Agentless Security
VMware vShield Endpoint + Trend Micro Deep Security

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 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 should be secured by the same strong protection technologies as physical machines. However, traditional agent-based solutions that are not designed for virtualization can result in several significant operational security issues. VMware and Trend Micro’s 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 VM, 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 VMs 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 agentless security for virtualized datacenters and desktop virtual machines. The joint solution comprises two mutually dependent solutions:

• **VMware vShield Endpoint™** is a unique solution that optimizes security for use in VMware 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™** Deep Security 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.
vShield Endpoint

vShield Endpoint is a unique solution that optimizes host and endpoint security for use in vSphere and View environments.

vShield Endpoint 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, tamperproof security virtual appliance (delivered by Trend Micro) that uses 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.

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. Trend Micro 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 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

1. vShield Endpoint enables agentless virtual machine introspection, monitoring current, new and reactivated virtual machines to ensure up-to-date security.

2. Deep Security uses a dedicated, security-hardened virtual appliance that integrates with vShield APIs to protect virtual machines from network- and file-based threats.

3. 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.

4. This approach enables security that protects the virtual server and desktop network and file systems without deploying in-guest security agents.