FICHA TÉCNICA

McAfee Security Suite for Virtual Desktop Infrastructure

La seguridad que necesita con un impacto mínimo en el rendimiento

La adopción de equipos de escritorio virtuales ya es una realidad, pero estas soluciones deben incorporar una seguridad sólida que proteja a las empresas sin ocasionar problemas de rendimiento ni afectar a la densidad de servidores prevista. Las soluciones antivirus tradicionales no funcionan bien en una infraestructura virtualizada. ¿La respuesta? McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), que ofrece una seguridad completa y optimizada para equipos de escritorio virtuales.

McAfee Security Suite for VDI proporciona protección antimalware optimizada para entornos virtuales, listas blancas para protegerse de amenazas de tipo zero-day, protección frente a intrusiones en computadoras de escritorio y protección de datos. También alerta a los usuarios sobre sitios web maliciosos y/o los bloquea.

Arquitectura de análisis optimizada

Debido a la naturaleza dinámica de las computadoras de escritorio virtuales, es preciso que su gestión sea especialmente meticulosa. Las imágenes deben mantenerse libres de malware mientras están offline o analizarse inmediatamente cuando los usuarios inician una sesión. Las soluciones antimalware no son los únicos servicios que se inician y, a menudo, los usuarios comienzan a trabajar en grupos, lo que genera picos de "bombardeos antivirus", que consumen todos los recursos e impiden a los usuarios iniciar una sesión.

Para eliminar retrasos y cuellos de botella en el proceso de análisis, McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) transfiere las operaciones de análisis, configuración y actualización de archivos DAT desde las imágenes individuales del sistema invitado a un dispositivo virtual u Offload Scan Server seguro. Generamos y mantenemos una caché global de los archivos analizados para garantizar que una vez que se ha confirmado que un archivo ha sido analizado y está limpio, las máquinas virtuales (VM) posteriores que acceden a ese archivo no tengan que esperar a que sea analizado. De esta forma, los recursos de memoria asignados a cada máquina virtual se reducen y pueden devolverse al grupo de recursos disponibles para optimizar su uso. La planificación inteligente de análisis bajo demanda garantiza que los análisis no interfieran en el funcionamiento del hipervisor.

Ventajas principales

- Ofrece descubrimiento y visibilidad con el software McAfee ePO y Cloud Workload Discovery.
- Proporciona una combinación exclusiva de listas blancas y listas negras para proteger los equipos virtuales frente al malware.
- Optimiza la seguridad para entornos virtuales de manera que tengan un impacto mínimo en el rendimiento.
- Añade protección frente a intrusiones y para la Web con protección de la memoria y protección de aplicaciones web.
- Aprovecha el software McAfee ePO para obtener visibilidad rápida, control e informes de todos los endpoints.
- Permite el despliegue flexible, multiplataforma y sin agentes.
- Admite el aprovisionamiento elástico de analizadores offline para ampliar en función de la demanda (multiplataforma).
- Integra inteligencia de reputación local para facilitar una respuesta más rápida a las amenazas (multiplataforma).

Administración de directivas específicas

La consola de McAfee® ePolicy Orchestrator® (McAfee ePO™) permite configurar las directivas y los controles que determinan el funcionamiento de McAfee MOVE AntiVirus. Los datos de computadoras de escritorio se pueden acumular y combinar con los de otros sistemas en paneles e informes unificados. Los administradores pueden configurar una directiva única por máquina virtual, grupo de recursos, clúster o centro de datos a través de Cloud Workload Discovery, adaptando sus necesidades de seguridad específicamente a la composición del centro de datos.

Despliegue sin agente para VMware

McAfee MOVE AntiVirus aprovecha VMware NSX o VMware vCNS para aumentar la eficacia. Para despliegues sin agente, utilizan el hipervisor como conexión de alta velocidad para permitir al dispositivo de máquina virtual de seguridad (SVM) de McAfee MOVE AntiVirus analizar las máquinas virtuales desde fuera de la imagen de invitado. Durante el análisis, el dispositivo SVM indicará a VMware NSX o VMware vCNS que guarde en caché los archivos limpios, o que elimine, ponga en cuarentena o deniegue el acceso a los archivos maliciosos.

Tras instalar y configurar el SVM de VMware y los componentes VMware NSX o VMware vCNS en los servidores VMware ESX, además de instalar el controlador para endpoints de VMware NSX o VMware vCNS en las máquinas virtuales de invitado, todas las imágenes quedan automáticamente protegidas sin necesidad de instalar nuestro software en cada máquina virtual cliente. Con nuestra implementación con vMotion, las máquinas virtuales pueden trasladarse de un host a otro y seguir perfectamente protegidas por el dispositivo SVM en el host de destino, sin que se vean afectados los análisis ni la experiencia de los usuarios.

La integración de McAfee MOVE AntiVirus con vCNS permite supervisar el estado del SVM en VMware vCenter y recibir alertas si el dispositivo SVM pierde la conectividad. El software McAfee ePO recibe datos de eventos sobre las máquinas virtuales concretas que puedan haber sufrido una infección. La integración profunda con NSX sincroniza las directivas creadas en el software McAfee ePO y las reglas asignadas en VMware NSX. El etiquetado automático de las máquinas virtuales vulnerables sin protección antimalware o las máquinas con malware permite poner en cuarentena inmediatamente las máquinas virtuales a través del firewall de VMware NSX.

Multiplataforma para todos los hipervisores

En instalaciones multiplataforma, el agente McAfee MOVE AntiVirus —un componente endpoint sencillo— se comunica con el servidor McAfee MOVE Offload Scan Server para supervisar el proceso antivirus en nombre de cada computadora de escritorio virtual. Un agente del software McAfee ePO administra las directivas y las funciones de análisis. También es posible designar una imagen de referencia y analizarla para utilizarla como referencia maestra limpia. Como resultado, un administrador puede rellenar previamente las cachés globales con imágenes limpias para agilizar el arranque de las computadoras de escritorio virtuales.

Configuración de McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Despliegue multiplataforma
  - Despliegue sin agente
- Cloud Workload Discovery para nube privada (VMware y OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- Tecnología McAfee SiteAdvisor® Enterprise
- McAfee ePolicy Orchestrator

FICHA TÉCNICA

Cuando un usuario accede a un archivo, el servidor McAfee MOVE Offload Scan Server realiza un análisis en tiempo real, que devuelve una respuesta a la máquina virtual. Los usuarios pueden recibir notificaciones sobre los problemas a través de una alerta emergente y los archivos pueden ponerse en cuarentena hasta que se tome una decisión. Se puede configurar cada equipo de escritorio virtual con directivas individuales específicas definidas en la consola del software McAfee ePO o bien se puede optar por administrar los equipos virtuales como un grupo.

Como las cargas de trabajo aumentan y disminuyen en despliegues multiplataforma, se pueden añadir o eliminar automáticamente dispositivos SVM desde el grupo de recursos para aumentar o disminuir su capacidad, lo que proporciona una capacidad de adaptación ilimitada y una utilización eficiente de los recursos. Las notificaciones de eventos ayudan a los administradores a comprender las tendencias de uso de SVM para optimizar la administración de recursos.

McAfee MOVE AntiVirus en despliegues multiplataforma mejora la inteligencia de reputación global de McAfee Global Threat Intelligence con datos locales de McAfee Threat Intelligence Exchange, un módulo adicional, que se vende por separado, para identificar y combatir de forma instantánea el número cada vez mayor de muestras de malware únicas. Gracias a McAfee Threat Intelligence Exchange, McAfee MOVE AntiVirus se coordina con McAfee Advanced Threat Defense para analizar de forma dinámica el comportamiento de las aplicaciones desconocidas en un entorno aislado (o sandbox) e inmuniza de manera automática a todos los endpoints frente al malware que se acaba de detectar.

Función	Por qué necesita esta solución
Seguridad para la virtualización	▪ Mejora de la seguridad de las cargas de trabajo desplegada en infraestructuras de escritorio virtuales sin comprometer el rendimiento ni la utilización de recursos. ▪ Despliegue sin agente optimizado para VMware para mejorar el rendimiento y la densidad de máquinas virtuales. No es necesario instalar/actualizar nuestros agentes en cada equipo de escritorio virtual, lo que reduce la complejidad y mejora enormemente la facilidad de uso. ▪ Despliegue multiplataforma para todos los hipervisores que admite el aprovisionamiento elástico de analizadores offline para adaptarse a la demanda y se integra con inteligencia de reputación local para facilitar una respuesta más rápida a las amenazas.
Protección esencial de endpoints	▪ La protección antivirus de McAfee analiza con más rapidez, utiliza menos memoria, requiere menos ciclos de CPU y protege mejor que ningún otro producto. ▪ Prevención de intrusiones en host para proteger a las empresas de las amenazas de seguridad complejas que pueden introducirse de manera intencionada o no. ▪ McAfee SiteAdvisor® Enterprise impide a los usuarios interaccionar con sitios web peligrosos y permite la personalización de directivas para restringir el acceso a sitios web potencialmente peligrosos, asegurando así el cumplimiento de las directivas.

FICHA TÉCNICA

Función	Por qué necesita esta solución
Listas blancas de aplicaciones	▪ Reducción significativa del impacto en el rendimiento del host en comparación con los controles de seguridad de endpoints tradicionales. ▪ Protección contra las amenazas persistentes avanzadas (APT) y de tipo zero-day sin actualizaciones de firmas, lo que disminuye el tiempo que se tarda en conseguir protección. ▪ Uso de listas blancas dinámicas, que requieren menos gastos generales operativos que las listas tradicionales.
Cloud Workload Discovery	▪ Proporciona visibilidad total de las cargas de trabajo de la nube privada y sus plataformas subyacentes para identificar controles de seguridad deficientes.
Protección para archivos y soportes extraíbles (cifrado)	▪ Cifrado mucho más sencillo y con menos riesgos con protección de archivos y soportes extraíbles. ▪ Rendimiento casi nativo en hosts cifrados mediante la implementación optimizada de la tecnología Intel® AES-NI. ▪ Cifrado automático, transparente e implementado por directivas de archivos y carpetas y de soportes extraíbles (unidades USB, CD, DVD). ▪ Permite a los usuarios cifrar soportes USB extraíbles y transferir la información de manera segura. ▪ Permite el acceso seguro a los datos en recursos compartido de red.
Administración centralizada con el software McAfee ePO	▪ Administración de forma centralizada de despliegues físicos, virtuales y en la nube para disponer de un mejor control de la seguridad, incluida la administración de directivas, el despliegue, la visibilidad y la administración de la seguridad en todas las plataformas. ▪ Simplificación de los procesos operativos y reducción del tiempo que emplea el personal administrativo. ▪ Costos de hardware inferiores debido a una reducción de servidores.

Más información

Las soluciones de McAfee le ofrecen la seguridad que necesita con un mínimo impacto en el rendimiento. Visite **www.mcafee.com/mx/products/data-center-security-suite-for-vdi.aspx**.

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx