McAfee Security Suite for Virtual Desktop Infrastructure

La seguridad que necesita y la flexibilidad que merece

La adopción de equipos de sobremesa virtuales (VDI) ya es una realidad, pero estas soluciones deben incorporar una sólida seguridad 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 VDI, que ofrece una seguridad completa optimizada para equipos de sobremesa virtuales.

Ventajas principales

- Descubrimiento y visibilidad de entornos VMware vSphere con el software McAfee ePO y McAfee Data Center Connector for VMware vSphere. Combinación única de listas negras y blancas que protege del malware a equipos físicos y virtuales.
- Seguridad optimizada para entornos virtuales con un impacto mínimo en el rendimiento.
- Protección frente a amenazas desconocidas al impedir la ejecución de aplicaciones no deseadas en los equipos de sobremesa virtuales.
- Protección añadida frente a intrusiones y la Web con un firewall para equipos de sobremesa, protección de la memoria y protección de aplicaciones web.
- Aprovechamiento del software McAfee ePO para obtener visibilidad de un vistazo, control y generación de informes de todos los endpoints.

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 ordenadores de sobremesa y protección de datos. También alerta a los usuarios sobre sitios web maliciosos y les impide acceder a ellos.

Arquitectura de análisis optimizada

Debido a la naturaleza dinámica de los ordenadores de sobremesa 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 (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.

Administración de directivas específicas

La consola del software McAfee® ePolicy Orchestrator® (McAfee ePO™) permite configurar las directivas y los controles que determinan el funcionamiento de McAfee MOVE AntiVirus. Los datos de ordenadores de sobremesa 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 McAfee Data Center Connector, adaptando sus necesidades de seguridad específicamente a la composición del centro de datos.

intel Security

Configuración de McAfee Security Suite for VDI

McAfee MOVE AntiVirus for Virtual Desktops (VDI)

- McAfee MOVE AntiVirus
  - Despliegue con múltiples hipervisores
  - Despliegue sin agente
- McAfee Data Center Connector for vSphere
- Software McAfee VirusScan® Enterprise for Windows
- Software McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- Tecnología McAfee SiteAdvisor® Enterprise
- Software McAfee ePolicy Orchestrator

Despliegue sin agente para aprovechar la eficacia de VMware vShield

Para despliegues sin agente, VMware vShield Endpoint utiliza el hipervisor como conexión de alta velocidad para permitir al dispositivo McAfee MOVE AntiVirus Security Virtual Appliance analizar las máquinas virtuales desde fuera de la imagen de invitado. Durante el análisis, el dispositivo SVA indicará a vShield que guarde en caché los archivo limpios, o que elimine, ponga en cuarentena o deniegue el acceso a los archivos maliciosos.

Tras instalar y configurar el dispositivo SVA y los componentes necesarios de vShield en los servidores ESX, además de instalar el controlador de vShield en las máquinas virtuales invitadas, todas las imágenes estarán protegidas automáticamente desde el momento de su creación. No es necesario instalar software de McAfee 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 SVA en el host de destino, sin que se vean afectados los análisis ni la experiencia de los usuarios. La integración con McAfee permite supervisar el estado del SVA en vCenter y recibir alertas si el dispositivo SVA pierde la conectividad. El software McAfee ePO recibe datos de eventos sobre las máquinas virtuales concretas que puedan haber sufrido una infección.

Múltiples hipervisores para cumplir las normativas y mejorar la facilidad de uso

En instalaciones con varios hipervisores, el agente McAfee MOVE AntiVirus —un componente endpoint sencillo— se comunica con el servidor Offload Scan Server para supervisar el proceso antivirus en nombre de cada ordenador de sobremesa 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 los ordenadores de sobremesa virtuales.

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 sobremesa 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.

Más información

Las soluciones de McAfee le ofrecen la seguridad que necesita y la flexibilidad que merece. Visite **www.mcafee.com/es/products/data-center-security-suite-for-vdi.aspx**.

Función	Por qué necesita esta solución
Seguridad para la virtualización	• Mejora de la seguridad de las cargas de trabajo desplegada en infraestructuras de sobremesa virtuales sin comprometer el rendimiento ni la utilización de recursos. • Opciones de despliegue con varios hipervisores y sin agente: despliegue para entornos virtualizados de varios proveedores (VMware, Citrix, Hyper-V). • Despliegue sin agente optimizado para VMware para mejorar el rendimiento y la densidad de máquinas virtuales. No es necesario instalar/actualizar agentes de McAfee en cada equipo de sobremesa virtual, lo que reduce la complejidad y mejora enormemente la facilidad de uso.
Protección esencial de endpoints	• Protección antivirus para servidores físicos que NSS Labs considera número uno en la protección frente a exploits de tipo zero-day y ataques de evasión. • 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.
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 requiere menos gastos generales operativos que las listas tradicionales.
Visibilidad total de las máquinas virtuales en las nubes privadas	• Descubrimiento automático de máquinas virtuales en las nubes privadas (VMware vSphere).
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	• Capacidad de gestión en un solo panel de máquinas físicas y virtuales, incluidas las de las nubes públicas y privadas, para una mayor visibilidad de la seguridad. • Simplificación de los procesos operativos y la inversión de tiempo necesario para el personal administrativo. • Costes de hardware inferiores debido a una reducción de servidores.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com