Solution Brief

Optimize Virtual Desktop Security and Performance with Trend Micro

AT A GLANCE

VMware vShield leverages the unique advantages virtualization brings to security – such as introspection, change awareness and the ability to leverage existing investments - to deliver better than physical cloud security. vShield makes VMware clouds more secure than any other environment because it:

1 **Provides comprehensive protection** for cloud deployments

2 **Reduces complexity of implementation** and management

3 **Enhances infrastructure performance**

4 **Accelerates IT compliance**

Trend Micro Agentless Security for VMware View

Virtualization is the foundation for cloud computing architectures. As the customer-proven leader in virtualization, VMware is charting the course to cloud computing. Working in concert with industry leaders, like Trend Micro, VMware is helping businesses of all sizes migrate to cloud computing, the new era in IT that finally addresses the compounding problems of IT cost, complexity and security.

Clouds Built on VMware – More Secure Than Any Other Environment

Just like virtualization is indispensable for transitioning legacy applications to a new cloud infrastructure, it also can be an indispensable security enabler in a cloud environment. VMware vShield families of products create the groundwork for the next generation of cloud security.

The New Desktop Paradigm for Enhanced Endpoint Security

VMware View 5 delivers on the promise of user-centric computing for customers on their journey to IT as a service. With VMware View customers are able to pull the OS and applications off the physical desktop hardware and manage OS, applications and data in the private cloud, delivering IT as a service.

VMware View 5 simplifies IT management while increasing security and control of end user computing in the private cloud. Granular levels of control enable IT to customize the user experience, access, and personalization in accordance with corporate policy. VMware View 5 delivers the highest fidelity experience for users who need applications, unified communications and 3D graphics as part of their daily workspace. With access available from a wide variety of device platforms and performance optimizations to accommodate a broad range of users, VMware View delivers on the promise of a new way to work. IT can now deliver elastic desktop services from the cloud with ultimate control, flexibility and performance, and most of all, security.

The Comprehensive Security Approach

Trend Micro—the recognized leader in virtualization security—has teamed up with VMware to provide virtualization-aware security that's been optimized for virtual desktop environments. They have developed a comprehensive protection suite for virtual desktop environments that offers the highest security available for a wide spectrum of virtual desktop scenarios. Trend Micro Deep Security with VMware vShield Endpoint and VMware View maximize your virtual desktop protection and performance.

SERVER AND VIRTUAL DESKTOP PROTECTION

Trend Micro Deep Security

The first and only security partner solution architected specifically for VMware

- First to integrate with VMsafe API's
- First to integrate with vShield Endpoint APIs
- First to deliver agentless antimalware

Over 1000 customers for agentless antimalware in the first year

Up to 3x higher virtual desktop consolidation ratios over leading traditional physical desktop antimalware solutions.

Trend Micro Deep Security offers a single security platform for physical, virtual, and cloud servers as well as virtual desktops. Trend Micro was the first security vendor to integrate with VMware vShield APIs to provide you with better protection, less administrative complexity, and increased performance through cutting-edge agentless technology. Built to handle the rigors of virtual desktop environments, VMware and Trend Micro solutions maximize protection and security while preserving performance and increasing ROI.

Using virtual desktops can help you retain the control and security you need because your desktops are running on protected servers in your data center. Plus, with virtual endpoints, sensitive data is stored and protected in the data center when a device is lost or stolen. However, 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. With Trend Micro agentless antimalware running in the VMware environment, you get virtualization-aware security that combats threats specific to virtual environments while also maximizing performance.

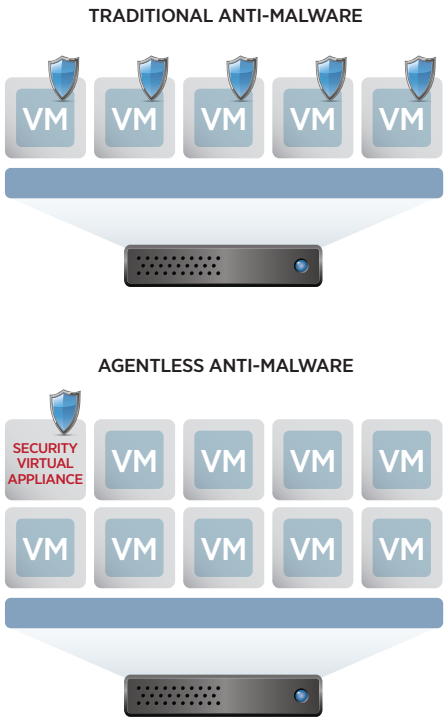
Unique Challenges in Virtual Desktop Environments

Both physical and virtual desktops need antimalware protection, but virtual desktop antimalware security must be designed for a shared resource environment. If traditional physical security is deployed, the antimalware across all of the individual virtual desktop instances can create performance degradation on the host—sabotaging the improved efficiencies you're trying to achieve with virtual desktops. And the ease of virtual desktop provisioning can make it difficult to keep virtual desktop security current. Only virtualization-aware security can combat these virtual desktop security challenges:

- Resource Contention: In virtual desktop deployments, numerous desktops share the host's hardware resources, often at a ratio of 60-to-1 or higher. Simultaneous security updates and full-system scans can result in a dramatic loss of desktop performance—limiting availability or reducing VM consolidation ratios.
- Instant-On Gaps: 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.
- 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 antimalware protection.

Optimize Virtual Desktop Security and Performance with Trend Micro

Compare the Traditional Antimalware Model to Agentless Antimalware



- Higher VD Densities
- Stronger Security
- Better Manageability
- Faster Performance

VMWARE AND TREND MICRO

Trend Micro Virtual and Cloud Security

- Deep Security for server and virtual desktop security
- SecureCloud for data protection

Trend Micro VMware Ready Security Virtual Appliances

- Web Security
- Messaging Security
- Email Encryption
- Data Loss Prevention

Trend Micro Agentless Security Appliances Designed for VMware Virtual Desktops

Trend Micro Deep Security integrates with VMware vShield Endpoint APIs to offer you agentless antimalware. This agentless security is ideal for your VMware View virtual desktops environment because it optimizes virtualization performance and reduces administrative complexity. 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. Resource-intensive operations, such as full system scans, are run from the separate scanning security virtual appliance.

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 machines and underlying host. And agentless security also reduces your administrative complexity with no agents to deploy, configure, or update.

Security Designed for Virtual Desktops Helps Drive Your Business Forward

- Increased virtual desktop ROI—Staggering updates and scans, and eliminating the agents off the guest virtual machines reduces the resource burden on the underlying host—maximizing your performance and increasing your virtual desktop consolidation ratios.
- Always-on, tamper-proof security—The dedicated, hardened security virtual appliance provides up-to-date protection for VMs throughout their lifecycle, including virtual patching.
- Enhanced visibility and control— Trend Micro Deep Security with VMware vShield Endpoint and VMware View provide detailed insight into virtual desktop security and simplify compliance of virtualized environments.

The power of virtual desktops can transform your organization. And Trend Micro integrated with VMware provides the security you need to optimize virtual desktop protection and performance. Everyone wins when you're providing your users access to their desktops, applications, and data anywhere, any time, on any device.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com