security</i>	10
Conclusion	11

EXECUTIVE SUMMARY

Virtual Desktop Infrastructure (VDI) has the potential to be highly transformative in how IT manages desktop environments and utilizes computing resources. However, what should not be lost in VDI investigations and trials is that the entire desktop environment, inclusive of desktop security, is subject to change in structure and operation. Furthermore, if this change is not thoroughly considered, the resulting structure and operation could compromise the protective capabilities of desktop security that exists in traditional physical desktops when desktops become virtualized. Alternatively, the full strength of desktop security remains with virtual desktops but the make-or-break measurement of VDI efficiency—desktop density—is sacrificed. Neither outcome is desirable or even tolerable.

In order for maximum server density and strong desktop security to co-exist, VDI and desktop security vendors must co-develop a solution. Anything less lays out a welcome mat for the ever-lurking hacker community or restrains VDI adoption and expansion as the milestones in VDI business plans become harder to reach.

As described in this white paper, a new architectural approach has been jointly developed by VMware and Trend Micro, which brings the muscle of physical desktop security to virtual desktops while optimizing density among the virtual desktop-hosting servers.

INTRODUCTION

Modern organizations are constantly striving to improve operational efficiency. One sign of this efficiency drive is the sales of laptops exceeding desktop PCs in 2009. For organizations, this shift in PC device type improved employee productivity and organizational efficiency as the means to engage in work expanded from statically located, business day desktop PCs to anywhere and anytime laptops.

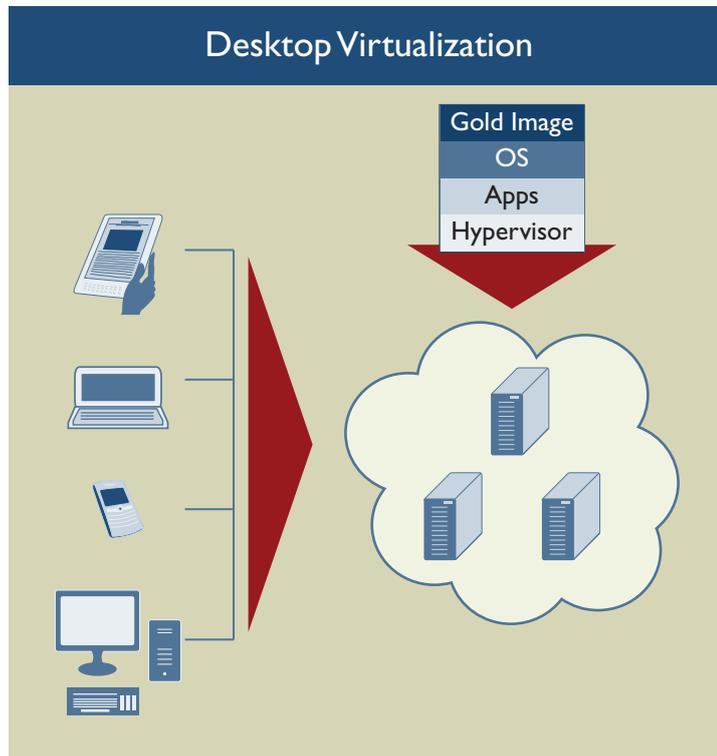
Efficiency is the holy grail of the modern enterprise. As defined by Webster, efficiency is “effective operation as measured by a comparison of production with cost (as in energy, time, and money).” Making employees and services more efficient has to involve IT. IT departments faced with a mobile workforce and tasked with improving the efficiency of employees and lowering costs have gravitated toward virtualization to improve the operational efficiency of the data center and to provide services to employees regardless of platform, lowering energy costs and spending. In particular, Virtual Desktop Infrastructure (VDI) is a popular choice for organizations looking to improve their IT efficiency across the board.

Server-based VDI is the creation of a user’s desktop environment, from operating system through applications, in a virtual machine (VM), run on a hypervisor¹ and

¹ Virtualization is made possible through a powerful software platform called a hypervisor. The hypervisor runs on the physical server and allows it to be segmented into multiple isolated VMs. The leading hypervisors are VMware, Citrix’s XenServer, and Microsoft’s Hyper-V. Hypervisors are inexpensive (VMware and Citrix offer their hypervisors as free, downloadable applications), easy to implement, and easy to manage through management software usually offered separately.

hosted in a centralized server (see Figure 1). The hosting server simultaneously supports multiple virtual desktops, with the number of virtual desktops supported limited by several factors, most notably the configurations of the desktops and the computing capacity of the server. The virtual machine instances that contain the virtual desktops are established and torn down based on business requirements—an on-demand attribute. Also, based on business requirements and rules, virtual machines can move from one physical server to another (i.e., VM mobility).

Figure 1—A Server-Based VDI Environment



This sharing of the collective computing capacity within a server farm and VM mobility among physical servers has the potential to significantly reduce a corporation's computing overhead and the costs associated with maintaining computing resources individually for each end user. With virtual desktops being customizable for each end user (again, based on corporate policies), end users retain the individuality required in their business roles but can access these resources from a variety of locations and devices (e.g., thin clients, desktop PCs, laptops, and tablets). However, this individuality and expanded access potential of server-based VDI also increases the security challenges faced by the organizations.

ADVANTAGES OFFERED BY A VDI DEPLOYMENT

By providing a centralized system, server-based VDI provides centralized control for hardware, software and applications, leading to increased utilization levels and lower management costs. VDI has the ability to enhance security, auditing, and other

compliances from a central point of contact. Server-based VDI has the ability to support a wide range of operating systems and applications without the need of installation at individual desktops.

To employees, VDI offers a single, device-independent interface to all their work applications, whether they are Windows-based, Web-based, or Software as a Service. These applications can also be delivered to a variety of devices—regardless of the operating system. This allows for:

- Increased productivity, without restraints of place or device
- The ability for employees to use their preferred personal devices
- Consolidation of applications that allows employees to access the needed applications without knowing or caring about the location of those applications

To the enterprise IT department, VDI is a way to manage user access to corporate assets by protecting and encapsulating corporate applications at the desktop. Benefits include:

- **Increased application availability**—Server-based VDI allows virtualized desktops to utilize a single, master “golden image” of each application and operating system. Upgrades, patches and maintenance activities can be completed centrally, replicated, and rolled out to users on demand.
- **Reduction in software errors**—Each time a user opens an app, it is certified to be clean and virus-free. Flawed or compromised images are merely discarded. This means that apps always perform at peak levels and with the highest level of trust (i.e., a “clean” application).
- **Decreased IT time spent on maintenance**—Virtualized desktops, with single software images, theoretically require significantly less maintenance than installed applications.

SECURITY CHALLENGES RELATED TO VDI

While VDI can offer organizations improved efficiencies and improve the security posture of an organization, there are many challenges that organizations may encounter when deploying VDI. These challenges are not trivial for many organizations and have called into question the Return on Investment (ROI) of VDI. Three key challenges with VDI deployments are described below.

Performance Degradation from Resource Contention

An organization moving to VDI in order to gain efficiencies in processing may be surprised to find that there are situations that can slow a virtualized server to a halt; resource contention being one of them. Resource contention occurs when multiple virtual machines simultaneously demand access to the same computing resources. Ironically, and described next, security best practices related to antivirus can bring virtualized environment to its knees.

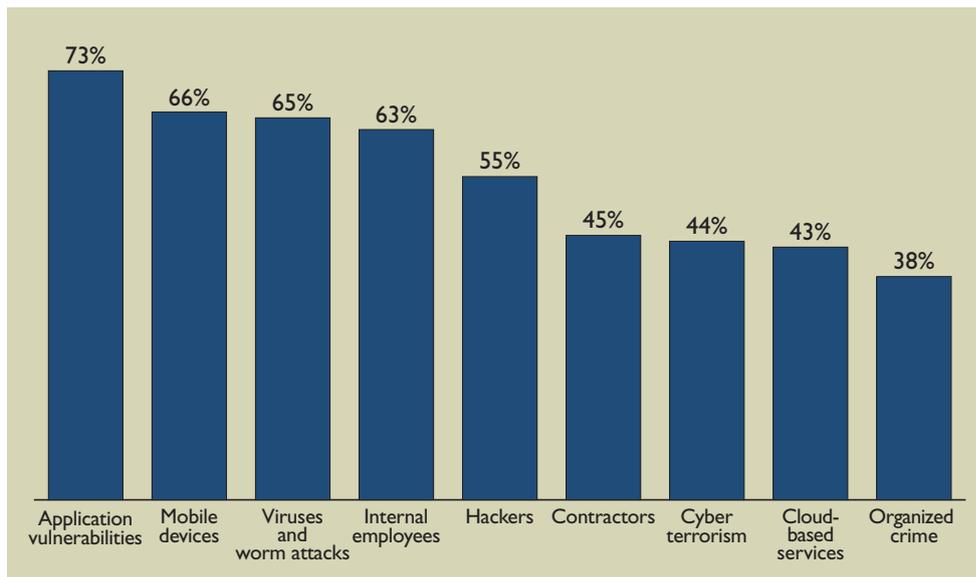
Regularly updating antivirus on all machines and performing regular system scans is an information security best practice. Unfortunately, VDI presents a unique challenge for administrators. Dubbed “antivirus storms,” many organizations have experienced resource contention issues related to the operation of antivirus software causing significant performance issues, leading to lowered ROI and misused resources.

Antivirus storms—or another common variation dubbed “the 9 a.m. problem”—occur when multiple virtual machines in VDI-hosting servers perform antivirus updates or system scans at the same time. This occurs because many organizations manage their antivirus in a VDI in the same manner as a physical deployment. In a physical desktop environment, updating machines only requires a small amount of CPU resources. In a VDI environment, it is not just one virtual desktop updating, but as many as 10 or 15 all on the same server. This spike in demand quickly consumes the CPU resources of the server and can significantly slow down performance.

Zero-Day Threat Environment Poses Increased Risk for VDI

Zero-day threats drive a significant portion of new attacks against organizations. Some of the highest profiled attacks in 2011—RSA, Sony, and Epsilon—were all traced back to users opening documents that had exploited software security vulnerabilities that are unknown to the software developer. These vulnerabilities are being detected by the hacker community first and exploited before the software developer can close the vulnerability (i.e., issue a software update). In a 2010 Frost & Sullivan survey, information security professionals ranked application vulnerabilities as their top security concern, beating out mobile devices, viruses and worms, and internal employees for the top spot.

Figure 2—Application vulnerabilities were reported as the top threat to organizations



In a server-based VDI environment, application vulnerabilities can be even more dangerous, as numerous machines are hosted on a single server. A successful attack against a single server hosting a VDI can propagate malware to a pool of end user desktop images with a single attack. In practical terms, server-based VDI creates a homogeneous environment, which significantly improves administration but requires improved security, as a single exploit is guaranteed to work across the entire set of images.

Lower than Expected ROI from Poor VDI Deployments

Organizations that are not properly configuring their virtualized environments may find they are getting a low ROI on new desktop VM deployments. This could be related to a number of different issues, such as:

- **Underutilization of virtualized servers**—Allocating the appropriate resources for virtualized environments can be challenging. IT departments that have not done their homework may be implementing server-based VDI with too many physical servers. Resource contention issues, such as the antivirus storms described above, may force organizations to maintain too many physical servers compared to industry best practices, resulting in a lower ROI.
- **Lack of updating of IT policies and procedures for a VDI environment**—Many organizations attempt to define and follow policies for virtualized desktops that are the same as those with physical desktops. However, backup and software distribution policies, for example, should be adjusted to handle the resource allocation challenges posed by a VDI.
- **Reliance on traditional security products**—Traditional security products—especially endpoint security products—rely on the existence of a heavy agent on the desktop. The agent performs regular security updates and scans. In a virtualized environment, this practice contributes to the aforementioned resource contention, leading to significant limitations on achievable virtual desktop density. Security products that are designed to recognize and allocate resources in a virtualized environment are necessary.

The first two concerns can be addressed through education and adherence to VM best practices. The third bullet, however, requires products that are designed from the ground up to integrate with VDI. This requires that security be provided at the hardware, hypervisor level and throughout all the desktop VMs holistically, not separately.

COMMON BUT INAPPROPRIATE RESPONSES TO THESE CHALLENGES

The previously mentioned security challenges can have a profound effect on operational efficiency. The transformation from physical desktops to server-based VDI can be an expensive project and sold on the promise of improve IT efficiency and ROI, therefore some IT and desktop security organizations may choose to drastically address problems in a manner that impact desktop security. Some common approaches to server-based VDI deployment issues are listed below.

Randomization or Disabling of Updates

Resource contention may cause administrators to randomize or alter the times and frequencies that VM antivirus products are updated. While this may alleviate resource contention issues, it does not eliminate the redundancy of virtual desktops pulling the same updates over and over, nor does it close the security gaps that open up in a virtual environment as new or reactivated virtual machines turn on. Given the speed that a zero-day exploit can spread, randomizing or time-delayed updates can leave machines unprotected, allowing for infections to take root.

Reliance on Physical Network Infrastructure Products (IDS/IPS and Firewalls)

Another common response to VDI challenges is to turn off antivirus completely, relying only on physical network infrastructure products. In theory, this approach may seem plausible, especially with non-persistent VDI sessions, which operate from a clean state with every new session. The problem is that turning off antivirus on the virtual machines eliminates the security between virtual machines. Should a user introduce a virus on their virtual machine, all the other machines on the same server would be vulnerable and the traditional security products would never recognize the attack occurrence. In addition, any loss of corporate or personal data during the time the virtual desktop was unprotected and subsequently compromised would be irreversible.

HOW VMWARE AND TREND MICRO'S AGENTLESS ARCHITECTURE APPROACH SOLVES VDI SECURITY AND ROI CHALLENGES

The security and ROI challenges mentioned above require a new approach to security. Many of the stopgap solutions being employed by administrators only increase the risk to the organization. Instead of trying to adapt traditional security methods to a virtualized environment, administrators should look at a solution that is integrated directly into the VDI environment and relies on proven security technology. VMware and Trend Micro have worked together to create products that address security directly in the virtualized environment.

VMware vShield Endpoint Provides the Foundation

VMware vShield Endpoint strengthens security for virtual machines and their hosts while enabling and improving the performance of endpoint security solutions. vShield Endpoint enables offloading of antivirus processing and allows a reduction in memory footprint for security on virtual hosts by eliminating antivirus software from virtual machines and centralizing those functions elsewhere. VMware Infrastructure administrators can centrally manage VMware vShield Endpoint through the vShield Manager console, which integrates with VMware vCenter Server to manage the platform. vShield Endpoint plugs directly into the VMware vSphere platform, is deployed on a per-host basis and consists of three components:

- A hardened virtual appliance provided by Trend Micro
- Driver for virtual machines to offload file events
- VMware Endpoint Security (EPSEC) ESX module to link the first two components at the hypervisor layer

The vShield Endpoint driver is enabled for the protected vSphere-based virtual machine and requires only a few megabytes of memory for operation. The driver monitors virtual machine file events and notifies the antivirus engine, which scans and returns a disposition for the file(s). It also supports scheduled full and partial file scans initiated by the antivirus engine in the virtual security appliance. When remediation is required, administrators can specify the actions to take using the existing antivirus manager, while vShield Endpoint enforces remediation action automatically within the respective virtual machines.

Trend Micro Deep Security Integrates with vShield to Provide Security

vShield provides the foundation for security in a virtual environment. Organizations also need an agentless antivirus solution that provides antivirus via a dedicated hypervisor-integrated virtual appliance. This deployment method eliminates the problem of AV storms by eliminating resource contention. This architecture shift can help lower the cost of VDI while at the same time improving security, thereby helping to justify and accelerate VDI investments. Two key features provided by Deep Security in conjunction with vShield are the management of resource availability and virtual patching. These two features alone address many of the security and administrator challenges experienced in managing a server-based VDI.

Deep Security Manages Resource Availability and Contention

By utilizing the control and insight provided by vShield, Trend Micro's Deep Security product offers the ability to manage resource availability and contention in a virtualized environment. By providing the following, a VDI environment can maintain appropriate security while avoiding performance barriers:

- Removes concurrent scans and updates per VDI host and resulting antivirus storms by serializing all scans from a single virtual appliance per host
- Improves CPU, memory and I/O resource efficiency on the host machine by getting rid of redundant agents in every desktop virtual machine
- Instantly protects all virtual desktops, including new, incoming or reactivated machines without the need for a pattern update window that is common with agent-based solutions
- Creates a new layer of isolation between malware and anti-malware, improving its defensive capabilities in the face of tampering attempts by malware on the target virtual desktop.
- Maintains availability and performance of the VDI host

These features are critically important, allowing organizations to maintain a strong security posture while adapting security to the VDI. This solution can only be achieved through the integration of vShield and Deep Security since both components play different roles in the overall solution.

Deep Security Provides Virtual Patching of Endpoints, Addresses Zero-Day Threats

In order to address challenges posed by zero-day threats, Trend Micro's Deep Security also provides intelligent, virtual patching of virtual endpoints. Deep Security has the ability to scan the VDI and determines missing patches and existing vulnerabilities, both on the operating system and within a number of common desktop applications. Deep Security automatically recommends a set of lightweight, fast-to-deploy filters that virtually patches the vulnerabilities, allowing IT departments the flexibility to apply the real patches at their own pace. Periodic running of these recommendation checks will also remove any filters that are no longer needed once the actual patches are installed. The Deep Security virtual patching capability can also be delivered without any footprint in the desktop virtual machine, via the same virtual appliance that is already providing agentless antivirus protection.

CONCLUSION

Improving organization efficiency is a necessity in today's fiercely competitive global market. IT departments, in particular, have found themselves leading the charge for improving efficiency in the organization, while also lowering costs. Server-based VDI offers a number of advantages to end users and IT departments alike. End users gain desktop consistency and accessibility from most anywhere, and IT gets to leverage virtualization technologies in lowering hardware and management costs. That being said, security is already a challenge for organizations, and securing a virtualized environment requires new products and new thinking in order to realize a positive ROI without compromising security.

Resource contention issues and zero-day exploits significantly increase the risks and lower the ROI of server-based VDI deployments. Without adequate tools to manage these challenges, IT administrators might be tempted to turn off services entirely, putting organizations' data and infrastructure at risk. Organizations relying on server-based VDI need security solutions developed from the ground up to address the specific challenges presented by a virtualized environment.

Trend Micro's Deep Security product, in conjunction with VMware's vShield Endpoint, provides the technology and intelligence needed to help IT departments secure their server-based VDI without sacrificing their security posture or losing the operational and financial benefits of a server-based VDI. By providing resource management and awareness, organizations can have a server-based VDI deployment that is just as secure as traditional physical desktops.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.

For information regarding permission, write:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Auckland	Dubai	Mumbai	Sophia Antipolis
Bangkok	Frankfurt	Manhattan	Sydney
Beijing	Hong Kong	Oxford	Taipei
Bengaluru	Istanbul	Paris	Tel Aviv
Bogotá	Jakarta	Rockville Centre	Tokyo
Buenos Aires	Kolkata	San Antonio	Toronto
Cape Town	Kuala Lumpur	São Paulo	Warsaw
Chennai	London	Seoul	Washington, DC
Colombo	Mexico City	Shanghai	
Delhi / NCR	Milan	Silicon Valley	
Dhaka	Moscow	Singapore	