VMware vShield Endpoint

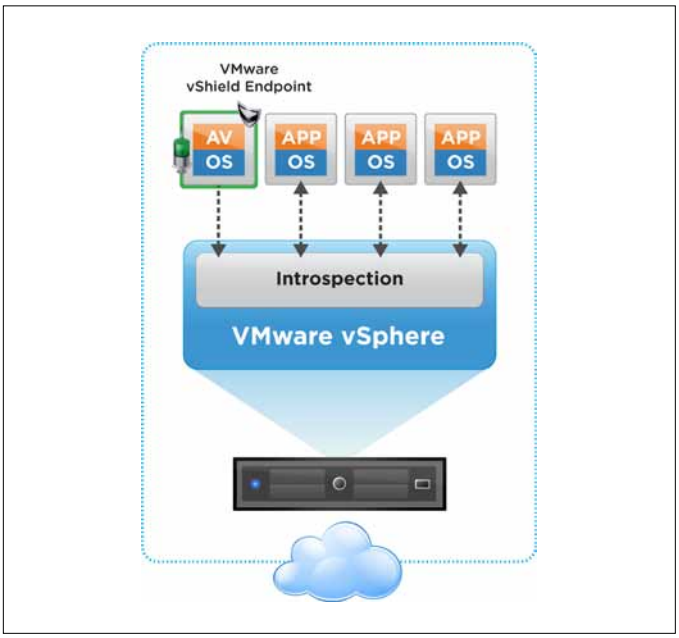
Enhanced Endpoint Security and Performance for Virtual Datacenters

AT A GLANCE

VMware vShield™ Endpoint strengthens security for virtual machines while improving performance for endpoint protection by orders of magnitude. vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. The solution is designed to leverage existing investments by allowing customers to manage antivirus and anti-malware policies for virtualized environments with the same management interfaces they use to secure physical environments.

KEY BENEFITS

- Improve consolidation ratios and performance by eliminating antivirus agents from guest virtual machines.
- Streamline antivirus and anti-malware deployment and monitoring in VMware environments.
- Improve security by consolidating antivirus software agents to reduce the attack surface.
- Satisfy compliance and audit requirements through logging of antivirus and anti-malware activities.



vShield Endpoint improves performance and consolidation ratios for antivirus and anti-malware in virtualized environments.

What is vShield Endpoint?

vShield Endpoint revolutionizes the thinking behind how to protect guest virtual machines from viruses and malware. The solution optimizes antivirus and other endpoint security for use in VMware vSphere® and VMware View™ environments.

vShield Endpoint improves performance by offloading virus-scanning activities from each virtual machine to a secure virtual appliance that has a virus-scanning engine, as well as the stored antivirus signatures. For antivirus and anti-malware functions, this architecture eliminates the software agent footprint in guest virtual machines, frees up system resources, improves performance and eliminates the risk of antivirus "storms" (overloaded resources during scheduled scans and signature updates). Because the secure virtual appliance - unlike a guest virtual machine – doesn't go offline, it can continuously update antivirus signatures, giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

vShield Endpoint enhances security with a hardened, tamper-proof secure virtual appliance (delivered by VMware partners) that uses the robust and secure hypervisor introspection capabilities in vSphere, reducing the vulnerability of the antivirus and anti-malware service itself.

vShield Endpoint also provides VMware partners with interfaces to implement not just file scanning, but also memory and process scanning. Organizations can simultaneously use multiple security solutions; for example, they can use the sensitive data discovery capability in VMware vShield App with Data Security in one secure virtual appliance while using an antivirus solution in another secure virtual appliance.

Organizations can demonstrate compliance and satisfy audit requirements through detailed logging of activity from the antivirus or anti-malware service.

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

How Does vShield Endpoint Work?

vShield Endpoint plugs directly into vSphere and consists of three components:

- Hardened secure virtual appliances, delivered by VMware partners
- Thin agent for virtual machines to offload security events (included in VMware Tools)
- VMware Endpoint ESX® hypervisor module to enable communication between the first two components at the hypervisor layer

For example, in the case of an antivirus solution, vShield Endpoint monitors virtual machine file events and notifies the antivirus engine, which scans and returns a disposition. The solution supports both on-access and on-demand (scheduled) file scans initiated by the antivirus engine in the secure virtual appliance.

When remediation is necessary, administrators can specify actions to take using their existing antivirus and anti-malware management tools, and vShield Endpoint manages remediation actions within the affected virtual machines.

How is vShield Endpoint Used?

The management console provided by the VMware partner is used to configure and control the partner's software hosted in the secure virtual appliance. VMware partners can provide a user interface that makes the management experience (including policy management) exactly like managing software hosted on a dedicated physical security appliance.

Virtual infrastructure administrators have a vastly reduced level of effort because virtual machines have no antivirus agents to manage. Instead, the partner's management console is used to manage the secure virtual appliance. This approach also avoids the need to administer frequent updates per virtual machine. For deployment, VMware Tools includes the thin agent, and the ESX module enables hypervisor introspection.

Virtual infrastructure administrators can easily monitor deployments to determine, for example, whether an antivirus solution is operating properly.

Key Features

Antivirus and Anti-Malware Offloading

- vShield Endpoint improves performance by using the vShield Endpoint ESX module to offload virus-scanning activities to a secure virtual appliance where the antivirus scanning is enforced.
- Tasks such as file, memory and process scanning are offloaded from virtual machines to a secure virtual appliance through a thin client agent and partner ESX module.
- vShield Endpoint EPSEC manages communication between virtual machines and the secure virtual appliance, using introspection at the hypervisor layer.
- Antivirus engine and signature files are updated only within the security virtual appliance, but policies can be applied across all virtual machines on a vSphere host.

Remediation

- vShield Endpoint enforces antivirus policies that dictate whether a malicious file should be deleted, quarantined or otherwise handled.
- Thin agent manages file remediation activity within the virtual machine.

Partner Integrations

- The EPSEC API enables VMware anti-virus partners to integrate with vShield Endpoint by providing introspection into file activity in the hypervisor. Essential anti-virus functions are supported through this API.

vShield Manager, Policy Management and Automation

- vShield Manager provides full-featured deployment and configuration of vShield Endpoint.
- Representational State Transfer (REST) APIs allow customized, automated integration of vShield Endpoint capabilities into solutions.
- Monitoring reports provided.
- vShield Manager can be leveraged as a vCenter plug-in.

Logging and Auditing

- Event logging is based on industry-standard syslog format.

Supported Releases

For information on supported releases of vSphere, ESX, and View environments, visit http://vmware.com/products.

Related Products

The vShield family of security products also includes VMware vShield Edge for perimeter security; vShield App with Data Security to protect applications from network-based attacks and discover sensitive data; vShield Manager; and vShield Bundle, which includes all products.

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the VMware vShield Administration Guide at http://www.vmware.com/pdf/vshield_41_admin.pdf.

For additional information on vShield products, visit http://vmware.com/products.

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