When Desktops Go Virtual

Virtualization Security.

Addressing security challenges in your virtual desktop infrastructure

A Trend Micro White Paper | February 2011

WHEN DESKTOPS GO VIRTUAL

I. VIRTUAL DESKTOP INFRASTRUCTURE

Server virtualization is well on its way to becoming mainstream. Enterprises have achieved significant savings in hardware and operating cost by optimizing resource utilization. This widespread acceptance is due in part to advanced virtualization technologies which have further increased the availability of mission-critical resources. Having experienced the cost and efficiency benefits of virtualization in the data center, many enterprises are eager to extend those same advantages into other areas of their business. This has fueled a new wave of virtualization—at the desktop. Enterprises are looking to virtualize desktops to lower costs, speed provisioning, and streamline support and management—often on a much bigger scale than at the data center.

With Desktop Virtualization, often also referred to as VDI, customers can leverage a multitude of stationary and mobile devices to access their desktop, which is actually running on powerful, centralized server in the data center. VDI combines the robust virtualization technology known from server virtualization with advanced session management and innovative network protocols to provide a user experience very similar to working on a dedicated desktop PC. However, overall resource utilization is much more efficient as the server hardware is shared by tens of desktops—all while completely isolating each from the other. .

One of the strengths of VDI is its ability to support a full range of desktop types and desktop use cases, ranging from dedicated desktops to semi-public or public kiosk-type applications. This is essential to overall adoption of the technology, since many users want all the benefits offered by a traditional desktop. VDI gives users the features they need, such as personal storage space, but without the failure issues. At the other end of the spectrum, administrators want ease of administration. As much as possible, they want to eliminate the hassles of maintaining, provisioning, and patching endpoints—especially those that have limited or even single-application use, such as endpoints used for call-centers or public libraries. Virtualizing these endpoints creates opportunities for cost and resource optimization in several areas.

DEPLOYMENT AND INITIAL PROVISIONING OF ENDPOINTS

VDI streamlines deployment and speed time to functionality. Virtualized endpoints are typically all based on a base image (“Gold Image”). That image consists of the operating system, relevant patches, and standard applications. Deploying new virtualized desktops is as easy as creating a copy or clone of that base image and starting it up as a new instance on the VDI host system.

EXTENDED DESKTOP HARDWARE LIFECYCLE

Operating systems and applications have grown increasingly resource hungry. For example, rolling out Windows 7 to older hardware sometimes creates challenges, requiring enterprises to replace the systems with newer hardware. In VDI environments, all operating systems and applications run on powerful central servers. This minimizes the importance of the hardware performance on the actual desktop PC. Because this enables existing desktop hardware resources to be used for a prolonged period of time, enterprises are able to extend endpoint hardware refresh cycles.

REGULATORY COMPLIANCE

Because with VDI all systems are centralized in the data center, complying with regulations is much easier. Controls mandated by regulations can be implemented and enforced to virtualized endpoints in a repeatable, streamlined fashion in the data center—much easier than in a traditional desktop environment, where endpoints are dispersed.

ENDPOINT BACKUP

Creating backup of dispersed desktop computers has always been a challenge for enterprises. In particular, increased mobility and ever growing storage capacities have made creating backups increasingly difficult. In a VDI environment desktops are centralized, making the backup of all desktops a much easier task. Because the backup data never leaves the high-performance infrastructure at the data center, the entire process of backing up becomes easy, fast, and painless.

DATA PROTECTION

Confidential or sensitive data on dispersed endpoints—especially mobile endpoints—is hard to control. Enterprises put a lot of effort in endpoint data loss prevention, hard-disk encryption, and other technologies designed to prevent data from being accessed—especially in cases where a laptop is lost or stolen. In a VDI environment, it is easier to protect data because it resides on a central server and never leaves the secure boundaries of the corporate data center.

OPERATIONS, MAINTENANCE, AND SUPPORT

Maintaining desktops in a VDI environment is much easier than in traditional environments. Rolling out patches, deploying new software, and even adding RAM or hard-disk capacity all happens at the central server level. This eliminates concerns about endpoints being switched off at the time of patching or software deployment. The ability to dynamically allocate hardware resources to virtualized desktops not only saves time, it also enables much more efficient use of hardware resources. For example, if a user calls in with a support issue, the support staff can access the virtualized desktop in the data center rather than having to access a physical machine that might be remote.

II. SECURITY CONSIDERATIONS ON VIRTUALIZED DESKTOPS

Depending on the use case for VDI desktops, security requirements can vary significantly. On one side of the spectrum, you have a knowledge-worker scenario, with long-lasting sessions on dedicated, persistent desktops with access to critical corporate data and full access to the internet. This use case requires more comprehensive protection and cleaning capabilities. On the other side of the spectrum of VDI use cases, you have desktops that are non-persistent and get re-created on the fly as users log in. For this use case, a better choice might be an agent-less solution, with basic anti-malware protection but a drastically reduced management overhead.

WHEN DESKTOPS GO VIRTUAL

Common to all VDI scenarios is the need for some level of security. Even if reverting a virtual desktop to a clean state is easier and less painful than with a physical desktop, risks do exist in any desktop scenario due to the difficulty of controlling users who frequently:

- Surf the web and might access malicious web content.
- Might be lured into exposing confidential information
- Open potentially malicious email-attachments
- Install applications and “tools” on their desktops

In addition to behavioral differences, system-specific threats present significant security challenges. Systems need to be continually up to date to protect from these threats. Protection should include:

- Shielding vulnerabilities from being exploited
- Preventing unauthorized access over the network
- Ensuring malware-free data storage.

The dynamic nature of the desktop requires a combination of several technologies to effectively protect virtualized deployments:

- Preventing exposure to threats with cloud-based security
- Detecting malicious files at the endpoint in real-time while maintaining system performance and keeping a small footprint.
- Shielding vulnerabilities before patches can be deployed
- Regular full-system scans (scheduled and/or on-demand) to detect and remove malware that might not have been detected earlier.

VDI-SPECIFIC REQUIREMENTS

When multiple virtualized desktops share a common hardware, even a powerful server can quickly become overwhelmed—especially during simultaneous actions. For desktops in particular, there are certain resource-intensive operations that cause no issue when executed on individual PCs, but can quickly result in an extreme load on the VDI system.

Full System Scans

During a full system scan, the entire file system is scanned for malware. This introduces a notable amount of load on any individual system. Typically, full system scans are scheduled by the administrator to take place at a certain time (e.g. 3PM on Thursdays). If several—or all—virtualized desktops start a full scan at the same time, the underlying shared hardware of the VDI server will experience extreme load, causing a slow-down of all virtual systems on the server. To ensure smooth operation and normal load on the host system, a VDI-aware endpoint security solution must serialize full scans for systems on the same VDI host.

Component Updates

Larger client updates present many of the same challenges and must be treated in a similar fashion to system scans. Pushing out a major update to multiple virtualized desktops at the same time can saturate the host's network connection and introduce high I/O load on the host. This can seriously impact the performance impact on the virtual desktops that are running at that time. This load balancing must also be addressed with VDI-aware endpoint security.

MULTIPLIED FOOTPRINT

Agent-based security that uses client-side pattern files is inefficient in a VDI deployment. This approach multiplies the effects of increasing memory footprint of ever-growing pattern files. Despite the advanced memory pooling in today's virtualization solutions, the overhead of storing and loading hundreds of MB of pattern files into memory—on every VM—is a waste of resources.

III. HOW TREND MICRO CAN HELP

Trend Micro has significant expertise in the area of virtualization security. Industry-leading products such as Deep Security, OfficeScan, and Core Protection for Virtual Machines clearly demonstrate Trend Micro's leadership in the area of virtualized security. The benefits of these mature virtualization security offerings are combined in a single solution for Virtual Desktop environments—Trend Micro Virtual Desktop Security. This robust solution offers all of the best technologies to effectively secure your Desktop Virtualization deployment, regardless of the individual use case.

FLEXIBLE DEPLOYMENT OPTIONS

Whether your deployment calls for an agent-less solution, automatically protecting every VM on a system without requiring a security agent in every desktop VM or whether you need the maximum security for a fully persistent desktop that only an in-guest agent can provide, Trend Micro Virtual Desktop Security has it.

Virtual Desktop Security provides the industry's first true agent-less antivirus solution for VDI. Integrating with the vShield hypervisor-level APIs in VMware vSphere 4.1, the individual file-IO and network-IO of every VM is intercepted and analyzed by a dedicated security VM on the host. This drastically reduces the management effort

Virtual Desktop Security also provides leading virtualization-aware in-guest security agents. As it detects the virtualization status of every endpoint, the solution doesn't introduce resource contention. Using file reputation technology with in-the-cloud signatures not only provides industry-best protection, it also dramatically reduces the agent's overall footprint and the requirement to be updated on a regular basis.

SERIALIZATION OF FULL SYSTEM SCANS PER VDI-SERVER

Virtual Desktop Security will allow only a given number of virtualized endpoints to perform a full system scan at the same time. With this serialized approach, the overall impact on performance is low, yet all systems will be scanned—one after the other.

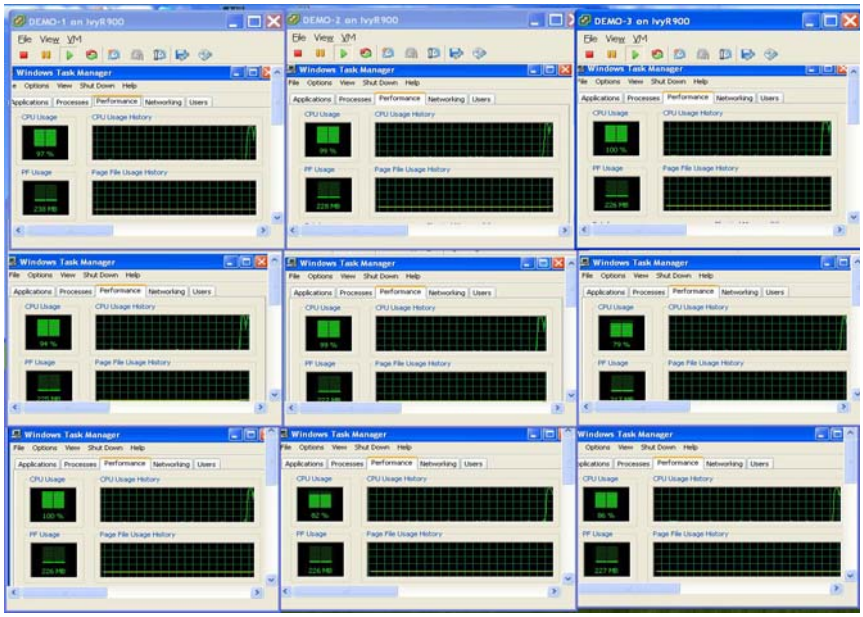

Figure 1: Without VDI-awareness: all guests start scanning at the same time

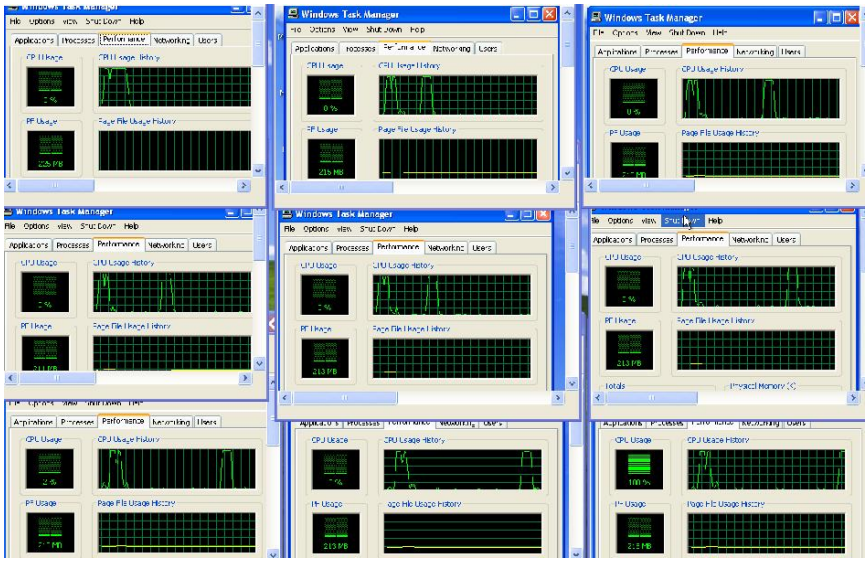

Figure 2: WITH VDI-awareness: Full Scans happen one at a time, optimizing the user experience for all virtual desktops

SERIALIZATION OF CLIENT UPDATES PER VDI-SERVER

Similar to the serialization of full scans, the security management system will only run updates on a limited number of virtualized desktops per VDI server at the same time.

PRE-SCANNING AND WHITELISTING OF BASE IMAGES

Most virtual desktops will be created using the same base image. Administrators can pre-scan and whitelist the elements of that base image. The result is that in each instance of virtual desktop, Virtual Desktop Security agents will only scan for deviations from the base image. This eliminates most extraneous scanning, resulting in much shorter scan times which ultimately contribute to lower performance impact and increased productivity.

INTEGRATION WITH VDI MANAGEMENT

Trend Micro Virtual Desktop Security integrates with VDI management platforms from Citrix and VMware to retrieve information about the status and location of secured virtual desktops. Agentless deployments fully integrate status and security information of infrastructure-level security with VMware vCenter. This helps optimize resource utilization across the entire virtual desktop environment and enables security to become an integrated part of your desktop virtualization deployment instead of a power-hungry on-top solution.

IV. SUMMARY

Virtual desktop infrastructure carries the potential for significant savings. However, given the dynamic nature of desktop computing, virtualizing endpoints will raise significant challenges. The temptation will be to treat virtual desktops like data center servers when it comes to protection. But this will quickly prove ineffective. Applying standard desktop security solutions to these environments may lead to sub-optimal performance and may prevent enterprises from realizing the full potential savings. VDI-aware endpoint security is key to maintaining performance and productivity of all virtualized desktops without compromising the privacy and security of either the system or the user. The right endpoint security for virtual desktops will also help your enterprise achieve the cost and efficiency advantages of increased VM density.

With Trend Micro Virtual Desktop Security, Trend Micro reconfirms its commitment to and leadership in virtualization security—helping you to get the most out of your virtualization efforts.

To learn more about Trend Micro virtualization and cloud security solutions, contact your Trend Micro representative or visit www.trendmicro.com/virtualization .