McAfee Cloud Workload Security

Proteja sus cargas de trabajo en la nube privada y pública. 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, que incluyen contenedores, que están en un flujo constante. 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 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 inigualable que permite, con una sola directiva automatizada, garantizar la seguridad de todas sus cargas de trabajo en su tránsito por los entornos de nube híbrida, pública y privada, con el fin de facilitar la excelencia operativa a sus equipos de ciberseguridad.

Visibilidad en tiempo real

Descubrimiento automático

La existencia de instancias de cargas de trabajo y contenedores Docker no descubiertos genera brechas en la seguridad y ofrece a los ciberdelincuentes un hueco para infiltrarse en su empresa. McAfee Cloud Workload Security descubre los contenedores Docker y las instancias de cargas de trabajo elásticas en entornos Amazon Web Services (AWS), Microsoft Azure y VMware, y controla 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.
- Descubra y supervise los contenedores Docker, y protéjalos con microsegmentación.
- La defensa frente a amenazas optimizada para máquinas virtuales ofrece medidas de corrección multicapa.
- La administración centralizada y los flujos de datos automatizados reducen drásticamente la complejidad de los entornos híbridos y multinube.
- 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

Seguridad moderna para las cargas de trabajo

Protección frente a amenazas avanzadas

McAfee Cloud Workload Security 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. La protección frente a amenazas avanzadas, que incluye aprendizaje automático, 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.

Consolidación de eventos

McAfee Cloud Workload Security 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 también tecnologías de terceros, como AWS GuardDuty. 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 Cloud Workload Security 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 Cloud Workload Security. Los eventos de conexión de red de GuardDuty se representan en un gráfico de flujo cuando el tráfico corresponde al descubierto por McAfee Cloud Workload Security.

Excelente seguridad para la virtualización

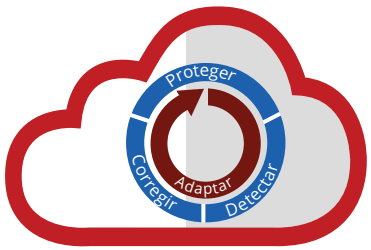
McAfee Cloud Workload Security protege frente al malware sus máquinas virtuales de la nube privada sin consumir recursos básicos y sin costos de explotación adicionales. Disfrute de una protección contra el malware que programa de manera inteligente las tareas que consumen muchos recursos, como los análisis bajo demanda, de manera que se realicen en momentos en los que el hipervisor no esté sobrecargado.

Virtualización 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 ayuda a reducir las posibilidades de errores de configuración e incrementa la eficacia de la reparación.

Principales ventajas (continuación)

- Disfrute de una sencilla protección multicapa frente a las intrusiones y el malware avanzados.
- Visualice y descubra las amenazas para la red sin necesidad de instalar un agente.
- Proteja su entorno aplicando las medidas correctivas directamente desde la solución.



Cloud Workload Security

Visibilidad y **control integrales**

Supervisión de la integridad de los archivos (FIM)

Esta función 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.

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. Esta función 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.

Administración simplificada

Coherencia gracias a la administración 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.

Despliegue automatizado

Con la ayuda de las herramientas de automatización del despliegue que ofrecen empresas como Chef, Puppet y Ansible, puede desplegar tecnología de seguridad automáticamente en varios entornos de la nube.

Mejor cobertura de seguridad

McAfee Cloud Workload Security 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	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Administración centralizada (McAfee® ePO™ Platform)	✓	✓	✓
Compatibilidad con varias nubes (AWS, Azure, VMware)	✓	✓	✓
Uso de microsegmentación para poner en cuarentena cargas de trabajo y contenedores	✓	✓	✓
Prevención de amenazas para el sistema operativo del servidor (Windows y Linux)	✓	✓	✓
Prevención de exploits e intrusiones en host	✓	✓	✓
Administración de cifrado para la nube	✓	✓	✓
Administración de firewall nativo para AWS y Azure (grupos de seguridad)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (sin agente y multiplataforma)	✓	✓	✓
Firewall basado en host	✓	✓	✓
Protección frente amenazas adaptable y aprendizaje automático		✓	✓
Visualización del tráfico de red y microsegmentación		✓	✓
Análisis del tráfico de red nativo de la nube combinado con la calificación de reputación obtenida de Global Threat Intelligence		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
Interacción con McAfee® Virtual Network Security Platform		✓	✓

Más información

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