

# McAfee Web Gateway Cloud Service

## Seguridad web nativa de la nube para una protección omnipresente

La protección frente a las amenazas sofisticadas procedentes de la Web precisa de tecnología avanzada, pero no tiene por qué disparar los costos y aumentar la complejidad. La seguridad web desde la nube permite a los equipos de seguridad obtener las mismas ventajas que ofrecen los dispositivos in situ en cuanto a protección avanzada contra amenazas, pero sin el costo de hardware y los recursos necesarios para su mantenimiento. El acceso a la Web desde fuera del perímetro de la red es cada vez mayor, lo que convierte a la nube en el punto habitual de contacto para dispositivos y usuarios en sus desplazamientos. En lugar de diseñar la seguridad para el tráfico que circula hacia una única ubicación, es más eficiente diseñarla a partir del endpoint. La unificación del control de acceso y la protección frente a amenazas para la nube y la Web permite a su plantilla trabajar con una productividad máxima, mientras crea una experiencia de administración de la seguridad eficiente y coherente.

### Protección universal y asequible

La administración de dispositivos de seguridad web in situ es costosa y agrega más carga de trabajo a los equipos de seguridad, a menudo ya al límite de su capacidad. El despliegue de seguridad web como servicio en la nube reduce el costo total de propiedad. Ya no existe la necesidad de comprar, poseer y mantener dispositivos de hardware. Todos los recursos que antes se empleaban para mantener dispositivos, en tareas como ampliaciones y aplicación de parches de software, pueden ahora reasignarse a iniciativas más estratégicas dentro del equipo de TI o de la organización de seguridad de TI.

En un despliegue híbrido, pueden utilizarse al mismo tiempo tanto dispositivos como el servicio en la nube. La mayoría de las empresas optan por este modelo para mantener la propiedad y el control de los dispositivos en red, y amplían la protección desde la nube a las pequeñas oficinas remotas o a los usuarios itinerantes.

Los equipos de TI que centralizan el tráfico web de las oficinas remotas a través de la infraestructura de conmutación de etiquetas multiprotocolo (MPLS), para que lo filtre un dispositivo gateway web en la red, se benefician inmediatamente de la seguridad web

### Principales ventajas

- La forma más asequible de desplegar seguridad web, sin necesidad de hardware ni software in situ.
- Mucho más que protección básica; la emulación de comportamientos bloquea el malware de tipo zero-day en milisegundos a medida que se procesa el tráfico.
- Ampliación de la protección a los usuarios fuera de la red. El modelo en la nube elimina el perímetro de red tradicional.
- Unificación con la consola McAfee® MVISION Cloud (CASB) para una administración de seguridad eficiente y coherente.

### Síguenos



## FICHA TÉCNICA

a través de la nube. La centralización del tráfico es cara y agrega complejidad a la red. En lugar de eso, las oficinas remotas pueden enrutarse directamente a la nube para recibir protección, lo que reduce los circuitos MPLS y simplifica la arquitectura de red.

Por último, el acceso de los empleados a la Web ya no se limita al perímetro de la red, lo que deja a los usuarios que se encuentran fuera de ella desprotegidos o invisibles para el equipo de TI. Trasladar la seguridad web a la nube invierte este perímetro. El tráfico web de usuarios y dispositivos fuera de la red puede enrutarse automáticamente del endpoint a la nube, lo que permite mantener una conexión segura cuando los usuarios trabajan desde casa, en un aeropuerto, una cafetería o cualquier otra ubicación fuera de la red. La red ya no se circunscribe al tráfico dentro de los muros físicos, sino que se extiende fuera de ellos desde dondequiera que se desplace el endpoint.

### Arquitectura global y de alto desempeño

McAfee® Web Gateway Cloud Service está concebido para los entornos empresariales, y muchas organizaciones conseguirán un mayor nivel de desempeño que el que actualmente obtienen con un modelo in situ. Por ejemplo, in situ, cuando se necesita aumentar la capacidad, el equipo de TI se ve obligado a adquirir y desplegar un nuevo dispositivo, algo que puede llevar de días a semanas. En nuestra nube, los aumentos de la capacidad demoran aproximadamente 15 minutos gracias al diseño de nube elástica integrado en nuestro servicio.

Si un dispositivo in situ falla y necesita repararse, puede bloquear el acceso a Internet y afectar a la seguridad general si está configurado para permanecer abierto al tráfico de la Web en caso de fallo. En caso de que se produzca un problema en uno de nuestros centros de datos, nuestro servicio en la nube redirigirá automáticamente todo el tráfico web al centro de datos más cercano y más rápido, garantizando de inmediato la continuidad.

La arquitectura de nuestro servicio en la nube está diseñada además para “emparejarse” con la red troncal de los puntos de intercambio de tráfico de Internet (IXP) más grandes del mundo. Esto elimina los saltos de enrutamiento de proveedores de servicios de Internet (ISP) intermediarios, que agregan latencia a la conexión. Con menos saltos a los proveedores de contenido más populares, como Microsoft Office 365 y Google, los usuarios consiguen conexiones más rápidas a través de nuestro servicio en la nube que las que obtendrían si se conectaran directamente al Internet abierto.

McAfee Web Gateway Cloud Service es un servicio global. El contenido web se proporciona en el idioma local, por lo que independientemente de dónde se conecte el usuario, obtendrá, por ejemplo, resultados de búsquedas de Google en su idioma. Para ver las ubicaciones y el estado actual de los centros de datos en los que se procesa el tráfico web, visite <https://trust.mcafee.com>.

### Principales ventajas (continuación)

---

- Arquitectura probada: McAfee Web Gateway Cloud Service está diseñado como versión multiinquilino de McAfee Web Gateway, el dispositivo in situ de confianza que utilizan empresas de todo el mundo.

## FICHA TÉCNICA

### Protección frente a las amenazas sofisticadas

Los equipos de seguridad son a menudo incapaces de hacer frente a malware y ataques selectivos muy sofisticados que eluden las defensas tradicionales, lo que provoca una pérdida de recursos y actuaciones “reactivas” permanentes para poder corregir los problemas en los endpoints. A diferencia del filtrado URL y los enfoques basados en firmas tradicionales para hacer frente a las amenazas web, el servicio McAfee Web Gateway Cloud Service protege los endpoints de malware de tipo zero-day y sin archivos a través de la emulación en línea de los archivos, de código JavaScript y HTML. Esto permite prevenir el malware de tipo zero-day antes de que llegue a alcanzar a un usuario y mejora las tasas de bloqueo aproximadamente un 20 % frente al filtrado URL y a las soluciones basadas en firmas. Las operaciones de seguridad tienen un costo menor y mayor flexibilidad de recursos gracias a que se reduce el número total de incidentes de malware. Si aún queda algo sospechoso, puede enviarse a McAfee Cloud Threat Detection, nuestra solución de análisis de amenazas avanzadas basada en la web, disponible como complemento, que se integra de forma nativa con McAfee Web Gateway Cloud Service.

Las amenazas web se distribuyen con frecuencia a través de tráfico cifrado para ocultarse de las defensas de seguridad web. Prácticamente todas las aplicaciones en la nube, como las de almacenamiento o redes sociales, utilizan por defecto tráfico cifrado. El servicio McAfee Web Gateway Cloud Service puede descifrar e inspeccionar completamente el tráfico cifrado HTTPS, lo que permite la prevención del malware y la visibilidad de las aplicaciones en la nube dentro de los canales cifrados.

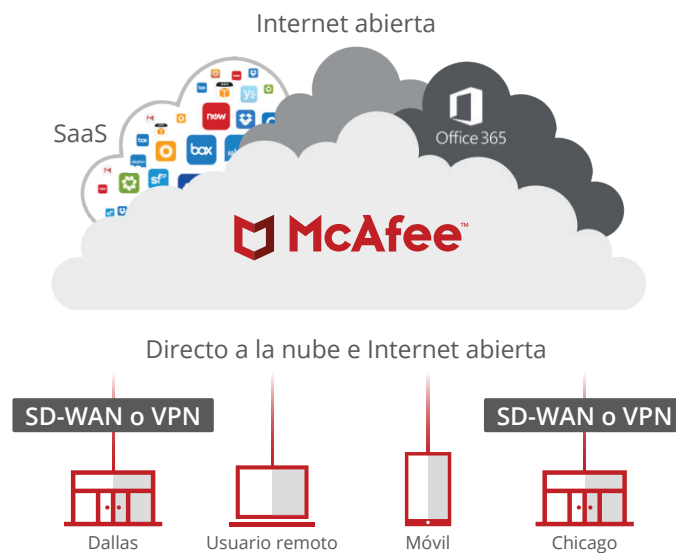


Figura 1. Arquitectura nativa de la nube para seguridad web y de nube.

## FICHA TÉCNICA

### Control de acceso y protección frente a amenazas unificados para la nube y la Web

Los servicios de la nube presentan varios niveles de riesgo y se puede acceder a ellos con dispositivos gestionados y personales. La unificación de McAfee Web Gateway Cloud Service y McAfee MVISION Cloud (CASB) permite controlar el acceso a todos los servicios de la nube y protege frente a las amenazas que se producen en ellos, desde una sola consola. Las directivas combinadas ofrecen un control de la nube sin precedentes;

con MVISION Cloud para la visibilidad y el control de los servicios de la nube autorizados, a través de la API y el proxy inverso, y McAfee Web Gateway Cloud Service para la supervisión y el bloqueo de los servicios de la nube y el tráfico web no autorizados, a través del proxy de reenvío. El servicio de la nube de alto riesgo se bloqueará, para evitar que los usuarios finales puedan acceder a estos servicios y mantenerlos a salvo frente a pérdidas de datos accidentales o malware.

### ¿Dónde está el servicio McAfee Web Gateway Cloud Service?

---

Visite <https://trust.mcafee.com> para estar al día de las novedades y conocer la ubicación de nuestros centros de datos, la disponibilidad, etc.

### Más información

---

Para obtener más información, visite [www.mcafee.com/mx/products/web-gateway-cloud-service.aspx](http://www.mcafee.com/mx/products/web-gateway-cloud-service.aspx)



Av. Paseo de la Reforma No.342 Piso 25  
Colonia Juárez, México DF  
C.P. 06600  
+52-55-50890250  
[www.mcafee.com/mx](http://www.mcafee.com/mx)

McAfee y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, LLC o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Copyright © 2020 McAfee, LLC. 4423\_0220 FEBRERO DE 2020