SOLUTION OVERVIEW

Protect Your Desktops with Agentless Security from VMware and Trend Micro

KEY BENEFITS

Protect virtualized desktops from the latest threats and

- **Deliver higher consolidation ratios** – Offload security scans from individual virtual machines to a single security virtual appliance on each VMware vSphere® host and significantly increase virtual-machine density.
- **Optimize resources** – Eliminate antivirus storms and resource contention from multiple security agents.
- **Simplify management** – Eliminate agents and the need to configure and update each one.
- **Enable stronger security** – Provide comprehensive and instant-on protection for virtual machines, coordinated by a single, dedicated security virtual appliance delivering five different protection mechanisms.

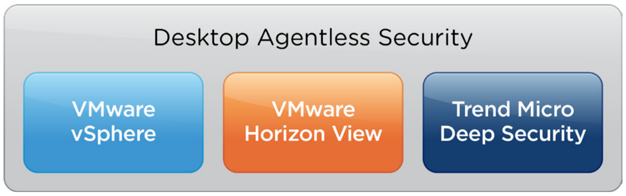
Overcome Security Challenges in Dynamic Environments

Every organization should use strong protection technologies to secure both virtualized and physical machines. Yet traditional agent-based security solutions, designed for physical machines, have proved ill-equipped to support virtual desktops. To prevent significant operational issues—increased consumption, antivirus storms, instant-on gaps and operational overhead—and effectively support virtualized environments, organizations need to deploy an agentless security solution that provides "better-than-physical" protection for their virtual machines.

Deploy Agentless Security to Protect Virtualized Desktops

Long-standing partners VMware and Trend Micro have teamed together to deliver the first agentless security solution designed for VMware software deployments. From the software-defined data center to virtual desktop infrastructure (VDI) and cloud deployments, the joint solution helps prevent threats, improve consolidation ratios, optimize resources, simplify management and enable stronger security across virtualized IT infrastructures.

The complete solution consists of the following components:



- **VMware vSphere®** – A proven virtualization foundation, vSphere helps to transform data centers into dynamic, easier-to-manage infrastructures for private, public and hybrid cloud environments. It includes a unique and comprehensive set of capabilities for high availability, security, resource optimization and business continuity. Included with vSphere is VMware vShield Endpoint™, which strengthens and optimizes security in vSphere and VMware Horizon View™ environments while improving performance for endpoint protection by orders of magnitude. vShield Endpoint enables offloading of security processing to dedicated security-hardened virtual machines—for example, offloading antivirus and antimalware agent processing to a dedicated secure virtual appliance, delivered by VMware partners.
- **VMware Horizon View** – Providing end users with workspace freedom of choice, Horizon View helps simplify IT management, increase security and improve control of end-user access. It also decreases IT costs by centrally delivering desktop services from a private, public or hybrid cloud. Horizon View enables highly available, scalable, secure and reliable desktop services unmatched by physical PCs.
- **Trend Micro Deep Security** – Trend Micro Deep Security provides a comprehensive security platform integrated with VMware APIs. After four years of releases and collaborative development with VMware, Deep Security is the first security product in the market to provide an agentless security platform comprising antimalware, Web

reputation, firewall, intrusion prevention and integrity monitoring through a single virtual appliance, thereby removing the need to provision each virtual machine with multiple in-guest security agents. Built to handle the rigors of virtual desktop environments, Deep Security delivers better protection, easier manageability, and improved resource efficiency and virtual-machine density, and it has proved itself in the real world over thousands of customer deployments.

Enhance and Optimize Security with vSphere

vSphere is the world's leading platform for building virtual and cloud infrastructure. It helps IT meet service-level agreements (SLAs) for the most demanding business-critical applications, at the lowest TCO. The VMware vSphere Hypervisor architecture includes a robust, production-proven, high-performance virtualization layer that allows multiple virtual machines to share hardware resources with performance that can match (and in some cases exceed) native throughput.

Included with vSphere, vShield Endpoint improves performance by offloading key security functions to a dedicated security appliance, eliminating the security-agent footprint in virtual machines. This advanced framework makes system resources available, speeds performance and eliminates the risk of security "storms"—that is, overloaded resources during scheduled scans and signature updates.

In combination with Trend Micro's hardened, tamper-proof Deep Security virtual appliance, vShield Endpoint enhances security by leveraging the strong and secure hypervisor introspection capabilities in vSphere. Together, these technologies prevent a compromise of protection capabilities. They also enable organizations to demonstrate compliance and satisfy auditor requirements, because the solution includes detailed activity logs.

To simplify IT management, vShield Endpoint can be centrally managed by administrators through the included VMware vShield Manager™ console. Already seamlessly integrated with VMware vCenter Server™, vShield Manager facilitates unified security management for virtual data centers.

Simplify IT and Boost ROI with Trend Micro Deep Security

Trend Micro Deep Security provides a comprehensive security platform designed to simplify security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules easily expand the platform to ensure system, application and data security across physical, virtual and cloud servers, as well as virtual desktops. Deep Security provides a wide range of agentless security options for VMware virtual machines, including antimalware, Web reputation, integrity monitoring, intrusion prevention and firewall capabilities. These security options integrate in the same virtual appliance for increased protection on VMware virtual machines. All of these modules and an additional module for log inspection are also available in the form of an integrated multifunction agent, enabling businesses to use a combination of agentless and agent-based deployment configuration that best supports their virtual desktops and their physical, virtual and cloud servers.

Learn How It Works

The agentless security solution from VMware and Trend Micro provides "better-than-physical" protection for virtual machines. The following capabilities enable the solution to resolve key operational issues:

- **Comprehensive monitoring eliminates instant-on gaps** – When virtual machines are activated and deactivated in rapid cycles, it is difficult to consistently provision security to those virtual machines and keep them up to date. Dormant virtual machines can eventually deviate so far from the baseline that simply powering them on introduces massive security vulnerabilities. As part of vSphere, vShield Endpoint enables agentless virtual-machine introspection, monitoring current, new and reactivated virtual machines to ensure up-to-date security.
- **Virtual appliance integration prevents antivirus (AV) storms** – When traditional AV solutions simultaneously initiate scans or scheduled security updates on all virtual machines on a single physical host, an "AV storm" can result, creating an extreme load on the system and reducing performance. Similar storms can occur with other types of scans and updates. Deep Security uses a dedicated, security-hardened virtual appliance that integrates with VMware vShield™ APIs to protect virtual machines from network- and file-based threats.
- **Efficient communication reduces resource consumption** – Traditional security occupies a significant amount of memory in each virtual machine, especially when multiple security agents are installed to provide a range of protection. This approach reduces consolidation ratios and increases CapEx and OpEx. vShield Endpoint enables Deep Security to communicate with the guest virtual machines to implement security such as antivirus, integrity monitoring, intrusion detection and prevention, Web application protection, application control and firewall services.
- **Agentless solution lowers operational overhead** – Administrators need to provision security agents in new virtual machines, continually reconfigure these agents as the virtual machines move around or change state, and roll out pattern updates on a regular basis. This can be extremely time-consuming and still result in security gaps. The joint solution enables security that protects the virtual server and desktop network and file systems without deploying in-guest security agents.

Protect Your Desktops and Improve IT Efficiency

Today, organizations using the joint Trend Micro and VMware solution are experiencing significantly higher virtual desktop consolidation ratios than organizations using leading physical desktop antimalware solutions. With multiple agentless security modules for VMware virtual machines now available—all on one security platform—now is the time to learn more about how our joint solution can help your organization protect virtualized data centers, desktops and cloud deployments from the latest threats while improving IT efficiency.

For information about agentless security or to purchase this joint solution from VMware, call 1-877-VMWARE (outside North America, +1-650-427-5000), visit http://www.vmware.com/products or search online for an authorized reseller. Additional information about Trend Micro Deep Security is available at http://www.trendmicro.com/deepsecurity.

vmware®

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