

VDI Security for Better Protection and Performance

Addressing security and infrastructure challenges in your VDI deployments



Trend Micro, Incorporated

- » See why you need security designed for VDI environments to address the unique security challenges of virtualization while optimizing the resource benefits of VDI.

THE MOVE TO 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 and are moving towards virtualizing more business critical servers. This widespread acceptance is due in part to advanced virtualization technologies which have further increased the availability of resources. Having experienced the cost and efficiency benefits of virtualization with servers, many enterprises are eager to extend those same advantages into other areas of their business. This has fueled a wave of virtualization at the desktop. Enterprises are looking to virtualize desktops to lower costs, speed provisioning, streamline support and management, and reduce risks.

With Virtual Desktop Infrastructure, often also referred to as VDI, desktops are delivered as a managed service from the data center. Employees can leverage a multitude of stationary and mobile devices to access their desktop, which is actually running on a powerful, centralized server. 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. Providing the level of features and access needed by different user types is essential to overall adoption of the technology. For example, many users want all the benefits offered by a traditional desktop, such as personal storage space, but without the failure issues.

At the other end of the spectrum, administrators turn to VDI for ease of administration. VDI can help them eliminate the hassles of provisioning, maintaining, and patching endpoints—especially those that have limited or even single-application use, such as endpoints used for call-centers or public libraries.

Even in this initial overview of VDI implementation, many of the VDI benefits are apparent—efficient resource utilization, ease of application and data access, flexible use case deployment, and simplified provisioning, maintenance, and patching. These benefits are worth exploring in more detail along with additional VDI benefits around business agility, security, and cost savings. But to safely leverage these benefits, organizations need security that is designed for VDI environments, addressing the unique security challenges of virtualization while optimizing the resource benefits available through VDI.

BENEFITS OF VIRTUAL DESKTOP INFRASTRUCTURE

Business Agility

VDI can help you transform your business. With virtual desktop images located in a central location in the data center, administrators can more easily provision, maintain, and support endpoints. And this structure makes it simple for employees to gain access anytime, anywhere, and on any device, increasing productivity. Overall, VDI can increase business agility and allow organizations to focus more on innovation and growth and less on basic administrative tasks.

- **Deployment and initial provisioning of endpoints:** VDI streamlines deployment and speeds time to functionality. Virtualized endpoints are typically all configured 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.
- **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. And central maintenance eliminates concerns about endpoints being switched off at the time of patching or software deployment, ensuring timely updates. And VDI also simplifies support. 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.
- **Anytime, anywhere, any device access:** Personal PCs, tablets, and smartphones have become more affordable and intuitive, and many employees want to be able (and sometimes demand) to use these devices for work. VDI centralizes storage of applications and data and can provide consistent access to this content across multiple devices. This gives employees the flexibility to work when and where they need to and to use the device that is most appropriate for the situation. VDI increases productivity by giving employees more choices in how to best approach their tasks.

Improved Security

Not only does centralizing VDI in the data center simplify provisioning, operations, maintenance, and support, it also improves security because administrators have more control over desktop applications and data. With the VDI instances collocated on servers, administrators can more easily backup endpoints, deploy and maintain security, and meet compliance regulations.

- **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.
- **Regulatory compliance:** With VDI systems centralized in the data center, complying with regulations is also much easier. Controls mandated by regulations can be implemented and enforced to virtualized endpoints in a repeatable, streamlined fashion—much easier than in a traditional desktop environment, where endpoints are in the hands of remote and mobile workers.

Cost Savings

Businesses also turn to VDI for cost savings. Many of the benefits mentioned above also provide cost advantages. Lowering the administrative burden can reduce costs, and the anytime, anywhere, any device access improves productivity, potentially generating more revenue. And more centralized security reduces risks and prevents breaches and data loss as well as their corresponding costs. Another cost savings element which is discussed below, is the extended PC hardware use lifecycle due to desktops being delivered as a managed service.

Yet when planning VDI projects, organizations need to consider the initial implementation costs of VDI. The on-going cost benefits of VDI may eventually outweigh the initial VDI deployment expenses, but organizations should be ready for these up-front expenditures when planning VDI projects. And finally security must be evaluated when considering VDI costs. Using the wrong security can limit the infrastructure benefits of VDI, delivering a lower than expected ROI.

- **Extended desktop hardware lifecycle:** Operating systems and applications have grown increasingly resource hungry. For example, rolling out newer operating systems 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.
- **Weighing the cost of initial VDI implementation:** If organizations expect to realize cost savings upon deploying VDI, they may be sorely disappointed. Initial VDI costs often include additional storage, staff training and implementation time, licenses fees, and other infrastructure expenditures that can add up to substantial sums. However, businesses can still achieve cost savings with VDI as the on-going cost savings should eventually outweigh the initial expenditure. Organizations should assess the initial VDI investment

and weigh this against anticipated savings over time in addition to the other business and security benefits provided by VDI.

- **The impact of security on VDI cost savings:** The type of security used in VDI environments also impacts cost savings. Deploying traditional endpoint security in virtualization environments can sap resources, lower performance, and reduce VM densities—increasing the overall costs of the VDI project. VDI security is necessary, but it should not sacrifice performance and ROI. Instead, businesses should turn to security that leverages the virtualization platform and optimizes the VDI benefits received.

SECURITY CONSIDERATIONS FOR VIRTUALIZED DESKTOPS

Virtual desktops should be secured by the same strong security technologies as physical desktops. However, the shared resource environment of VDI creates unique security challenges and infrastructure considerations that should be addressed by the VDI security solution.

Traditional Endpoint Security Software in VDI Environments

Traditional agent-based solutions that are not architected for virtualization can result in a number of significant operational security issues.

- **Resource consumption:** Traditional security agents occupy a significant amount of memory in each virtual desktop, especially when multiple security agents are installed on each machine to provide a range of protection.
- **Security storms:** Traditional endpoint security software solutions are not designed for the shared resource environments of VDI. When security scans or scheduled updates are performed by these solutions, they are simultaneously initiated on all virtual desktops on a single physical host. The result is a “security storm” that can quickly result in an extreme load on the system, saturating the host's network connection and introducing high I/O load on the host. This impact on performance is particularly evident with antivirus solutions but is also impacted by other types of endpoint security.
- **Instant-on gaps:** VDI allows virtual desktops to be easily provisioned, moved, cloned, deactivated and reactivated as needed. But when virtual desktops are activated and deactivated in rapid cycles, it is difficult to consistently provision security to those virtual desktops and keep them up to date. Dormant virtual desktops can eventually deviate so far from the baseline that simply powering them on introduces massive security vulnerabilities. And if these virtual desktops are then replicated, the problem is compounded.
- **Operational overhead:** With traditional endpoint security, administrators need to provision security agents in new virtual desktops, continually reconfigure these agents as the virtual desktops move or change state, and rollout pattern updates to these agents on a regular basis. This can be extremely time consuming and still result in security gaps.

- **Compliance and data privacy:** With the ease of provisioning and mobility of virtual desktops, it can be difficult to maintain an auditable record of the security state of a virtual desktop at any given point in time. Yet, many regulations require proof of current security in virtual environments.

By impacting VDI resources and performance, traditional endpoint security software reduces consolidation ratios and increases CAPEX and OPEX. And with increased security risks, more administration, and less visibility for compliance, applying traditional endpoint security software to VDI environments significantly reduces other VDI benefits that could be experienced by the organization. Instead, organizations need security that is designed for VDI environments, enabling organizations to maximize the benefits received while providing better security that addresses the challenges of virtualization environments.

Virtualization-aware Security for VDI Environments

VDI security should leverage the virtualization platform to provide visibility and to optimize resources while providing security designed for virtualization environments.

- **Integration with the virtualization platform:** VDI security should integrate with the hypervisor APIs. This integration allows the security solution to communicate with the guest virtual desktops and gain visibility into the VDI security that is needed for compliance. VMware is an example of a virtualization platform vendor that has opened up its APIs to security vendors through vShield Endpoint.
- **Dedicated security virtual appliance:** Through integration with the hypervisor, a dedicated security virtual appliance can be used to coordinate security across the various VDI instances on the same host physical machine. Security scans and updates can be staggered to preserve resources. Resource-intensive operations, such as full system scans, are run from this separate scanning security virtual appliance. The security virtual appliance can also ensure that virtual desktops are secure when provisioned and that dormant virtual desktops are ready with the latest security updates when reactivated, providing “always-on” security.
- **Agentless security:** When a dedicated security virtual appliance is integrated with the virtual platform APIs, the security solution can communicate with the guest virtual desktops and deliver agentless security. With this agentless protection there is no extra footprint from a security agent to impact the virtual desktops and the underlying host, which preserves resources and performance. And agentless security also reduces administrative complexity with no agents to deploy, configure, or update.
- **Comprehensive agentless security platform:** Agentless security for VDI can deliver multiple types of security all in one solution and all coordinated through the security virtual appliance. As with physical desktops, key security for virtual desktops includes antivirus, intrusion detection and prevention, web application control, and firewall. This combined security also enables virtual patching to safeguard against zero-day threats and reduce the need for emergency patching. Providing these VDI security technologies in one agentless security solutions eliminates the need for multiple security agents on each virtual desktop, further optimizing resources and performance.

VDI security can leverage hypervisor APIs to enable the use of dedicated security virtual appliances and agentless security. Unlike traditional endpoint security software designed for physical endpoints, this agentless approach reduces the burden on guest virtual desktops and the underlying host, allowing for increased VM densities and improved VDI ROI.

Addressing Traditional Security Issues with VDI-aware Security

The security challenges and infrastructure issues created by traditional endpoint security software in virtual environments is discussed above. The following table summarizes how security designed for VDI environments alleviates these issues.

Table 1: Addressing Traditional Endpoint Security Issues with Security Designed for VDI

VDI Issues Caused by Traditional Endpoint Security	Impact of Traditional Security or Infrastructure Issue on VDI	Alternative Approach by Virtualization-aware VDI Security	Benefit of Virtualization-aware Security for VDI
Resource Consumption	Security agents on each VDI instance consume excessive resources	Agentless security using a dedicated security virtual appliance that integrates with hypervisor APIs	Agentless security for several VDI security technologies eliminates the need for multiple security agents on each virtual desktop
Security Storms	Traditional security initiates simultaneous security scans and updates across VDI instances on the same host impacting resource and performance	Dedicated security virtual appliance coordinates staggered scans and updates	Eliminating simultaneous scans and updates preserves resources on the underlying host and increases performance
Instant-on Gaps	Dynamic nature of VDI instances can lead to out-of-date security, particularly on reactivated or cloned virtual desktops	Dedicated security virtual appliance communicates with VDI instances to ensure up-to-date security	“Always-on” security provides current security for VDI instances throughout their lifecycle—including new and reactivated virtual desktops
Operational Overhead	Security agents need to be provisioned, reconfigured, and updated—requiring significant administration	Agentless security using a dedicated security virtual appliance that integrates with hypervisor APIs	No agents to deploy, configure, or update reduces administration
Compliance and Data Privacy	Security deployed per virtual desktop limits visibility and compliance reporting	Integration with hypervisor APIs and virtualization platform management	Insight across VDI instances to provide a consolidated view of security and improve compliance reporting and audits

Using security designed for physical desktops in your virtual desktop infrastructure may result in performance degradation, lower VM densities, and reduction of virtual desktop ROI. Instead, to safely embrace virtual desktops, customers need security that addresses the challenges unique to this IT environment.

HOW TREND MICRO CAN HELP

As the leader in virtualization security for two consecutive years¹, Trend Micro is in a unique position to be able to help businesses with VDI security. Trend Micro was the first security vendor to integrate with VMware vShield Endpoint APIs for agentless security and the only vendor to go beyond agentless antivirus for a full suite of agentless security options.

Trend Micro designed its solution, Trend Micro Deep Security, to integrate with vShield Endpoint APIs to offer agentless security for VMware virtual environments. This agentless security is ideal for VMware View virtual desktops because it optimizes virtualization performance and reduces administrative complexity.

How Trend Micro Deep Security Secures VDI

Trend Micro Deep Security delivers the VDI security approach discussed above. A dedicated, security-hardened virtual appliance integrates with the VMware hypervisor APIs to access a small VMware driver in each guest virtual desktop to coordinate staggered updates and scans without the need for a traditional security agent in each virtual desktop.

The security virtual appliance ensures that virtual desktops are secure when dormant and ready with the latest security updates when reactivated. This “always-on” agentless security delivers virtual patching to safeguard against zero-day threats and reduce the need for emergency patching on virtual desktops.

With a dedicated security virtual appliance and agentless protection there is no extra footprint from a security agent to impact the virtual desktops and underlying host. And agentless security also reduces administrative complexity with no agents to deploy, configure, or update.

A Full Suite of Agentless Security Options for VDI

Trend Micro Deep Security provides a comprehensive security platform designed to protect physical, virtual, and cloud servers, as well as virtual desktops. Tightly integrated modules easily expand the platform with comprehensive protection for virtual desktop environments that offers the highest security available for a wide spectrum of virtual desktop scenarios. Virtual desktops primarily benefit from antivirus, intrusion detection and prevention, web application protection, and bidirectional stateful firewall. Agentless integrity monitoring and application control are also available, but mainly used for server protection.

Complementary Trend Micro VDI Security

Trend Micro OfficeScan lets you consolidate your endpoint security into one solution for both physical and virtual desktops. This is an agent-based solution, but unlike physical endpoint security solutions that are not designed for virtual environments, OfficeScan recognizes whether an agent is on a physical or virtual endpoint, and optimizes protection and performance for its specific environment.

For virtual desktops, OfficeScan serializes scans and updates, and white lists base images and previously scanned content to preserve the host resources. OfficeScan VDI security is ideal for current OfficeScan customers that are looking to virtualize their desktops.

For more information on Trend Micro OfficeScan VDI Security, visit:

<http://www.trendmicro.com/officescan>.

¹ Source: 2012 Technavio—Global Virtualization Security Management Solutions

This agentless security integrates in the same virtual appliance for increased protection on VMware virtual machines. Agent-based security is also available for these security options as well as log inspection, allowing businesses to combine agentless and agent-based deployment configurations that best support their physical, virtual, and cloud servers and virtual desktops on a variety of platforms.

Integration with VDI Management

Deep Security 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.

By providing better protection for VDI environments while optimizing VDI resources and performance, Trend Micro Deep Security accelerates VDI ROI.

SUMMARY

Traditional agent-based solutions that are not architected for virtualization can result in a number of significant operational security issues.

Virtual desktop infrastructure carries the potential for significant benefits in business agility, security, and cost savings. However, given the dynamic nature of desktop computing, virtualizing endpoints will raise significant challenges. Applying traditional endpoint security solutions to these environments may lead to sub-optimal performance and may prevent enterprises from realizing the full potential savings and ROI of their VDI projects.

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 enterprises achieve the cost and efficiency advantages of increased VM density.

With Trend Micro Deep Security, organizations can benefit from Trend Micro's leadership in virtualization security—helping businesses get the most out of their virtualization efforts. To learn more about Trend Micro virtualization and cloud security solutions, contact your Trend Micro representative or visit www.trendmicro.com/deepsecurity.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.

U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003

www.trendmicro.com.