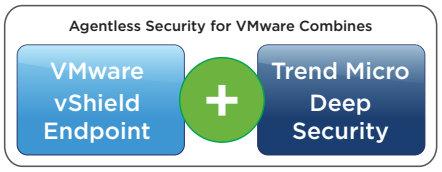
VMware vShield Endpoint + Trend Micro Deep Security

VMware vShield Endpoint + Trend Micro Deep Security Agentless Security for Virtual and Cloud Environments

KEY BENEFITS

This joint solution protects virtualized datacenters and desktops from the latest threats, while delivering

- **Higher density** by offloading security scans from individual virtual machines to a single security virtual appliance on each VMware vSphere® host
- **Optimized resources** by eliminating antivirus storms and resource contention from multiple security agents
- **Simplified management** by eliminating agents and the need to configure and update each one
- **Stronger security** by providing instant-on protection for new virtual machines and tamper-proof security coordinated by the dedicated security appliance



VMware and Trend Micro have partnered to deliver the first agentless security solution designed for VMware virtualized datacenters, desktops and cloud deployments.

Challenges of Traditional Agent-Based Security Solutions

Virtualized datacenters and desktops need to be secured by the same strong protection technologies as physical machines. However, traditional agent-based solutions not designed for virtualization can result in significant operational security issues. The VMware® and Trend Micro agentless security solution provides "better-than-physical" protection for virtual machines, resolving these issues:

- **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 reduces consolidation ratios and increases CapEx and OpEx.
- **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.
- **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.
- **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.

Solution Overview

VMware and Trend Micro have partnered to deliver the first agentless security solution designed for VMware® software-defined datacenters, desktops and cloud deployments. The joint solution includes the following components:

- **VMware vSphere®,** which delivers the foundation to transform datacenters into dynamic, simplified infrastructures for private, public and hybrid cloud environments. It includes the most comprehensive set of unique capabilities for availability, security, resource optimization and business continuity.
- **VMware vShield™ Endpoint™,** which is part of vSphere 5.1, optimizes security for use in vSphere and VMware View® environments. It enables offloading of security processing to dedicated security-hardened virtual machines delivered by VMware partners.
- **Trend Micro Deep Security™,** which provides a security-hardened virtual machine that integrates with vShield Endpoint and other VMware APIs to offer agentless antivirus, integrity monitoring, intrusion detection and prevention, firewall, virtual patching, and Web application protection for VMware virtual machines.

SOLUTION COMPONENTS

Trend Micro and VMware agentless security solution consists of these components:

- VMware vSphere
- VMware vShield Endpoint
- Trend Micro Deep Security (virtual appliance)

SECURITY PARTNER

Trend Micro is a leading VMware security partner. Trend Micro Deep Security is the first VMware security partner solution designed specifically to

- Integrate with VMware VMsafe® APIs
- Integrate with vShield Endpoint APIs
- Deliver agentless antimalware (feature available since 2010)
- Deliver multiple agentless security options

Optimizing Security with vShield Endpoint

VMware vShield Endpoint, part of VMware vSphere, improves performance by offloading key security functions to a dedicated security appliance, eliminating the security agent footprint in virtual machines. This advanced architecture frees up system resources, improves performance, and eliminates the risk of security "storms" (overloaded resources during scheduled scans and signature updates).

vShield Endpoint enhances security with a hardened, tamper-proof security virtual appliance (delivered by Trend Micro) that uses the robust and secure hypervisor introspection capabilities in vSphere, preventing compromise of the protection capabilities. Using detailed activity logs from the security service, organizations can demonstrate compliance and satisfy auditor requirements.

Administrators can centrally manage vShield Endpoint through the included VMware vShield Manager™ console, which integrates seamlessly with VMware vCenter Server™ to facilitate unified security management for virtual datacenters.

Simplified Security with Trend Micro Deep Security

Trend Micro Deep Security provides a comprehensive server 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 server, 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 antivirus, integrity monitoring, intrusion detection and prevention, Web application protection, application control and a bidirectional stateful firewall.

These security options integrate in the same virtual appliance for increased protection on VMware virtual machines. Agent-based security and log inspection are also available, enabling businesses to combine agentless and agent-based deployment configurations that best support their virtual desktops and their physical, virtual and cloud servers.

How It Works

- vShield Endpoint enables agentless virtual-machine introspection, monitoring current, new and reactivated virtual machines to ensure up-to-date security.
- 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.
- 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.
- This approach enables security that protects the virtual server and desktop network and file systems without deploying in-guest security agents.

Trend Micro and VMware now have more than 2500 customers enjoying the benefits of agentless security. Virtual desktop consolidation ratios are up to three times higher than those of leading physical desktop antimalware solutions. Multiple agentless security modules for VMware virtual machines are now available—all on one security platform.

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