CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

Servicio de seguridad en el perímetro (SSE)

Planifica la consolidación de los servicios de seguridad e implementa a tu ritmo

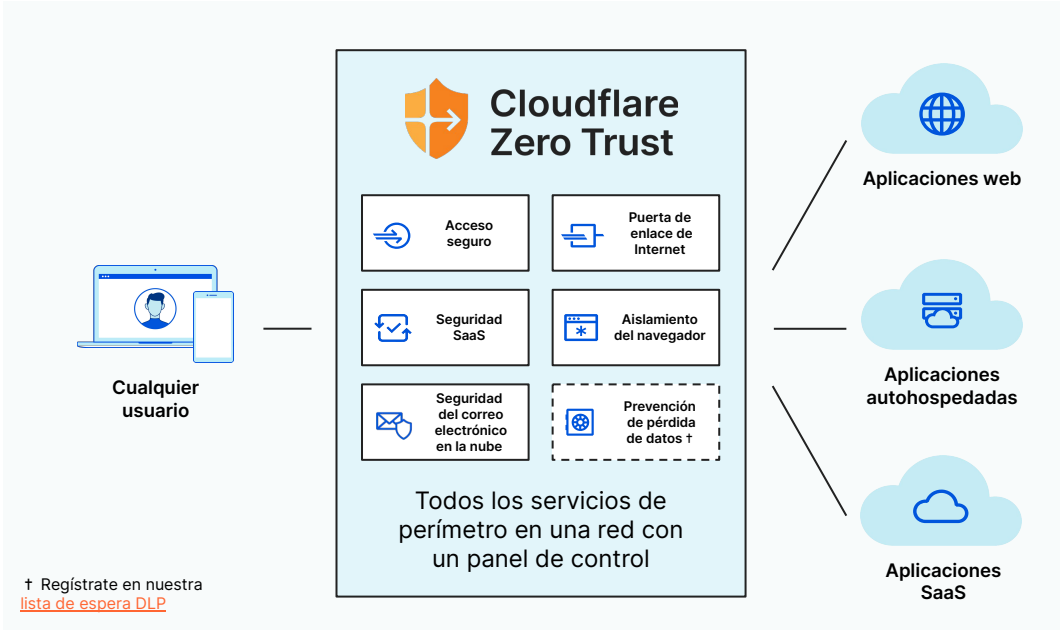
Convergencia en la nube

La complejidad de mantener varias soluciones específicas está obligando a la mayoría de las organizaciones a consolidar sus proveedores preferidos. Hoy en día, contar con las mejores capacidades y amplias plataformas no tiene por qué ser incompatible. Conforme la mayoría de los compradores de TI se inclinan por la consolidación, los proveedores de seguridad están aprovechando el momento para ampliar el valor de sus plataformas de seguridad más allá de lo que cada servicio puede lograr individualmente.

El enfoque SSE, que está a caballo entre los productos específicos y la consolidación integral, ahonda más en las capacidades de seguridad que la mayoría de las ofertas SASE (perímetro de servicio de acceso seguro), ya que no está vinculado a la infraestructura de red. En nuestra opinión, nuestra plataforma Zero Trust coincide con el conjunto de servicios SSE de Gartner y permite converger productos específicos que antes eran distintos: ZTNA, VPN, SWG, filtrado de DNS, CASB, RBI y firewall como servicio (FWaaS).

"Consolida los proveedores y reduce la complejidad y los costes conforme se renuevan los contratos de SWG, CASB y VPN (sustituyéndolos por un enfoque ZTNA). Aprovecha el mercado convergente que nace de la combinación de estos servicios".[1]

Gartner



† Regístrate en nuestra lista de espera DLP

Sustitución de la VPN
Simplifica y protege la conexión de cualquier usuario a cualquier recurso

Seguridad SaaS
Visibilidad y control de las aplicaciones, incluido el correo electrónico

Protección web
Protege tus datos de las amenazas a través de cualquier puerto y protocolo

Modernización de la seguridad
Mejora la productividad, simplifica las operaciones y reduce la superficie de ataque

SSE, un puente a SASE

Si bien la convergencia de los servicios de seguridad y perímetro de red es el objetivo final de SASE, algunas empresas quizás no busquen una consolidación integral con un único proveedor debido a su trayectoria o infraestructura actual. Independientemente de tu estrategia SASE a largo plazo, Cloudflare puede ayudarte a modernizar la seguridad, a transformar tu red corporativa o a ambas cosas.

Proveedor integral de SASE
Para las empresas que deseen unificar por completo los servicios de seguridad y perímetro de red en un solo proveedor, Cloudflare One, nuestra plataforma SASE, ofrece una red Zero Trust como servicio sobre nuestra red global de más de 275 ciudades.

Varios proveedores de SASE
Para aquellos con implementaciones SD-WAN maduras o equipos de seguridad y red fragmentados, Cloudflare Zero Trust puede ayudar a modernizar la seguridad y lograr una implementación SSE, aprovechando las asociaciones SD-WAN para SASE de varios proveedores.

SSE, implementación modular

La migración a SSE en la nube no debe ser un cambio repentino. Cloudflare Zero Trust ayuda a las organizaciones a eliminar el hardware al ritmo que deseen. Muchas empresas comenzarán su recorrido hacia Zero Trust añadiendo una solución ZTNA a su VPN conforme avanzan hacia la sustitución completa. La optimización de la seguridad de SaaS es la segunda prioridad para la mayoría, seguida de estrategias más amplias de protección de datos y amenazas.

Nuestra arquitectura uniforme y componible facilita la adopción modular de los servicios de seguridad. Las empresas pueden implementar combinaciones personalizadas de servicios que se adapten a sus casos de uso prioritarios. No se trata de la ley del "todo o nada".

"Realiza un inventario de equipos y contratos para implementar a lo largo de varios años una eliminación progresiva del perímetro local y del hardware de seguridad de las filiales en favor de un modelo SSE en la nube. Aborda la consolidación de los equipos locales, idealmente en un único dispositivo". [1]

Gartner

La integración favorece la innovación

Todos los servicios de Cloudflare se ejecutan en cada servidor en cada centro de datos en nuestra red global masiva, así que no hay deficiencias de cobertura o inconsistencias. Esta ventaja nos ayuda a ofrecer una inspección de paso único y a garantizar el máximo nivel de seguridad, rendimiento y fiabilidad.

Los servicios integrados de forma nativa también ofrecen más oportunidades creativas para combinar la funcionalidad de varios servicios y satisfacer los casos de uso deseados por nuestros clientes. Conforme estas líneas de productos se diluyen, la interacción entre servicios nos ayuda a resolver escenarios más avanzados y a modernizar verdaderamente la seguridad.

Refuerza la seguridad del acceso de terceros

- ZTNA (acceso a la red Zero Trust) y RBI (aislamiento remoto del navegador) se integran para proporcionar acceso seguro a terceros como proveedores y socios.
- Verifica la información contextual para validar el acceso y sirve aplicaciones en navegadores aislados para proteger los datos.
- El funcionamiento sin cliente de ambos servicios simplifica la implementación sin necesidad de descargas.

Visualiza y verifica las sesiones SSH

- ZTNA y SWG (puerta de enlace web segura) se integran para proporcionar visibilidad en todas las sesiones SSH para supervisar el acceso con privilegios.
- Simplifica el acceso a SSH con sesiones SSH sin cliente y basadas en el navegador a través de ZTNA.
- Proporciona visibilidad de la sesión SSH a nivel de red. Registra cada comando utilizando SWG como proxy.

Simplifica los flujos de trabajo de solución de SaaS

- SWG y CASB se integran para permitir un flujo de trabajo de "búsqueda y solución". Bloquea parte o toda la actividad sospechosa de SaaS directamente desde los resultados de seguridad de CASB.
- Amplía la visibilidad de SaaS para ayudar a detectar y solucionar los problemas que podrían dar lugar a fugas de datos o incumplimiento de la normativa.

Mejora la protección contra el phishing

- La seguridad del correo electrónico y el RBI se integran para combatir los sofisticados ataques de phishing y los ataques al correo electrónico corporativo.
- Ninguna información predictiva sobre amenazas es perfecta. Abrir enlaces de correo electrónico en un navegador aislado proporciona una capa adicional de protección.

Empieza tu recorrido hacia una red más rápida, fiable y segura

Probar ahora

¿Aún tienes dudas?
Más información sobre Cloudflare One

[1] Gartner Hype Cycle™ for Network Security, 2021