VMware vShield Endpoint

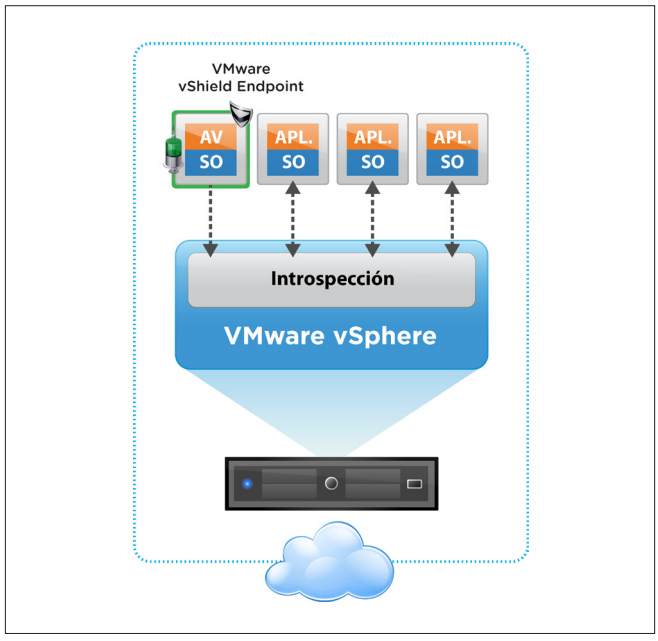
Seguridad y rendimiento mejorado de los puntos de acceso para los centros de datos virtuales

INFORMACIÓN BÁSICA

VMware vShield™ Endpoint refuerza la seguridad de las máquinas virtuales y mejora significativamente el rendimiento de protección de los puntos de acceso. vShield Endpoint descarga el procesamiento de agentes antivirus y contra software malintencionado a un dispositivo virtual seguro, dedicado en exclusiva a esta finalidad, proporcionado por los partners de VMware. La solución se ha diseñado para aprovechar las inversiones existentes permitiendo a los clientes gestionar las políticas antivirus y contra software malintencionado aplicadas a los entornos virtualizados con las mismas interfaces de gestión que se utilizan para proteger los entornos físicos.

PRINCIPALES VENTAJAS

- Mejore la proporción de consolidación y el rendimiento eliminando los agentes antivirus de las máquinas virtuales guest.
- Racionalice la implementación y supervisión de programas antivirus y contra software malintencionado en entornos de VMware.
- Mejore la seguridad consolidando los agentes del software antivirus para reducir la superficie de ataque.
- Satisfaga los requisitos de cumplimiento y auditoría gracias al registro de actividades de antivirus y contra software malintencionado.



vShield Endpoint mejora el rendimiento y la proporción de consolidación para los programas antivirus y contra el software malintencionado en entornos virtualizados.

¿Qué es vShield Endpoint?

vShield Endpoint revoluciona la manera de plantearse cómo proteger las máquinas virtuales guest contra virus y software malintencionado. La solución optimiza los servicios de antivirus y la seguridad de los puntos de acceso para su uso en entornos de VMware vSphere® y VMware View™.

vShield Endpoint mejora el rendimiento porque descarga las actividades de análisis antivirus de cada máquina virtual a un dispositivo virtual seguro donde se encuentra el motor de análisis antivirus y se almacenan las firmas del antivirus. Para las funciones de antivirus y contra software malintencionado, esta arquitectura elimina el espacio que ocupan los agentes de software en las máquinas virtuales guest, libera recursos del sistema, mejora el rendimiento y elimina el riesgo de "tormentas" de antivirus (sobrecarga de los recursos durante los análisis programados y las actualizaciones de firmas). Dado que, al contrario que las máquinas virtuales guest, el dispositivo virtual seguro no se desconecta, puede actualizar continuamente las firmas del antivirus, con lo cual proporciona una protección ininterrumpida a las máquinas virtuales del host. Además, las nuevas máquinas virtuales (o las existentes que se habían desconectado) se protegen de inmediato con las firmas de antivirus más recientes en el momento en que entran online.

vShield Endpoint mejora la seguridad con un dispositivo virtual seguro, reforzado y a prueba de manipulaciones (proporcionado por los partners de VMware), que utiliza las capacidades robustas y seguras de introspección de hipervisor de vSphere, de tal forma que reduce la vulnerabilidad del propio servicio de antivirus y contra software malintencionado.

Por añadidura, vShield Endpoint proporciona a los partners de VMware interfaces que permiten implementar el análisis no solo de los archivos, sino también de la memoria y los procesos. Las organizaciones pueden utilizar varias soluciones de seguridad simultáneas; por ejemplo, pueden usar la funcionalidad de detección de datos confidenciales de VMware vShield App with Data Security en un dispositivo virtual seguro mientras usan una solución de antivirus en otro.

Las organizaciones pueden demostrar el cumplimiento y satisfacer los requisitos de auditoría gracias al registro detallado de actividades del servicio de antivirus o contra software malintencionado.

Los administradores pueden gestionar vShield Endpoint de forma centralizada mediante la consola vShield Manager incluida, que se integra perfectamente con VMware vCenter™ Server para facilitar la gestión unificada de la seguridad en los centros de datos virtuales.

¿Cómo funciona vShield Endpoint?

vShield Endpoint se conecta directamente a vSphere y consta de tres componentes:

- Dispositivos virtuales seguros reforzados, suministrados por los partners de VMware
- Agente ligero para que las máquinas virtuales descarguen los eventos de seguridad (incluido en VMware Tools)
- Módulo de hipervisor de VMware Endpoint ESX® para permitir la comunicación entre los dos primeros componentes en la capa de hipervisor

Por ejemplo, para una solución de antivirus, vShield Endpoint supervisa los eventos de archivos de las máquinas virtuales y se los notifica al motor antivirus, que realiza un análisis y devuelve una disposición. La solución admite análisis al realizar el acceso y según demanda (programados) iniciados por el motor antivirus en el dispositivo virtual seguro.

Cuando es necesaria una solución, los administradores pueden especificar las acciones que se deben tomar con las herramientas existentes de gestión de programas antivirus y contra software malintencionado, y vShield Endpoint gestiona las acciones en las máquinas virtuales afectadas.

¿Cómo se utiliza vShield Endpoint?

La consola de gestión que el partner de VMware proporciona se utiliza para configurar y controlar el software del partner alojado en el dispositivo virtual seguro. Los partners de VMware pueden proporcionar una interfaz de usuario que permite que la experiencia de gestión (incluida la gestión de políticas) resulte exactamente igual que la gestión del software alojado en un dispositivo de seguridad físico dedicado.

El esfuerzo de los administradores de la infraestructura virtual se reduce drásticamente, porque las máquinas virtuales no poseen agentes antivirus que haya que gestionar. En cambio, la consola de gestión del partner se utiliza para gestionar el dispositivo virtual seguro. Este enfoque también evita la necesidad de administrar actualizaciones frecuentes en todas y cada una de las máquinas virtuales. Para la implementación, VMware Tools incluye el agente ligero, mientras que el módulo de ESX permite la introspección de hipervisor.

Los administradores de la infraestructura virtual pueden supervisar con facilidad las implementaciones para determinar, por ejemplo, si una solución de antivirus funciona correctamente.

Características principales

Descarga de los programas antivirus y contra software malintencionado

- vShield Endpoint mejora el rendimiento usando el módulo vShield Endpoint ESX para descargar las actividades de análisis antivirus a un dispositivo virtual seguro que se encarga de realizarlas.
- Varias tareas, como el análisis de archivos, memoria y procesos, se descargan de las máquinas virtuales a un dispositivo virtual seguro a través de un agente de cliente ligero y un módulo de ESX del partner.
- La función EPSEC de vShield Endpoint gestiona la comunicación entre las máquinas virtuales y el dispositivo virtual seguro mediante introspección en la capa de hipervisor.
- El motor antivirus y los archivos de firma solo se actualizan en el dispositivo virtual seguro, pero se pueden aplicar políticas en todas las máquinas virtuales de un host vSphere.

Reparación

- vShield Endpoint aplica políticas de antivirus que dictan cuándo se debe eliminar o poner en cuarentena un archivo malintencionado, o qué se debe hacer con él.
- Un agente ligero gestiona la actividad de reparación de archivos en la máquina virtual.

Integraciones de partners

- El API EPSEC permite a los partners de antivirus de VMware integrar sus soluciones con vShield Endpoint, porque proporciona introspección de la actividad de archivos en el hipervisor. Las funciones antivirus esenciales se admiten gracias a esta API.

vShield Manager, gestión y automatización de políticas

- vShield Manager proporciona implementación y configuración completas de vShield Endpoint.
- Las API basadas en la transferencia de estado representacional (REST) permiten una integración personalizada y automatizada de las funcionalidades de vShield Endpoint en las soluciones.
- Se generan informes de supervisión.
- vShield Manager se puede utilizar como complemento de vCenter.

Registro y auditoría

- El registro de eventos se basa en el formato estándar del sector syslog.

Versiones compatibles

Para obtener información sobre versiones compatibles de entornos de vSphere, ESX y View, visite http://vmware.com/products.

Productos relacionados

La familia vShield de productos de seguridad incluye asimismo VMware vShield Edge para la seguridad perimetral; vShield App with Data Security para proteger las aplicaciones contra ataques basados en la red y detectar datos confidenciales; vShield Manager; y vShield Bundle, que engloba todos los productos.

Más información

Para obtener más información o comprar productos de VMware, llame al +34 91 412 50 00 en España (o marque el 877-4-VMWARE si se encuentra en Norteamérica o el +1-650-427-5000 desde el resto del mundo), visite la página web www.vmware.com/products o busque un reseller autorizado online. Para obtener especificaciones de productos y requisitos del sistema detallados, consulte la guía de administración de VMware vShield en http://www.vmware.com/pdf/vshield_41_admin.pdf.

Para obtener información adicional sobre productos de vShield, visite 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.
C/ Rafael Botí 26 - 2ª planta. 28023 Madrid. Tfno: +34 91 412 50 00 Fax: +34 91 412 50 01 www.vmware.com/es