McAfee Cloud Workload Security

Proteja las cargas de trabajo de su infraestructura híbrida. Con más seguridad, más rapidez y más facilidad.

Ante la evolución de los centros de datos de las empresas, cada vez se migran más cargas de trabajo a los entornos de la nube. La mayoría de las empresas cuentan con un entorno híbrido con una combinación de cargas de trabajo in situ y en la nube, incluidos contenedores, que están en constante cambio. Esto introduce un riesgo para la seguridad, ya que los entornos en la nube (tanto privada como pública) requieren nuevos métodos y herramientas para su protección. Las empresas necesitan visibilidad centralizada de todas las cargas de trabajo en la nube, y total seguridad frente a errores de configuración, malware y fugas de datos.

McAfee® Cloud Workload Security (McAfee® CWS) automatiza el descubrimiento y la defensa de los contenedores y las cargas de trabajo elásticas, con el fin de eliminar los puntos ciegos, proporcionar seguridad frente a las amenazas avanzadas y simplificar la administración de varias nubes. McAfee ofrece una protección que permite, con una sola directiva automatizada, garantizar la seguridad de todas sus cargas de trabajo en su tránsito por los entornos privados, públicos y multinube virtuales, con el fin de facilitar la excelencia operativa a sus equipos de ciberseguridad.

Seguridad moderna para las cargas de trabajo: casos prácticos

Descubrimiento automático

La existencia de instancias de cargas de trabajo y contenedores Docker no gestionados genera brechas en la seguridad y ofrece a los ciberdelincuentes un hueco para infiltrarse en su empresa. McAfee CWS descubre las instancias de cargas de trabajo elásticas y contenedores Docker en entornos de Amazon Web Services (AWS), Microsoft Azure, OpenStack y VMware. También supervisa continuamente la presencia de nuevas instancias. Así, disfrutará de una visión centralizada e integral de todos los entornos y eliminará los puntos ciegos para las operaciones y la seguridad que pueden dar lugar a riesgos de ataque.

Principales ventajas

- La visibilidad continua de instancias de cargas de trabajo elásticas elimina los "puntos ciegos" y, al mismo tiempo, automatiza los despliegues de directivas que tanto trabajo requerían en el pasado.
- La administración centralizada y las cargas de trabajo automatizadas reducen drásticamente la complejidad de los entornos híbridos y multinube.
- Visualice y descubra las amenazas para la red sin necesidad de instalar un agente.
- La defensa frente a amenazas optimizada para máquinas virtuales ofrece medidas de corrección multicapa.
- La integración con herramientas de automatización, como Chef y Puppet, permite aplicar la seguridad a las cargas de trabajo públicas y privadas en el momento del despliegue.

Síganos

Información detallada sobre el tráfico de red

Gracias al uso del tráfico de red nativo que proporcionan las cargas de trabajo en la nube, McAfee CWS es capaz de reforzar y aplicar la inteligencia de las fuentes de datos de McAfee® Global Threat Intelligence (McAfee® GTI). La información enriquecida permite mostrar propiedades como la puntuación de riesgo, la geolocalización, y otra información importante sobre la red. Esta información se puede utilizar para crear medidas de corrección automatizadas para proteger las cargas de trabajo.

Integración en las infraestructuras de despliegue

McAfee CWS crea scripts de despliegue para permitir el despliegue y la administración automáticas del agente de McAfee® para cargas de trabajo en la nube. Estos scripts permiten la integración en herramientas como Chef, Puppet, y otras infraestructuras DevOps para el despliegue del agente de McAfee para cargas de trabajo que ejecutan proveedores de servicios en la nube, como AWS y Microsoft Azure.

Consolidación de eventos

McAfee CWS permite a las empresas utilizar una sola interfaz para administrar numerosas tecnologías de medidas de corrección para entornos in situ y en la nube. Esto incluye la integración con otras tecnologías, como AWS GuardDuty, McAfee® Policy Auditor y McAfee® Network Security Platform.

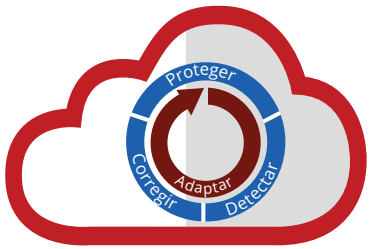
- Los administradores pueden aprovechar la supervisión continua y la identificación de comportamientos no autorizados que ofrece AWS GuardDuty, para disfrutar de otro nivel más de visibilidad de amenazas. Esta integración permite a los clientes de McAfee CWS ver los eventos de GuardDuty, que incluyen conexiones de red, sondeos de puerto y solicitudes DNS para instancias EC2, directamente desde la consola de McAfee CWS.
- McAfee Policy Auditor realiza comprobaciones basadas en el agente respecto a auditorías de configuración conocidas o definidas por el usuario para garantizar el cumplimiento con normativas como la ley Health Insurance Portability and Accountability Act (HIPAA), el estándar de seguridad de datos para la industria de las tarjetas de pago, PCI-DSS, los parámetros de seguridad y privacidad del Center for Internet Security (CIS Benchmark) u otros estándares de la industria. McAfee CWS informa sobre cualquier auditoría no satisfactoria para disponer de una visibilidad instantánea de los errores de configuración para cargas de trabajo en la nube.
- McAfee Network Security Platform es otra plataforma de seguridad en la nube que inspecciona el tráfico de red en entornos híbridos, así como de AWS y Microsoft Azure. Lleva a cabo inspecciones más profundas a nivel de paquetes del tráfico de red, y comunica las discrepancias o alertas a través de McAfee CWS. Esto ofrece visibilidad en un solo panel para entornos multinube con fines de corrección.

Aplicación de directivas para grupos de seguridad de red

McAfee CWS permite a usuarios y administradores crear directivas para grupos de seguridad de referencia y auditar las directivas que se ejecutan en las cargas de trabajo en función de estas referencias.

Principales ventajas (continuación)

- Consiga una protección multicapa frente al malware avanzado y las intrusiones.
- Descubra y supervise los contenedores Docker, y protéjalos con microsegmentación.
- Proteja su entorno aplicando las medidas correctivas directamente desde la solución.



Cloud Workload Security

Control total y plena **visibilidad**

Cualquier desviación o cambio frente a la referencia puede generar una alerta en la consola de McAfee CWS con fines de corrección. Los administradores también pueden configurar manualmente grupos de seguridad de red nativos desde McAfee CWS, lo que permite controlar directamente directivas para grupos de seguridad nativos de la nube.

Lo que diferencia a McAfee Cloud Workload Security: características y tecnologías principales

Compatibilidad de compilación nativa para la nube

Gracias a McAfee CWS, los clientes pueden consolidar la administración de varias nubes públicas y privadas en una única consola de administración, incluido AWS EC2, máquinas virtuales de Microsoft Azure, OpenStack y VMware Vcenter. McAfee CWS puede importar y permitir a los usuarios que trabajen en la nube con la nueva compatibilidad de compilación nativa para la nube para Amazon Elastic Container Service for Kubernetes (Amazon EKS) y Azure Kubernetes Service (AKS).

Administración sencilla y centralizada

Una sola consola ofrece directivas de seguridad coherentes y administración centralizada en entornos multinube con distintos servidores, servidores virtuales y cargas de trabajo en la nube. Los administradores también pueden crear varios permisos basados en funciones en el software McAfee® ePolicy Orchestrator® (McAfee ePO™), lo que les permite definir funciones de usuario de manera más específica y apropiada.

Visualización de la red con microsegmentación

Las funciones de visualización de la red específicas para la nube, las alertas de riesgos con prioridades y la microsegmentación ofrecen detección y control, con el fin de prevenir la progresión lateral de los ataques dentro de los entornos virtualizados y desde fuentes externas maliciosas. El apagado con un clic o la función de cuarentena ayudan a reducir las posibilidades de errores de configuración e incrementa la eficacia de la reparación.

Excelente seguridad para la virtualización

La suite McAfee CWS protege frente al malware sus máquinas virtuales de la nube privada mediante McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus). Y lo hace sin consumir recursos básicos y sin costes de explotación adicionales. McAfee MOVE AntiVirus permite a las organizaciones descargar las tareas de seguridad a máquinas virtuales dedicadas para una análisis optimizado de su entorno virtual.

Los usuarios consiguen protección antimalware a través de McAfee® Endpoint Security for Servers. Esta solución puede programar de manera inteligente las tareas que consumen muchos recursos, como los análisis bajo demanda, para evitar el impacto en los procesos empresariales críticos.

Etiquete y automatice la seguridad de las cargas de trabajo

Asigne las directivas adecuadas a todas las cargas de trabajo automáticamente con la capacidad de importar información de etiquetas de AWS y Microsoft Azure en el software McAfee ePO y asigne directivas en función de esas etiquetas. Las etiquetas de AWS y Microsoft Azure existentes se sincronizan con las etiquetas del software McAfee ePO para que puedan gestionarse automáticamente.

Corrección automática

El usuario define las directivas del software McAfee ePO. Si McAfee CWS encuentra un sistema que no está protegido por las directivas de seguridad del software McAfee ePO, y se detecta que contiene malware o virus, el sistema se pone automáticamente en cuarentena.

Protección frente amenazas adaptable

McAfee CWS integra medidas de protección globales, como el aprendizaje automático, la contención de aplicaciones, el antimalware optimizado para máquinas virtuales, la supervisión de la integridad de los archivos y la microsegmentación, con el fin de proteger sus cargas de trabajo frente a amenazas como el ransomware y los ataques selectivos. McAfee® Advanced Threat Protection bloquea los ataques sofisticados que no se habían detectado anteriormente, antes de aplicar técnicas de aprendizaje automático para aislar las cargas útiles maliciosas en función de los atributos de su código y su comportamiento.

Control de aplicaciones

La lista blanca de aplicaciones previene todos los ataques, tanto los conocidos como los desconocidos, ya que solo permite la ejecución de las aplicaciones de confianza y bloquea las cargas útiles que no han sido autorizadas. McAfee® Application Control ofrece protección dinámica basada en inteligencia sobre amenazas local y global, así como la posibilidad de mantener los sistemas actualizados sin desactivar las funciones de seguridad.

Supervisión de la integridad de los archivos

La función de supervisión de la intergridad de los archivos de McAfee lleva a cabo una supervisión continua con el fin de garantizar que los archivos y directorios de sus sistemas no hayan sufrido un ataque de malware, hackers o personal interno malintencionado. Los completos detalles de auditoría ofrecen información sobre cómo cambian los archivos en las cargas de trabajo del servidor y le avisan si se detecta la presencia de un ataque activo.

Cobertura de seguridad adecuada para su entorno multinube

McAfee CWS le garantiza el máximo de seguridad mientras aprovecha las ventajas de la nube. Cubre varias tecnologías de protección, simplifica la administración de la seguridad y evita que las ciberamenazas afecten a su empresa, para que pueda centrarse en su crecimiento. A continuación se incluye una comparativa de las funciones que ofrecen las distintas opciones disponibles.

FICHA TÉCNICA

Funciones	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
Administración centralizada (plataforma McAfee ePO)	✓	✓	✓
Compatibilidad con varias nubes (AWS, Microsoft Azure, VMware)	✓	✓	✓
Uso de microsegmentación para poner en cuarentena cargas de trabajo y contenedores	✓	✓	✓
McAfee MOVE (multiplataforma y sin agente)	✓	✓	✓
Prevención de amenazas para el sistema operativo del servidor de McAfee Endpoint Security (Windows y Linux)	✓	✓	✓
Firewall basado en host	✓	✓	✓
Administración de firewall nativo para AWS y Microsoft Azure (grupos de seguridad)	✓	✓	✓
Prevención de exploits e intrusiones en host	✓	✓	✓
Importación de información de etiquetas de AWS y Microsoft Azure en el software McAfee ePO.	✓	✓	✓
Corrección automática de cargas de trabajo no conformes	✓	✓	✓
Protección frente amenazas adaptable y aprendizaje automático		✓	✓
Virtualización y microsegmentación del tráfico de red		✓	✓
Análisis del tráfico de red nativo de la nube combinado con la calificación de reputación obtenida de McAfee GTI		✓	✓
Integración de McAfee® Virtual Network Security Platform (McAfee® vNSP)		✓	✓
Listas blancas dinámicas para servidores a través de McAfee Application Control			✓
Registro de auditoría continuo a través de la función de supervisión de la integridad de los archivos			✓
Protección de archivos y carpetas a través de McAfee® Change Control for Servers			✓

Más información

Para obtener más información, visite: **www.mcafee.com/es/products/cloud-workload-security.aspx**.

Las funciones y ventajas que ofrecen las tecnologías de McAfee dependen de la configuración del sistema y es posible que necesiten la activación de hardware, software o servicios. Encontrará más información en www.mcafee.com/es. Ningún sistema informático puede ser totalmente seguro.

McAfee Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es