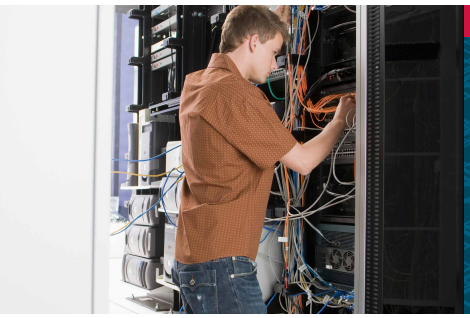

Extender la virtualización, mantener la seguridad

Decisiones de seguridad esenciales para infraestructuras virtualizadas

Dado que la virtualización de servidores y equipos de sobremesa es cada vez más crítica para las empresas, los equipos de TI se ven obligados a dar soporte a más usuarios, más carga de trabajo y más regiones geográficas, así como a responder a exigencias nuevas como el aprovisionamiento "just in time" y el autoservicio. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) adapta los sistema de seguridad a las especiales necesidades técnicas y de administración de la virtualización. Contribuye a aprovechar con seguridad las eficiencias de la virtualización, además de conseguir que la experiencia de los usuarios sea positiva.

Las tecnologías de virtualización son la prioridad número uno de los planes de los directores de informática para 2012[1]. Gracias a su compatibilidad con programas clave como la informática en la nube, el uso de los dispositivos propiedad de los empleados y la consolidación de servidores y centros de datos, la virtualización ayuda a conseguir dos objetivos: el ahorro en costes y la flexibilidad organizativa. La virtualización es esencial para tener éxito, pero plantea retos operativos y de gestión de riesgos diferentes a los de las instalaciones de seguridad física tradicionales. El nuevo modelo operativo que supone la virtualización requiere evaluar los procesos de seguridad, las directivas y las decisiones de despliegue tradicionales.

Cuellos de botella

El problema más evidente es el rendimiento de los análisis. En los despliegues tradicionales, cada sistema —equipo de sobremesa o servidor— ejecuta el antimalware de forma local, y realiza los análisis en el momento del acceso o según una programación para garantizar que el host no se infecte. No obstante, el modelo "por nodo" consume demasiados recursos en los entornos virtuales. Durante los eventos llamados "tormentas de análisis", esta operación puede consumir toda la memoria y capacidad de procesamiento del hipervisor e impedir que los usuarios abran sesiones nuevas. Durante años, muchos administradores optaron por desactivar el análisis o no aplicar las actualizaciones de software para proteger el rendimiento.

Sin embargo, como plataforma empresarial de corriente dominante, los entornos virtualizados se han convertido en la frontera para los ciberdelincuentes que aprovechan las vulnerabilidades del software y de las configuraciones. Sin herramientas de análisis de seguridad actualizadas y activas, las infraestructuras virtualizadas son campo abonado para los ladrones de información y otros atacantes.

Software de seguridad sin actualizar

El primer objetivo de un delincuente son las imágenes que se ejecutan sin antimalware o con antimalware no actualizado. El software de seguridad debe estar siempre en funcionamiento tanto en las imágenes online y offline como en las plantillas de imágenes. Solo las funciones de seguridad de sistemas y el contenido antimalware actualizados serán eficaces contra los atacantes.

Cuando la infraestructura de equipos de sobremesa virtualizados (VDI) crece, puede llegar a dar soporte a miles de máquinas virtuales (VMs) que entran en servicio y se retiran a diario, por lo que el mantenimiento de las herramientas de seguridad es menos predecible. Si bien las actualizaciones de seguridad de los servidores físicos que siempre están en funcionamiento pueden planificarse para el momento adecuado —cuando el uso es bajo—, las actualizaciones de seguridad de los usuarios de equipos de sobremesa deben tener en cuenta los flujos dinámicos de las VMs. Las imágenes activas estarán offline, se almacenarán y estarán inactivas durante la noche, o quizá durante algunas horas, después de lo cual los usuarios esperan tener acceso inmediato a sus sistemas virtualizados sin que las operaciones de inicio y análisis lo retrasen.

Mezcla de activos

Los centros de datos agregan aún más complejidad a los procesos. Servidores, sistemas de almacenamiento y redes se mezclan para que sean utilizados al máximo, pero esta mezcla tiene dos efectos. En primer lugar, se pierden las ventajas de la separación física de las bases de datos, los servidores de aplicaciones y web, y otros tipos de software. El aislamiento físico frustra las esperanzas de expansión de los autores de malware y hackers. En cambio, es necesario diseñar una seguridad más robusta para los sistemas virtualizados.

En segundo lugar, los procesos de gestión tienen que cambiar, dado que los servidores, sistemas de almacenamiento y las redes anteriormente separados ahora comparten la misma consola de administración. Esos recursos solían tener administradores y directivas diferenciados, pero ahora deben coexistir en un mismo entorno de directivas y procedimientos, a menudo gestionados por un solo administrador de la virtualización, un "superusuario". Ante esta situación, procesos y alertas compiten por la visibilidad de la administración y es necesario normalizar las directivas. Los administradores deben encontrar la manera de colaborar de forma operativa.

Múltiples proveedores

Muchas organizaciones añaden a estos cambios el desafío que plantea la diversidad de proveedores. Los distintos proveedores de soluciones de virtualización tienen fortalezas diferentes y muchas empresas requieren una segunda fuente para el software más crítico. Como resultado, las instalaciones pueden contar con una mezcla de hipervisores. Las imágenes tienen que protegerse, es necesario informar de que cumplen las normativas y además tener en cuenta los distintos atributos de cada producto.

"McAfee MOVE [AntiVirus] AV protege el entorno virtual de McKesson frente al código malicioso de forma integral y coherente. Ya que seguimos adoptando las tecnologías más recientes, en particular las soluciones de informática en la nube, la implementación de McAfee MOVE [AntiVirus] AV ofrece seguridad adicional a nuestro entorno virtual. La solución hace que el dimensionamiento y el despliegue sean más sencillos y garantiza que todos los sistemas cuentan con el mismo nivel de protección".

Patrick Enyart
Director ejecutivo
McKesson Information Security

Cumplimiento

Como si estos problemas no fueran suficientes, es necesario demostrar que los sistemas virtualizados satisfacen las expectativas de cumplimiento de normativas que se imponían y se siguen imponiendo a los sistemas físicos. Las regulaciones actuales especifican el mantenimiento regular del antimalware. Por ejemplo, la ley de protección de datos de Massachusetts (201 CMR 17:00) exige "versiones razonablemente actualizadas de los agentes de seguridad de sistemas, que deben incluir protección antimalware, parches y definiciones de virus, o una versión de dicho software que todavía reciba soporte con parches y definiciones de virus actualizadas, y que esté configurado para recibir actualizaciones de seguridad con regularidad".

Todos estos problemas suponen preocupaciones de orden práctico para las operaciones de seguridad diarias de los sistemas virtualizados en un panorama de amenazas dinámico. Los modelos de seguridad tradicionales del mundo físico deben extenderse —o reemplazarse— a favor de una seguridad optimizada para el mundo de la virtualización.

Operaciones optimizadas con McAfee MOVE

Cuando McAfee empezó a colaborar con la comunidad de virtualización hace ya varios años, vimos que los problemas operativos comenzaban a aparecer. Dimos respuestas con tecnología especializada para que nuestras mejores funciones de seguridad funcionaran eficientemente en las instalaciones de servidores y equipos de sobremesa virtualizados. McAfee MOVE AntiVirus ofrece seguridad y protección frente al malware sin poner en peligro el rendimiento, para poder sacar el máximo partido de las posibilidades de la tecnología de virtualización y mantener la productividad de los usuarios y la seguridad de los sistemas operativos invitados en las VMs.

Nuestra solución ofrece la flexibilidad de poder elegir el modelo de instalación preferido —que trabaje en varias plataformas de virtualización— o una opción "sin agente" que aprovecha las APIs de VMware vShield. Ambas opciones aprovechan al máximo el antimalware de McAfee, líder de la industria[2]. Además, la prevención de intrusiones y la capa de seguridad para aplicaciones web agregan protección adicional frente a los atacantes maliciosos.

Análisis: solo cuando es posible y necesario

McAfee MOVE AntiVirus libera recursos del hipervisor para destinarlos a otras funciones, al tiempo que garantiza que los análisis de seguridad actualizados se ejecutan de acuerdo con las directivas. Un dispositivo virtual o físico reforzado se hace cargo de la responsabilidad de procesar los análisis, mantener las configuraciones y actualizar los .DATs de firmas, de forma que el hipervisor se dedique a dar soporte a las imágenes invitadas.

La integración de McAfee MOVE AntiVirus con el software de administración para entornos virtuales permite evitar las "tormentas de análisis" provocadas por la solicitud de análisis inmediatos de parte de muchas imágenes. Es más, McAfee MOVE AntiVirus for Virtual Servers puede programar análisis de forma inteligente basándose en la disponibilidad del hipervisor y los recursos. No es necesario tener las VMs offline para analizarlas. Sin embargo, cuando están offline, McAfee puede analizarlas y actualizarlas para mantenerlas listas para usarse.

Uso de la información más reciente

McAfee MOVE AntiVirus protege las VMs con el mismo motor McAfee VirusScan® que utilizamos en nuestros productos antivirus para el mundo físico, líderes en el sector. Para que los análisis sean lo más actualizados posible sin disminuir el rendimiento, el dispositivo descarga y aplica las firmas más recientes al servidor de análisis y no a las VMs. McAfee MOVE AntiVirus consulta McAfee Global Threat Intelligence™ para obtener en tiempo real la reputación de los archivos cuando parecen sospechosos.

Más allá del análisis antimalware, McAfee MOVE AntiVirus for Virtual Desktops incluye un firewall para equipos de sobremesa y protección avanzada de memoria para limitar las actividades maliciosas y preservar la integridad de los archivos. Para ayudar a los usuarios a evitar los sitios web peligrosos que podrían introducir malware en la imagen mientras está operativa, McAfee también incluye alertas de reputación web y controles basados en directivas sobre el uso de la Web. Todas estas herramientas reducen la superficie de ataque de los sistemas virtualizados. Para conseguir la protección más robusta, pueden incluirse otras herramientas como las listas blancas de aplicaciones para impedir que aplicaciones o malware no deseados interrumpan las operaciones.

Seguridad en las redes

La virtualización también cambia la forma en que las organizaciones abordan la seguridad de las redes. Cuando las infraestructuras físicas se virtualizan, se necesitan nuevas estrategias para crear y mantener fronteras de seguridad en ausencia de particiones físicas. Otro problema es la portabilidad de las VMs y el impacto en las directivas de seguridad de redes. Las organizaciones necesitan contar con la capacidad de aplicar una seguridad uniforme a las redes con independencia de la ubicación física de las aplicaciones y servidores virtualizados.

McAfee ofrece una seguridad de redes integrada para entornos tanto físicos como virtualizados. McAfee Network Security Platform incluye inspecciones nativas de entornos virtuales gracias a la integración con la API de seguridad de redes de VMware vShield. Permite inspeccionar el tráfico e imponer el cumplimiento de directivas en y entre máquinas virtuales, con independencia de donde residan físicamente. Además, el acceso nativo a las herramientas VMware vCenter permite integrar la seguridad de las redes en los entornos virtuales.

Administración integral

McAfee MOVE AntiVirus utiliza McAfee ePolicy Orchestrator® (McAfee ePO™), el mismo entorno de administración de las herramientas de McAfee para la seguridad de endpoints físicos, información y redes que los administradores ya conocen. Desde un solo sistema de directivas y una única consola, cada administrador puede crear paneles personalizados para supervisar su información y lo que sea de su interés, así como generar informes de recursos específicos, como una mezcla de hosts físicos y virtuales, tanto endpoints como servidores. Esta compatibilidad de roles facilita que la seguridad se ajuste a la administración colaborativa de los centros de datos virtualizados. McAfee ePO también se integra con más de 100 productos de partners de McAfee Security Innovation Alliance, de forma que la TI pueda simplificar los flujos de trabajo de la infraestructura tecnológica.

Estandarización o especialización

Las opciones de implementaciones multiplataforma o sin agente significan que es posible mantener las relaciones con los proveedores actuales y futuros. La solución multiplataforma utiliza un agente ligero en cada imagen invitada para gestionar las directivas y los análisis, es decir, aprovecha el servidor de descarga para realizar análisis en el momento del acceso. Este método permite combinar los hipervisores de Citrix, VMware y Microsoft y conseguir una mayor flexibilidad o alojar distintos grupos de usuarios.

La alternativa sin agente se integra con VMware para aprovechar la inversión en este hipervisor. McAfee MOVE AntiVirus trabaja con VMware vShield Endpoint para analizar las máquinas virtuales fuera de las imágenes invitadas, sin que se ejecute ningún software de McAfee dentro de las propias imágenes. Con VMware vMotion, las máquinas virtuales analizadas pueden moverse de un host a otro sin afectar a los usuarios ni a los sistemas de análisis. La integración de McAfee ePO con VMware vCenter simplifica la supervisión y la gestión de incidentes.

Cumplimiento de normativas continuo

La plataforma McAfee ePO permite garantizar que las directivas de los entornos físicos y virtuales sean coherentes. Para ayudar a los procesos de cumplimiento de normativas, se puede crear una vista de auditoría de los datos pertinentes y generar informes ad hoc o planificados de conformidad con las regulaciones.

De cara al futuro

Ahora es posible adaptar la seguridad a los requisitos de la virtualización. McAfee ha optimizado las protecciones antimalware y de endpoints para que operen dentro del diseño y los procesos que logran que la virtualización sea eficiente. El análisis no obstaculiza a los usuarios activos, y el software de seguridad y los procesos de actualización de firmas respetan la naturaleza online y offline constante de las imágenes de los equipos de sobremesa y los servidores.

El diseño flexible permite trabajar con los proveedores de preferencia y aún así cumplir las normativas de seguridad. McAfee ayuda a obtener todas las ventajas de la virtualización, y evita que los usuarios y los datos se conviertan en presas de los ciberdelincuentes de hoy día. Seguimos invirtiendo en la integración y optimización de toda nuestra cartera de productos para que sea posible desplegar la seguridad más robusta con la mayor eficiencia cuando aumenta el uso de la virtualización.

Para obtener más información acerca de McAfee MOVE AntiVirus, acceda a www.mcafee.com/es/solutions/virtualization/virtualization.aspx o póngase en contacto con su representante o reseller de McAfee.

McAfee
An Intel Company

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es

[1] http://www.informationweek.com/news/storage/virtualization/232400150
[2] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

45601brf_virtualization_0512_fnl_ETMG