DATASHEET

VMware vShield Endpoint

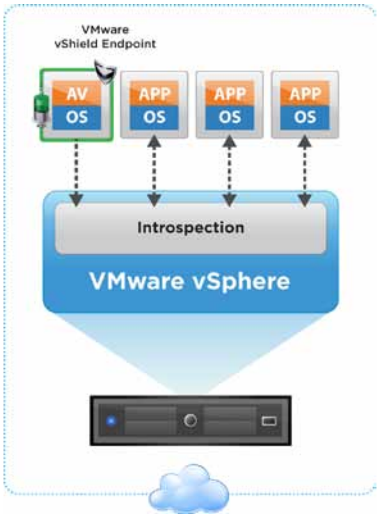
Endpoint Security for Virtual Datacenters

AT A GLANCE

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

KEY BENEFITS

- Streamline and accelerate antivirus and anti-malware deployment.
- Improve virtual machine performance and eliminate antivirus and anti-malware bottlenecks.
- Reduce risk by eliminating agents susceptible to attacks, and enforce remediation more easily.
- Satisfy audit requirements with detailed logging of antivirus and anti-malware activities.



VMware vShield Endpoint streamlines and optimizes antivirus and anti-malware deployments for virtualized environments.

What is VMware vShield Endpoint?

VMware vShield Endpoint is a unique solution that optimizes antivirus and other host and endpoint security for use in VMware vSphere™ 4.1 and VMware View™ 4.5 environments.

vShield Endpoint improves performance by offloading key antivirus and anti-malware functions to a security virtual machine, eliminating the antivirus agent footprint in virtual machines. This advanced architecture frees up system resources, improves performance of antivirus and anti-malware functions and eliminates the risk of antivirus “storms” (overloaded resources during scheduled scans and signature updates).

vShield Endpoint enhances security with a hardened, tamper-proof security virtual machine (delivered by VMware partners) that uses robust and secure hypervisor introspection capabilities in vSphere, preventing compromise of the antivirus and anti-malware service itself. Demonstrating compliance and satisfying auditor requirements are enabled through detailed logging of activity from the antivirus or anti-malware service.

Administrators can centrally manage VMware 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 VMware vShield Endpoint Work?

vShield Endpoint protects virtual machines and their hosts against viruses, malware and other threats. vShield Endpoint plugs directly into vSphere and consists of three components:

1. Hardened security virtual machine (delivered by VMware partners)
2. Driver for virtual machines to offload file events
3. VMware Endpoint Security (EPSEC) loadable kernel module (LKM) to link the first two components at the hypervisor layer

vShield Endpoint monitors virtual machine file events and notifies the antivirus engine, via VMware EPSEC, which scans and returns a disposition. It also supports scheduled full and partial file scans initiated by the antivirus engine in the security virtual machine.

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

How Is VMware vShield Endpoint Used?

Streamline antivirus and anti-malware deployment – With vShield Endpoint, administrators only need to deploy the enterprise antivirus engine and signature file to a single security virtual machine instead of each and every individual virtual machine on a vSphere host.

Improve virtual machine performance – vShield Endpoint helps organizations securely achieve higher consolidation ratios by offloading activities such as antivirus and anti-malware scans from individual virtual machines to a single security virtual machine on each vSphere host.

Prevent antivirus storms and bottlenecks – Administrators can use vShield Endpoint to prevent antivirus storms and prevent bottlenecks associated with multiple simultaneous antivirus and anti-malware scans and updates.

Protect Antivirus security software from attack – vShield Endpoint lets administrators deploy and run the antivirus and anti-malware client software in a hardened security virtual machine to prevent attacks that target antivirus and anti-malware solutions.

Key Features

Antivirus and Anti-Malware Offloading

- File scanning and other tasks are offloaded from virtual machines to a security virtual machine.
- VMware EPSEC LKM manages communication between virtual machines and the security virtual machine, using introspection at the hypervisor layer.

Antivirus and Anti-Malware Service Across Virtual Machines

- Antivirus engine and signature files are only updated within the security virtual machine, but policies can be applied across all virtual machines on a vSphere host.

Enforce Remediation

- Pre-defined policies dictate whether a malicious file should be deleted, quarantined or otherwise handled.
- vShield Endpoint driver manages file remediation activity within the virtual machine.

Partner Integrations

- Integration of VMware vShield Endpoint with security virtual machine solutions from VMware partners is facilitated through VMware EPSEC, which provides a library and API for introspection into file activity at the hypervisor layer.

Policy and Configuration Management

- vShield Manager provides full-featured configuration of vShield Endpoint policies.
- vCenter activates vShield capabilities on vSphere.
- REST APIs allow customized integration of vShield Endpoint capabilities into solutions.

Logging and Auditing

- Logging is based on syslog standard.
- REST APIs and vShield Manager provide access to third-party logging and auditing tools.
- Administrator defines logging on/off for antivirus and anti-malware file activity such as scanning.

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside of North America dial 650-427-5000), visit www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and systems requirements, refer to the VMware vShield Endpoint Administration Guide.