

Securing Your Virtual Desktop Infrastructure

Using virtual desktop infrastructure (VDI) can help you simplify provisioning and administration, extend your endpoint hardware investments, and make it easier for you to support employee-chosen endpoint devices. And with your desktops running on protected servers in your data center, VDI lets you retain the control and security you need. But to safely embrace virtual desktops, you'll need security that addresses the challenges unique to this IT environment. Using security designed only for physical desktops to protect your virtual desktops can degrade performance, lower VM densities, and significantly reduce your ROI. Instead, you can maximize protection and performance with virtualization-aware security that is designed to optimize the shared resource environment of virtual desktops.

VIRTUAL DESKTOP SECURITY CHALLENGES

Resource Contention

With VDI, numerous desktops share the host's hardware resources, often at a ratio of 60-to-1 or higher. With these high levels of density, simultaneous resource-intensive operations, such as major security updates and full-system scans, result in a dramatic loss of desktop performance. The impact can become so severe that the host is incapacitated and users lose their session connection, often being unable to reconnect for extended periods of time.

Propagating Out-of-Date Security

Virtual desktops can quickly be provisioned, cloned, reverted to previous instances, paused, and restarted, all relatively easily. Vulnerabilities or configuration errors may be unknowingly propagated, and dormant desktop images can be reactivated with out-of-date security.

ADDRESSING THESE CHALLENGES

VDI-aware Security

Resource contention can be overcome with VDI-intelligence that identifies virtualized desktops on VMware View and Citrix XenDesktop. VDI-aware security serializes scans and updates to preserve the system's performance and availability.

White Listing

You can leverage common VDI provisioning techniques to create base images and clones or linked clones. Then you start with the right security installed inside a base image to ensure up-to-date protection. When you prescan and white list the content of this base image, it will be excluded from subsequent scans. After that, only files added by the user—a small fraction of the VDI image—need to be scanned. Preventing the duplicate scanning of identical files across multiple VDI images further increases the system's performance and availability.

Dedicated Security Appliance

Another approach that can ensure up-to-date security while also maximizing virtual desktop performance is to use a dedicated, security-hardened virtual machine. By integrating with the hypervisor APIs, the VM accesses a small footprint driver in each guest VM to coordinate staggered updates and scans. Resource-intensive operations, such as full system scans, are run from the separate security VM. This ensures that virtual desktops are secure when dormant and ready with the latest security updates when reactivated. This "always-on" agentless security also delivers virtual patching to safeguard against zero-day threats and reduce the need for emergency patching on virtual desktops.

How do virtual desktops work?

You deliver desktops as a managed service from your data center. Virtual desktops are deployed through a private cloud to wherever they're needed—across local, remote, and branch offices. Applications and desktops are delivered faster and more consistently to a wider variety of clients.

Protection Points: Virtual Desktops

- Citrix XenDesktop
- VMware View

VDI Deployment

- 52% of companies worldwide have deployed or are piloting VDI
- Of companies that have VDI in production
 - An average of 42% of their endpoints are virtualized
 - In the next 12 months, 60% of their endpoints will be virtualized

Source: Trend Micro survey, May 2011

WHAT PATH ARE YOU TAKING TO VIRTUAL DESKTOP SECURITY?

You might turn to VDI to support a broad range of virtual desktop scenarios—from single application kiosk-type use in public environments to the complete replacement of your physical desktops. But regardless of your individual approach to your virtual desktop infrastructure, Trend Micro has a security solution that is designed to protect your path to VDI.

PATH 1: Extending Your Physical Endpoint Security to Protect Your Virtual Endpoints

- Looking to manage your physical and virtual endpoint security in one solution?
- Already an OfficeScan customer?
- Want to integrate your virtual desktop security with Citrix for improved performance?

Trend Micro OfficeScan

OfficeScan lets you consolidate your endpoint security into one solution for both physical and virtual desktops. But unlike physical endpoint 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.

PATH 2: Extending Your Server Virtualization Efforts to Virtual Desktops

- Looking for security that protects your virtual servers and virtual desktop infrastructure?
- Want to leverage your VMware environment to deploy agentless security to improve performance?
- Wish to manage your data center's physical, virtual, and cloud servers, as well virtual desktops all through one solution?

Trend Micro Deep Security

Trend Micro was the first company to integrate with VMware vShield Endpoint and other VMware APIs to deliver agentless security for virtual servers and desktops. A dedicated, security-hardened virtual machine integrates with the VMware hypervisor APIs to access a small footprint driver in each guest VM to coordinate staggered updates and scans without installing a security agent. Eliminating the agents off the guest virtual machines reduces the resource burden on the underlying host—maximizing your performance and increasing your VM densities. An agent-based option is also available for virtual desktops running in a Hyper-V or Xen-based hypervisor environment, as well as with any virtual desktops in local mode.

Choose the Right Endpoint Security for Your Enterprise

Depending on your unique environment, you may choose to start at the endpoint and extend your OfficeScan deployment to provide consistent security for both physical and virtual desktops. Or you may wish to leverage your VMware virtualization efforts in your data center by using Deep Security for agentless security. Either way you'll consume fewer resources and achieve higher consolidation ratios. Let the recognized leader in virtual security, help you achieve the VM density, security, and ROI you expect from your virtual desktop infrastructure.

Virtual Desktop Security Components

OfficeScan VDI Protection

- Antivirus
- Anti-spyware
- Anti-rootkit
- Firewall
- Web Threat Protection
- Scalable central management

Other OfficeScan Plug-ins Include:

- Data Loss Prevention
- Intrusion Defense Firewall
- Mobile Security
- Security for Mac

Deep Security VDI Protection

- Anti-malware
- Firewall
- Intrusion detection and prevention
- Web application protection
- Application control
- Virtual patching
- Integrity monitoring
- Log inspection
- Scalable central management

Trend Micro Smart Protection Network

Trend Micro virtual desktop security includes protection from the Smart Protection Network, a cloud client architecture that accesses threat intelligence from the cloud to drastically accelerate protection while lowering the resource impact on endpoints.

