McAfee Web Gateway Cloud Service

Seguridad web a través de la nube para una protección omnipresente

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.
- Eficacia de administración inigualable con la plataforma McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud como consola de administración unificada para todos los servicios en la nube de Intel Security.
- 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.

La protección frente a las amenazas sofisticadas procedentes de la Web precisa de tecnología avanzada, pero no tiene por qué disparar los costes 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 coste 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 eficaz diseñarla a partir del endpoint. Al conectar los endpoints (e incluso ubicaciones enteras) a la nube se consigue una protección omnipresente, que nunca abandona el nuevo perímetro, desplazado ahora fuera de los muros de la red.

Protección omnipresente y asequible

La administración de dispositivos de seguridad web in situ es costosa y añade 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 coste 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 a través de la nube. La centralización del tráfico es cara y añade complejidad a la red. En lugar de eso, las oficinas remotas pueden enrutarse directamente a la nube para recibir protección, lo que elimina los circuitos MPLS y simplifica la arquitectura de red.

intel Security

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 se trabaja 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 rendimiento

McAfee Web Gateway Cloud Service está concebido para los entornos empresariales, y muchas organizaciones conseguirán un mayor nivel de rendimiento 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 tardan aproximadamente 15 minutos gracias al diseño de nube elástica integrado en nuestro servicio.

Si cuando un dispositivo falla y necesita repararse se sigue permitiendo su acceso a la Web, puede bloquear el acceso a Internet y afectar a la seguridad general. 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 más grandes del mundo. Esto elimina los saltos de enrutamiento de proveedores de servicios de Internet (ISP) intermediarios, que simplemente añaden latencia a la conexión. Con menos saltos a los proveedores de contenido más populares, como Microsoft Office 365 y Google, los usuarios consiguen a menudo conexiones más rápidas a través de nuestro servicio en la nube que las que obtendrían si se conectaran directamente al Internet abierto.

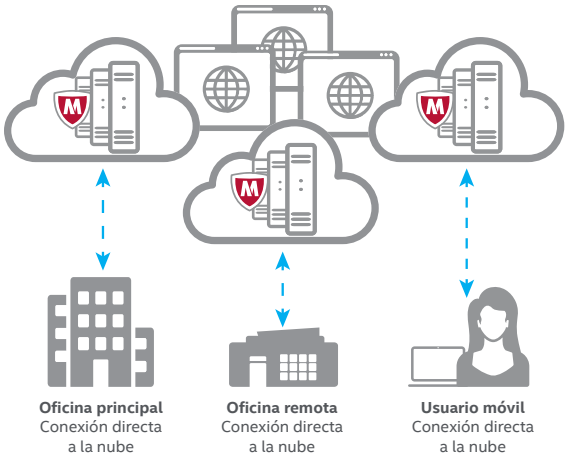

Figura 1. Despliegue de McAfee Web Gateway Cloud Service

McAfee Web Gateway Cloud Service es un servicio global. 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**. 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.

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 coste menor y mayor flexibilidad de recursos gracias a que se reduce el número total de incidentes de 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.

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.

Para la mayoría de los equipos de TI, resulta muy complicado controlar la proliferación de aplicaciones en la nube, en particular en el caso las "TI en la sombra" y los riegos que presentan los servicios elegidos por los usuarios. Gracias a una visibilidad total del tráfico web, incluido el tráfico HTTPS, los informes preconfigurados pueden mostrar los sitios web visitados, las aplicaciones en la nube que se utilizan y los correspondientes puntos de datos para evaluar el riesgo. Las TI en la sombra se descubren fácilmente comparando lo que realmente se utiliza con lo aprobado por el equipo de TI. Las aplicaciones en la nube, especialmente las de almacenamiento, también se utilizan cada vez más para distribuir mecanismos para el malware. La identificación de las aplicaciones que han distribuido malware puede ayudar a tomar decisiones informadas sobre directivas. Gracias un conocimiento total de los servicios en la nube a los que se accede, pueden implementarse más de 1600 controles de aplicaciones en la nube para minimizar el riesgo, como impedir cargas, el envío de mensajes o el bloqueo directo de aplicaciones.

Administración eficaz de la seguridad

La administración de la seguridad a través de varias consolas y directivas es muy laboriosa, en particular cuando la seguridad web in situ y basada en la nube se gestionan por separado. En un entorno híbrido, hay una sola consola tanto para los despliegues in situ como en la nube, un único conjunto de directivas y una interfaz de generación de informes.

Cuando se despliega de forma independiente sin hardware ni software in situ, el servicio McAfee Web Gateway Cloud Service se gestiona mediante la nube McAfee ePO Cloud, la consola de administración unificada para todos los servicios de seguridad basados en la nube de Intel Security, junto con protección para endpoints, lo que proporciona una eficacia sin precedentes en la administración de la seguridad.

El despliegue de seguridad web para endpoints es un reto, especialmente el enrutamiento y la autenticación. McAfee Client Proxy, un cliente de endpoints opcional, automatiza el enrutamiento y la autenticación a nuestro servicio en la nube, lo que garantiza una conexión generalizada a la nube con aplicación sistemática de directivas. McAfee Client Proxy funciona perfectamente en un despliegue híbrido con dispositivos in situ, y enruta de forma inteligente el tráfico al dispositivo mientras está en la red y al servicio en la nube cuando está fuera de ella. Hay disponibles opciones adicionales de enrutamiento y autenticación, que pueden elegirse en función de los requisitos de la organización.

Más información

Para obtener más información, visite **mcafee.com/es/products/web-protection.aspx**.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com