FICHA TÉCNICA

McAfee Management for Optimized Virtual Environments AntiVirus

Seguridad para su nube privada sin sacrificar el rendimiento

Las soluciones antivirus tradicionales no funcionan bien con una infraestructura virtualizada. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) ofrece protección antimalware optimizada y avanzada para sus computadoras de escritorio y sus servidores virtualizados. Puede implementarla en varios hipervisores, o elegir la opción sin agente, especial para VMware NSX o VMware vCNS. En cualquiera de los casos, tendrá seguridad de primera clase para la detección y la contención de amenazas inmediata con un mínimo impacto en el rendimiento de las máquinas virtuales. McAfee MOVE AntiVirus optimiza la protección antimalware para despliegues virtualizados, lo que libera los recursos del hipervisor, además de garantizar que los análisis de seguridad se realizan de acuerdo con las directivas.

Control de análisis optimizado

Debido a la naturaleza dinámica de las computadoras de escritorio invitadas y los servidores virtuales, es preciso que la gestión sea especialmente meticulosa. Las imágenes deben estar libres de malware cuando los usuarios inician una sesión. Esto puede ser difícil, ya que, 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 MOVE AntiVirus transfiere las operaciones de análisis, configuración y actualización de archivos DAT desde las imágenes individuales del sistema invitado a un servidor de análisis de descarga seguro. Generamos y mantenemos una caché global de los archivos analizados para garantizar que, una vez que se ha analizado un archivo y se ha confirmado que está limpio, las máquinas virtuales (VM) que accedan a él con posteridad no tengan que esperar a que sea analizado. De esta forma, disminuyen los recursos de memoria asignados a cada máquina virtual y pueden devolverse al grupo de recursos disponibles para optimizar su uso.

Ventajas principales

- **Evita los análisis en busca de malware:** protección inmediata con un impacto mínimo en la memoria y el procesamiento.
- **Previene los bombardeos antivirus:** las opciones incluyen análisis en tiempo real y bajo demanda.
- **Permite un despliegue flexible:** multiplataforma (para todos los hipervisores principales, máquinas virtuales Windows) o sin agente (máquinas virtuales VMware, Windows y Linux).
- **Mejora la optimización de recursos:** aprovisionamiento elástico de analizadores offline con notificaciones de eventos (multiplataforma).
- **Bloquea las amenazas desconocidas de tipo zero-day, en segundos:** inteligencia de reputación local combinada con análisis de comportamientos en un entorno aislado o *sandbox*, (multiplataforma, el módulo adicional se vende por separado).

McAfee MOVE AntiVirus permite utilizar directivas diferentes para análisis en tiempo real y bajo demanda para facilitar la ejecución de seguridad adaptada. Por ejemplo, los administradores pueden asumir un nivel de riesgo razonable para análisis en tiempo real con el fin de evitar que se reduzca el rendimiento y utilizar análisis bajo demanda con directivas más estrictas en otro momento posterior cuando el impacto en el rendimiento sea menor.

Visibilidad total e integral en todas las nubes

La falta de visibilidad dificulta la implementación de directivas de seguridad adecuadas para entornos virtualizados. McAfee Cloud Workload Security (McAfee CWS) abarca entornos in situ, de nube privada y de nube pública, como VMware y OpenStack, para ofrecer una visión completa de los centros de datos virtuales e introducir las propiedades clave, como los servidores, hipervisores y máquinas virtuales, en la consola de McAfee ePO. Una vez que los administradores consiguen visibilidad del estado de seguridad de todas sus máquinas virtuales y pueden monitorizar las relaciones hipervisor-máquina virtual casi en tiempo real, proteger el centro de datos virtual es mucho más fácil. Un panel personalizable muestra el estado del análisis de seguridad, resúmenes ejecutivos y datos del historial de seguridad de los activos.

McAfee CWS Essentials y McAfee CWS Advanced amplían la visibilidad y el control a las nubes públicas Amazon Web Services (AWS) y Microsoft Azure, y a los servidores físicos.

Administración de directivas específicas

La consola de McAfee ePO que ya conoce le permite configurar las directivas y los controles para McAfee MOVE AntiVirus. Puede acumular los datos virtuales con los que obtiene de sus sistemas físicos y nubes públicas para disfrutar de paneles e informes unificados. Los administradores pueden configurar una directiva única por máquina virtual, clúster o centro de datos a través de McAfee Cloud Workload Security, adaptando su seguridad específicamente a la composición del centro de datos.

Otras funciones de McAfee MOVE AntiVirus

Administración y visibilidad:

- Planificación instantánea de análisis bajo demanda de una máquina virtual o en un grupo de máquinas virtuales.
- Aumento de la precisión de análisis con análisis bajo demanda selectivos.
- Despliegue automático de un analizador offline en cada hipervisor a través de la integración con VMware NSX Service Composer.
- Información sobre problemas relacionados con paneles, informes y alertas de correo electrónico.

Simplificación del despliegue y la configuración:

- Despliegue y configuración de un analizador offline en varios hipervisores (sin agente).
- Restauración de los archivos en cuarentena mediante la consola de McAfee ePO (multiplataforma).

Ventajas principales (continuación)

- **Emplea la consola McAfee® ePolicy Orchestrator® (McAfee ePO™):** visibilidad integral y control de los despliegues físicos, virtuales y en la nube.

Configuraciones de McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
  - Despliegue multiplataforma
  - Despliegue sin agente
- Cloud Workload Security para nube privada (VMware y OpenStack)
- Software McAfee ePO

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
  - Despliegue multiplataforma
  - Despliegue sin agente
- Cloud Workload Security para nube privada (VMware y OpenStack)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Protección de memoria y protección de aplicaciones web
- Software McAfee ePO

- Diagnósticos detallados para el ajuste del rendimiento antivirus.
- Administración sencilla de directivas sin agente y multiplataforma.

Opción 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 Security Virtual Machine (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, junto con 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 los productos de McAfee con VMware vCNS permite supervisar el estado del SVM en VMware vCenter y recibir alertas si el dispositivo SVM pierde la conectividad. La consola de McAfee ePO recibe datos de eventos sobre las máquinas virtuales concretas que puedan haber sufrido una infección. La integración profunda con VMware NSX sincroniza las directivas creadas en la consola de 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.

Se admite el despliegue sin agente simultáneo de McAfee MOVE AntiVirus con VMware vCNS y VMware NSX, lo que facilita enormemente a los clientes de VMware vCNS la transición a VMware NSX.

Multiplataforma para todos los principales hipervisores

En instalaciones multiplataforma, como vSphere, Hyper-V, KVM y XenServer, el agente McAfee MOVE AntiVirus —un componente endpoint sencillo— se comunica con el dispositivo SVM para supervisar el proceso antivirus en nombre de cada máquina virtual. El agente McAfee MOVE AntiVirus mantiene una caché local y administra las directivas y las funciones de análisis. Puede designar una imagen de referencia y analizarla para utilizarla como referencia maestra limpia. Al llenar las cachés globales con imágenes limpias, el tiempo de arranque de las máquinas virtuales se reduce al máximo.

Cuando un usuario accede a un archivo, 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 maliciosos pueden eliminarse, denegar el acceso a los mismos o ponerse en cuarentena.

Como la demanda de análisis fluctúa 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 (McAfee GTI) con datos locales obtenidos de McAfee Threat Intelligence Exchange, un módulo adicional, que se vende por separado, para identificar y combatir de forma instantánea el número creciente 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. La integración de McAfee MOVE AntiVirus con McAfee Network Security Platform a través de McAfee Threat Intelligence Exchange proporciona una estrategia de seguridad por capas para ofrecer una protección unificada del perímetro y de las máquinas virtuales.

Administración de directivas unificada para despliegues sin agente y multiplataforma

Muchas empresas pueden querer aprovechar la capacidad de McAfee MOVE AntiVirus de admitir tanto despliegues sin agente como multiplataforma. McAfee MOVE AntiVirus ofrece a los administradores de seguridad la capacidad de definir y administrar directivas de seguridad coherentes utilizando un punto de extensión en la consola de McAfee ePO, de manera que la administración de ambos métodos se realiza de manera sencilla y sin complicaciones.

FICHA TÉCNICA

Arquitectura	Despliegue multiplataforma	Despliegue sin agente
Compatibilidad con plataforma de hipervisor	Todos los principales hipervisores, incluidos VMware, Citrix, Hyper-V y KVM	VMware
Plataforma de análisis	Windows 2008, Windows 2012 R2, Windows Server 2016, Windows 10 R4 y RS5	Linux Ubuntu 16.04
Escalabilidad de despliegue	Un dispositivo SVM puede proteger máquinas virtuales de varios hipervisores. Los dispositivos SVM se pueden aprovisionar de manera elástica.	Un dispositivo SVM por host ESX
Comunicación con máquinas virtuales	A través de la red	A través del supervisor
Protección de máquinas virtuales	Windows	Windows y Linux

Más información

Las soluciones de McAfee le ofrecen la seguridad que necesita y la flexibilidad que merece.

Encontrará más información en **www.mcafee.com/mx/products/move-anti-virus.aspx**.

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

OCTUBRE DE 2018