AGENTLESS SECURITY

Trend Micro Deep Security + VMware vShield Endpoint

VMware and Trend Micro have partnered to deliver the first agentless security platform architected for VMware virtualized data centers, virtual desktops, and cloud deployments.

Challenges with Traditional Agent-based Security Solutions

Virtualized data centers, desktops, and cloud computing should be secured by the same strong protection technologies as physical machines. However, traditional agent-based solutions that are not architected for virtualization can result in a number of significant operational security issues. VMware and Trend Micro's agentless security provides "better-than-physical" protection for virtual and cloud environments. A single platform integrates security technologies and resolves operational security issues:

- **Resource consumption:** Even when idle, traditional security agents occupy a significant amount of memory in each virtual machine (VM), especially when multiple security agents are installed on each VM to provide a range of protection. This reduces VM consolidation ratios and increases CAPEX and OPEX.
- **Security storms:** When protecting VMs, traditional security solutions do not realize they are in a shared resource environment. Scans or scheduled updates simultaneously initiate across all VMs on a physical host. The result is a "security storm" that causes an extreme load on the system and reduces overall performance. This resource impact is particularly significant with traditional antivirus solutions, but these "storms" can occur with other types of security scans and updates as well.
- **Instant-on gaps:** When VMs are activated and inactivated in rapid cycles, it is difficult to consistently provision security to those virtual machines and keep them up to date. Dormant VMs 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 VMs, continually reconfigure these agents as the VMs move around or change state, and rollout pattern updates to them on a regular basis. This can be extremely time consuming and result in security gaps.

Solution Overview

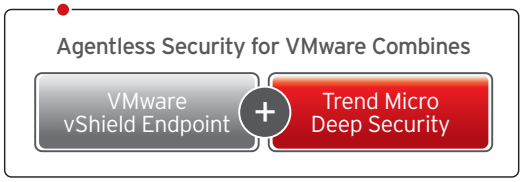
VMware and Trend Micro have partnered to deliver agentless security for virtualized data centers, virtual desktops, and cloud environments. The joint solution comprises two mutually dependent solutions:

- **VMware vShield Endpoint™** is a unique solution that optimizes security for use in VMware vSphere™ and VMware View™ environments. It enables agentless security through the offloading of security processing to dedicated security-hardened virtual machines delivered by VMware partners.
- **Trend Micro™ Deep Security** provides a security-hardened virtual machine that integrates with VMware vShield Endpoint and other VMware APIs to offer agentless antivirus, integrity monitoring for both files and hypervisor, intrusion detection and prevention, firewall, Web application protection, and application control for VMware virtual machines. Additional integration with VMware vCenter and vCloud Director coordinates security management across VMware virtual and cloud deployments.

Benefits

This joint solution provides full protection for VMware virtualized data centers, virtual desktops, and cloud deployments from the latest threats, while delivering:

- **Higher Density** by offloading security scans from individual VMs to a single security virtual appliance on each vSphere host
- **Optimized Resources** by eliminating security storms and resource contention from multiple security agents
- **Simplified Management** by removing agents and the need to configure and update each one
- **Stronger Security** by providing instant-on protection for new VMs and tamper-proof security coordinated by the dedicated security appliance



VMware vShield Endpoint

VMware vShield Endpoint is a unique solution that optimizes host and endpoint security for use in VMware vSphere™, VMware View™, and vCloud 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 security 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. Demonstrating compliance and satisfying auditor requirements are enabled through detailed logging of activity from the security service.

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 for VMware VMs, including antivirus, integrity monitoring for files and hypervisor, intrusion detection and prevention, Web application protection, application control, and bidirectional stateful firewall. And features such as virtual patching and agentless recommendation scan automate rule configuration for all VMs from the virtual appliance.

These security options provide integrated agentless security for increased protection on VMware virtual machines deployed in virtual data centers or vCloud-based private clouds, or even vCloud-based public clouds in which agentless security is offered by the service provider. Agent-based security is also available for these security options as well as log inspection, allowing businesses to combine agentless and agent-based deployment configurations that best support their physical and virtual servers, private, public, and hybrid clouds, and virtual desktops.

Deep Security Manager integrates with VMware vCenter™ Server (coordinates with vShield Endpoint and vShield Manager) as well as vCloud Director to facilitate unified security management across both agentless and agent-based protection for VMs in the VMware virtualized data center, virtual desktops, and cloud.

How It Works

1. VMware vShield Endpoint enables agentless VM introspection, monitoring current, new, and reactivated VMs to ensure up-to-date security.
2. Trend Micro Deep Security uses a dedicated, security-hardened virtual appliance that integrates with the VMware vShield and other APIs to protect VMs from network- and file-based threats.
3. VMware vShield Endpoint enables Trend Micro Deep Security to communicate with the guest VMs to implement security such as antivirus, integrity monitoring for files and hypervisor, intrusion detection and prevention, Web application protection, application control, and firewall.
4. Integration with vCenter and vCloud Director enables Deep Security Manager to provide unified management and common security policies across data center and cloud-based VMs.
5. This agentless approach enables security that protects virtual server and desktop network and file systems in virtual data center and cloud environments without deploying in-guest security agents.

Solution Components

Trend Micro agentless security for VMware consists of these components:

Core components

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

Additional VMware platform products needed

- VMware ESX/ESXi (at least one)
- VMware vCenter
- VMware View (only required for virtual desktops)
- VMware vShield Manager
- VMware vCloud Director (for cloud deployments)

Trend Micro is a Leading VMware Security Partner

Trend Micro Deep Security

- The first VMware security partner solution architected specifically to:
  - Integrate with VMware API's for network-based protection (IDS/IPS, firewall, etc.)
  - Integrate with vShield Endpoint APIs for file-based protection (AV, integrity monitoring)
  - Deliver agentless antimalware—available since 2010
  - Deliver multiple agentless security options—all in one security platform
- 4th generation of VMware integration
- Significantly higher VM densities over leading traditional agent-based security solutions as demonstrated by real world customer deployments
- Increased ROI with agentless architecture proven at thousands of customer implementations