McAfee Public Cloud Server Security Suite

Seguridad integral para cargas de trabajo en la nube de AWS y Azure

Ventajas principales

- Diseñado para cargas de trabajo de AWS y Azure
- Descubrimiento instantáneo
- Evaluación de la seguridad y corrección de amenazas
- Seguridad escalable
- Protección integral
- Uso de la consola de administración McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Opciones de despliegue con Chef, Puppet y OpsWorks
- Cumplimiento de las normativas
- Integración con otras soluciones de Intel Security

Las empresas, que están cambiando su estrategia de centros de datos para incluir (y a menudo con un uso preferente) instancias del servidor en la nube, son conscientes de que disponer de la protección adecuada pasa principalmente por considerar el modelo de seguridad compartida. Los proveedores de la nube pública, como Amazon Web Services (AWS) y Microsoft Azure, protegen el perímetro de la red y los usuarios deben proteger el contenido. ¿Pero cómo pueden las empresas más previsoras proteger sus cargas de trabajo en la nube contra las amenazas avanzadas persistentes y las de tipo zero-day, manteniendo el control de los costos con su estrategia de la nube? Estos son algunos de los retos a los que se enfrentan las empresas durante la adopción de la nube:

- Cada vez es más difícil hacer frente a las nuevas amenazas avanzadas y de tipo zero-day.
- Contar con visibilidad y con una administración centralizada se complica enormemente cuando se emplean varias infraestructuras en la nube.
- Preocupa el impacto que tiene en el rendimiento la seguridad de cargas de trabajo en la nube.

McAfee® Public Cloud Server Security Suite ofrece descubrimiento y control inmediatos de las cargas de trabajo de AWS y Azure, y las amenazas que sufren, para disfrutar de una protección completa, continua y coherente con un mínimo impacto en el rendimiento. Puede descubrir varios centros de datos o cuentas en la nube, máquinas virtuales y amenazas emergentes.

La seguridad global que proporciona McAfee Public Cloud Server Security Suite incluye de serie antivirus y prevención de intrusiones, junto a listas blancas avanzadas para proteger frente a amenazas de tipo zero-day, control de cambios para cumplir los requisitos de las normativas y administración de cifrado para proteger los datos. Una sola consola de administración facilita la gestión de varias nubes y la implementación de directivas. Las opciones de despliegue flexibles con las herramientas Chef, Puppet y OpsWorks DevOps ofrecen una experiencia perfecta con un mínimo de impacto.

intel Security

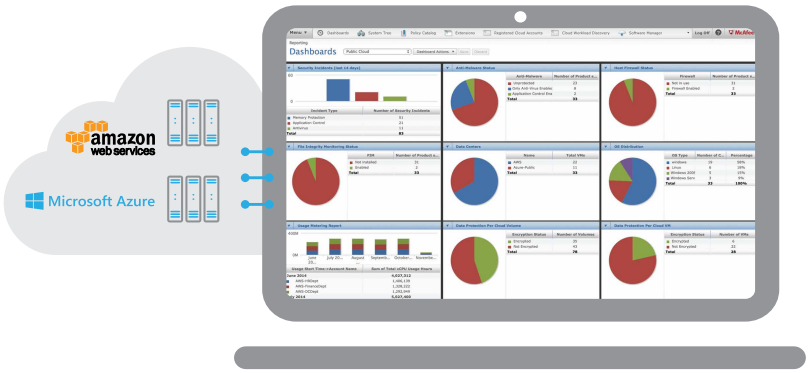

Figura 1. Una sola consola de administración para varias infraestructuras en la nube y distintas tecnologías de Intel Security.

Plataformas admitidas

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

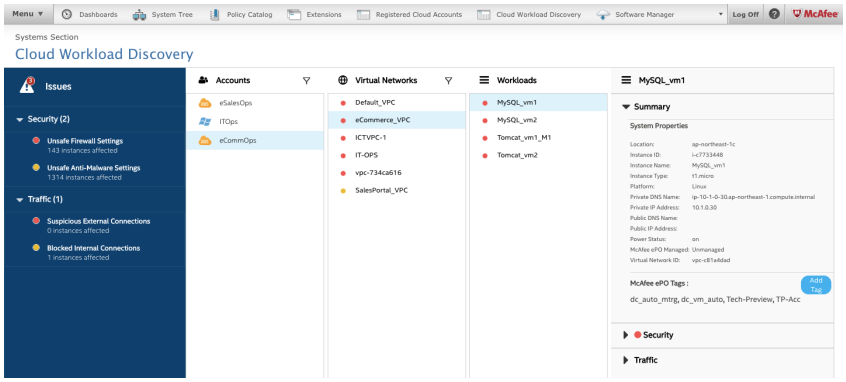

Figura 2. Descubrimiento y supervisión de varias infraestructuras en la nube y amenazas emergentes

Más información

Visite la página del producto: **www.mcafee.com/mx/products/public-cloud-server-security-suite.aspx**.

También disponible en **AWS Marketplace**.

Descubra las infraestructuras en la nube y las amenazas

Para mejorar el control de la infraestructura en la nube y descubrir las posibles amenazas, necesita contar con más visibilidad de ellas.

- Descubra todas las redes virtuales o nubes privadas virtuales (VPC), plantillas y cargas de trabajo de las infraestructuras de AWS y Azure en cuestión de minutos. Los primeros pasos para proteger de manera adecuada su infraestructura en la nube son: contar con información detallada de las cuentas de infraestructuras en la nube, saber qué usuarios tienen acceso a qué partes de la infraestructura de la nube, entender cómo se asignan las cargas de trabajo a las plantillas y VPC, y disponer de una instantánea rápida del árbol de sistemas asociado a la infraestructura de la nube.
- Consiga visibilidad de la seguridad de varias nubes desde una sola ubicación. Utilice información integral sobre amenazas, incluidas las fuentes de los ataques, para mejorar el control de la seguridad.
- Vea el tráfico entre cargas de trabajo y gestione el flujo de la información entre ellas, así como el acceso desde el exterior de la organización.

Supervise la nube y tome medidas más rápidas en caso de recibir alertas de seguridad

Cada vez es más importante poder realizar la reparación rápidamente, y esta solución permite evaluar los problemas de seguridad a un nivel más profundo y emprender acciones de manera inmediata.

- Identifique los problemas que requieren atención inmediata y tome las medidas adecuadas, utilizando códigos de color para las amenazas.
- Cree etiquetas personalizadas y asígnelas a las cargas de trabajo en función de sus objetivos concretos.
- Tome medidas para poner freno a los problemas de seguridad y adopte directivas o defina la reputación de las amenazas para defender la infraestructura frente a futuros incidentes de seguridad.
- Gestione el firewall para la nube con directivas personalizadas para cargas de trabajo individuales o grupos de cargas de trabajo. Administre las directivas para grupos de seguridad de AWS con el fin de controlar el tráfico para una o varias instancias.
- Identifique el tráfico sospechoso en nubes privadas virtuales (VPC) y tome medidas para impedir que la información crítica acabe en manos de los ciberdelincuentes.

Protección total frente a amenazas

McAfee Public Cloud Server Security Suite emplea un solo agente que proporciona varios niveles de seguridad que pueden gestionarse mediante una única consola de administración en varias plataformas en la nube. Esta solución se puede desplegar también con herramientas compatibles con DevOps, para ofrecer la mejor experiencia posible.

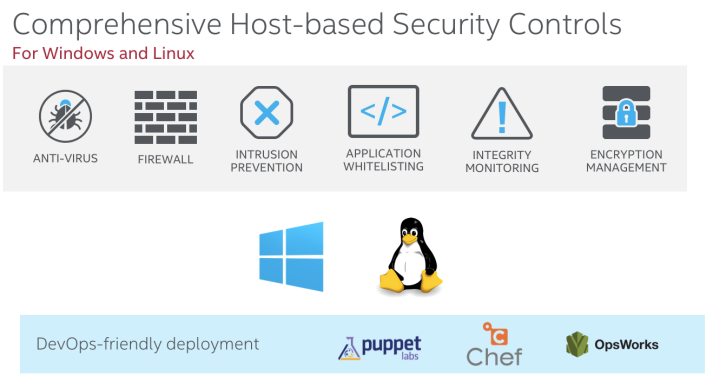

Figura 3. Seguridad integral para las cargas de trabajo de la nube pública.

Función	Ventajas
Opciones de despliegue con Chef, Puppet y AWS OpsWorks	• Las herramientas de despliegue de DevOps permiten planificar la seguridad y facilitan el despliegue. • La seguridad puede diseñarse como parte de las operaciones.
Descubrimiento de la carga de trabajo en la nube	• La visibilidad inmediata de las infraestructuras de la nube facilita el descubrimiento de los centros de datos virtuales, así como de las cargas de trabajo y los firewalls de la nube. • Alertas rápidas de amenazas con evaluación automática del estado de la seguridad. • Corrección más rápida de las amenazas con alertas por prioridad según la gravedad de las amenazas, y medidas para actuar inmediatamente frente a dichas alertas.
Una sola consola de administración para varias soluciones de seguridad de infraestructuras en la nube (software McAfee ePO)	• Extremadamente útil para la configuración de entornos híbridos. • Posibilidad de administrar en un panel cargas de trabajo físicas, virtuales y en la nube, y directivas. • Integra la nube de Intel Security y los partners con las tecnologías de seguridad in situ. • Tiene un costo total de propiedad inferior gracias a la integración de los procesos de seguridad y a las rápidas medidas de reparación.
Antimalware	• Máxima protección frente a malware. Protege sus sistemas y archivos frente a virus, spyware, gusanos, troyanos y otros riesgos para la seguridad. Detecta y limpia el malware, y permite a los usuarios configurar fácilmente las directivas para gestionar los elementos en cuarentena.
Firewall de host	• Protege las cargas de trabajo frente al acceso no autorizado y los ataques.
Prevención de intrusiones en host	• Bloquea proactivamente el tráfico de red malicioso o no deseado y los ataques, tanto conocidos como nuevos, mediante una tecnología patentada y galardonada. • Evita los cambios no deseados en las cargas de trabajo, mediante la restricción del acceso a determinados puertos, archivos, recursos compartidos, y claves y valores de registro. • La protección de memoria impide que amenazas o programas anómalos provoquen un desbordamiento del búfer y sobrescriban la memoria adyacente mientras se escriben datos en un búfer. Estos desbordamientos del búfer pueden dar lugar a la ejecución de código arbitrario en el equipo.
Listas blancas de aplicaciones	• Protegen contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas. • Mejoran la seguridad y reducen el costo de propiedad con listas blancas dinámicas que aceptan de manera automática el software nuevo que se ha agregado a través de los canales de confianza. • Reducen los ciclos de aplicación de parches gracias a listas blancas seguras de aplicaciones y a la protección avanzada de la memoria.
Supervisión de la integridad de los archivos	• Proporciona detección continua de los cambios a nivel de sistemas en las ubicaciones distribuidas y remotas. • Evita los cambios no autorizados en los archivos del sistema, los directorios y las configuraciones de importancia crítica. • Detecta y valida cada intento de cambio efectuado en tiempo real en la carga de trabajo e implementa la directiva de cambios por intervalo de tiempo, por origen o por ficha de trabajo aprobada.
Administración del cifrado	• Cifra los datos almacenados en volúmenes EBS de AWS con AWS Advanced Encryption Standard (AES). • Los volúmenes con datos preexistentes se pueden cifrar fácilmente. • Se integra con Key Management Service (KMS) de Amazon para el cifrado.

1. **http://www.mcafee.com/mx/resources/white-papers/wp-cloud-security-primer-techtarget.pdf**

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

62526ds_pcss_0716