CLOUDFLARE

RESUMEN DE SOLUCIÓN

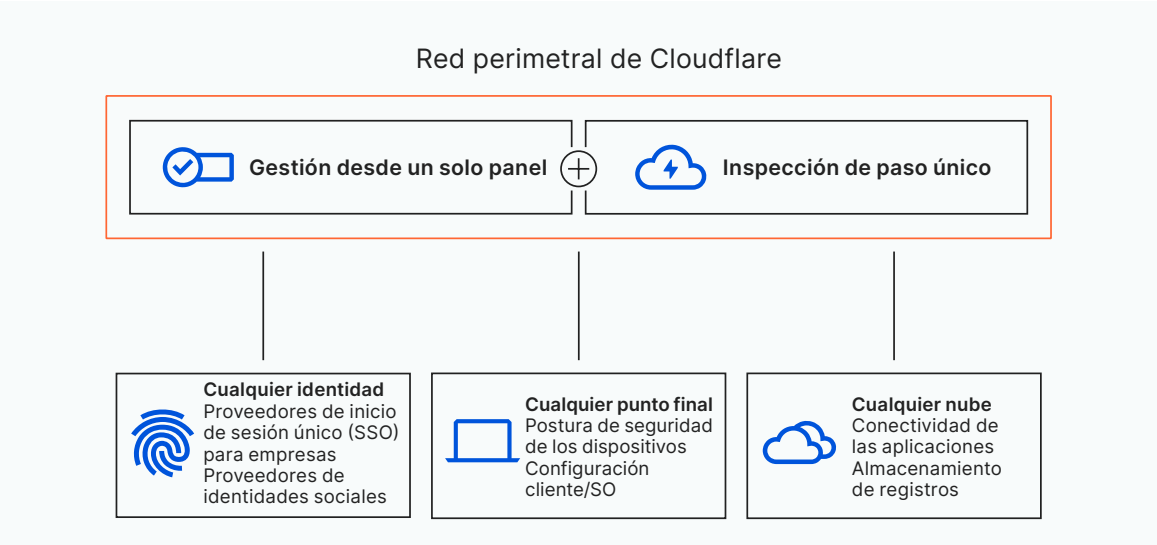
Integraciones de Cloudflare Zero Trust

Crea en los proveedores de identidad, de puntos finales y de nube que ya utilizas

Es inevitable compaginar distintos proveedores de identidad, de puntos finales y de nube en una organización, pero no tiene por qué ser un engorro. En Cloudflare, nuestro objetivo es proporcionar a tu organización la seguridad más eficiente de la forma más fácil. A diferencia de otros proveedores, no nos interesa con qué proveedores específicos de estas categorías trabajas, ahora o en el futuro.

Somos independientes de los proveedores. Por lo tanto, desde hace mucho tiempo, nuestra estrategia ha sido diseñar Cloudflare Zero Trust para integrar el mayor número posible de soluciones.

Mediante las integraciones, Cloudflare agrega señales en múltiples proveedores y sirve como un único panel de control para aplicar, en toda nuestra red global, políticas granulares según el contexto. Además, estas integraciones no requieren investigar densa documentación técnica.
Ya están integradas como flujos de trabajo para lograr una gestión con un solo panel más fluida.



Estos son los tres principios que seguimos para estar presentes allí donde estén los clientes:

- **Independiente de la identidad:** autentica a los usuarios en múltiples tipos de proveedores de identidad para un acceso fluido de todos los usuarios sin complicaciones de configuración.
- **Independiente de los puntos finales:** mejora las comprobaciones de la postura de seguridad de tu dispositivo gracias a una mayor granularidad y adaptabilidad, con señales tanto de tus proveedores favoritos de puntos finales como de nuestro cliente en el dispositivo.
- **Independiente de la nube:** protege las aplicaciones en cualquier nube pública o privada (local) para evitar dependencias de proveedor a largo plazo.

Agrega varias identidades a Cloudflare

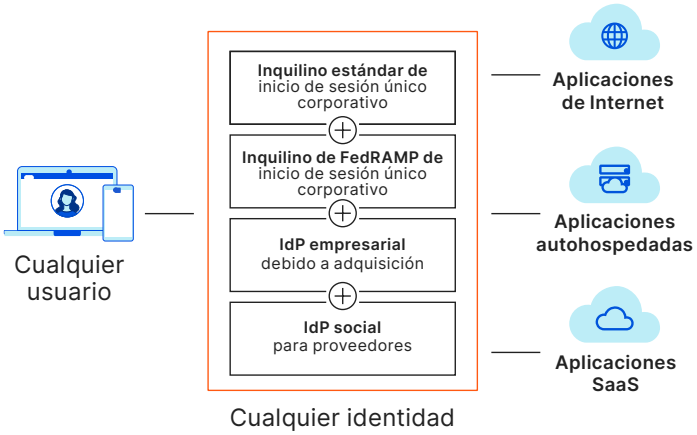
Inicio de sesión único múltiple

Cloudflare diseñó una de las primeras soluciones de acceso Zero Trust para admitir varios proveedores de identidad (IdP) al mismo tiempo. Hoy día, integramos IdP para empresas (como Okta o Azure AD), así como proveedores de identidades sociales (como LinkedIn o Github) y estándares de código abierto (como SAML u OIDC). Además, admitimos varias instancias del mismo IdP. Por ejemplo, el uso FedRAMP y no FedRamp de Okta.

Federa varias identidades a la vez

Nuestra capacidad de federar la identidad a través de muchos proveedores de identidad puede activar el proceso de creación de políticas con reconocimiento de identidad. Las organizaciones ya no necesitan crear integraciones personalizadas entre sus proveedores de identidad.

Es posible que, para las organizaciones en etapa de crecimiento con menos personal de seguridad de la información disponible, la federación sea una herramienta especialmente eficaz a la hora de escalar un enfoque Zero Trust, ya que evita las complicaciones de consolidar un único directorio centralizado.



Funciones clave

- Cloudflare integra múltiples IdP al mismo tiempo, de forma inmejorable
- Federa varios proveedores y varias instancias de cada proveedor.
- Incorpora más rápido los usuarios externos y socios resultado de fusiones y adquisiciones

Caso de uso:

Haz que los usuarios externos se sientan como ciudadanos de primera clase

El enfoque independiente de identidad de Cloudflare es especialmente útil al colaborar con usuarios externos a tu organización, por ejemplo, de proveedores, empresas adquiridas o socios. Es posible configurar, en cuestión de minutos, reglas de acceso de privilegio mínimo basadas en las identidades que ya aporten estos usuarios.

Esta sencilla flexibilidad evita la ineficiencia y los riesgos para la seguridad que suponen el suministro de licencias de inicio de sesión único, la implementación de VPN o la creación de permisos puntuales.

Los mejores socios de protección de puntos finales

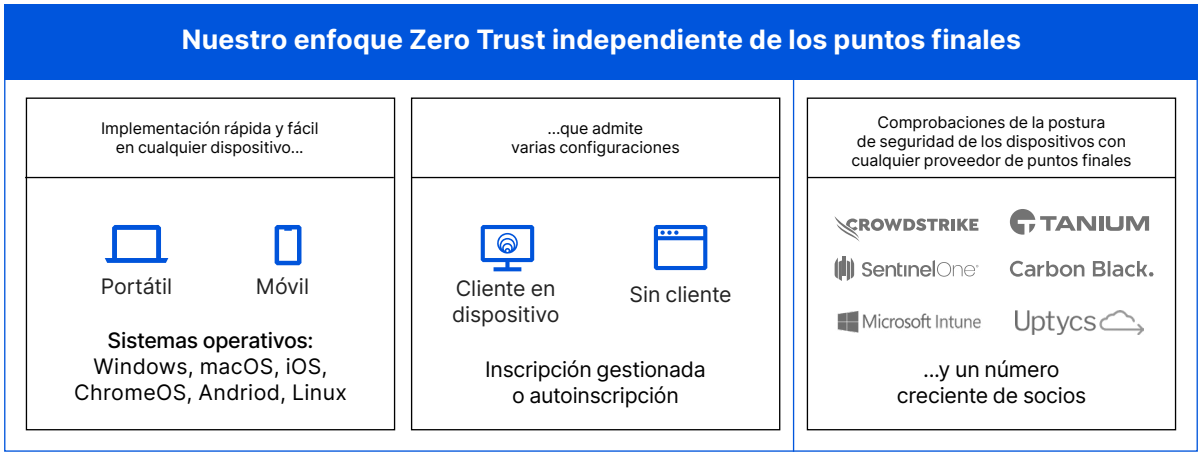
Asociaciones

Cloudflare cuenta entre sus socios con CrowdStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs y Microsoft Intune.

Los clientes pueden incorporar varios proveedores de protección de puntos finales al mismo tiempo y utilizar las señales de seguridad y las funciones de evaluación de riesgo de estas soluciones.

Configuración

Puedes configurar cualquiera de estos proveedores, con solo unos clics, en el panel de control de Cloudflare, con los flujos de trabajo integrados. Una vez configurados, Cloudflare puede comprobar que los dispositivos ejecutan tu software preferido de puntos finales. De esta forma, antes de permitir o denegar el acceso a una aplicación protegida, realiza una supervisión constante en busca de malware y otras amenazas.



Mejores integraciones mediante nuestro cliente en el dispositivo (WARP)

Para ampliar la seguridad, a menudo es necesario un cliente en el dispositivo, que puede mejorar las comprobaciones de la postura de seguridad del dispositivo con atributos adicionales. Hemos optimizado deliberadamente nuestro cliente para que su adopción sea flexible y sencilla.

Implementa en la mayoría de los sistemas operativos

- Nuestro cliente empresarial, WARP, funciona en un número cada vez mayor de los sistemas operativos más populares (p. ej., Windows, macOS, Linux, iOS, ChromeOS y Android).
- Nuestra moderna arquitectura WireGuard únicamente requiere pequeños ajustes de código específicos del sistema operativo.
- Nuestro cliente empresarial tiene una versión para el consumidor, que millones de usuarios utilizan a diario en todo el mundo. Al probar tantos usuarios individuales, WARP está mejor preparado que la mayoría de los clientes utilizados para Zero Trust.

Opciones de inscripción gestionada y autoinscripción

- Para los dispositivos administrados, documentamos las implementaciones con cualquier método basado en scripts en cualquier software popular de administración de dispositivos móviles.
- La autoinscripción de WARP puede ser útil para los usuarios externos, y se realiza en apenas unos minutos para cualquier equipo de escritorio o teléfono móvil.

Evita la dependencia de un proveedor de nube

Problema

A algunos proveedores, más monolíticos, les interesa especialmente que aumentes tu consumo de sus servicios de nube, específicamente, en las capas de almacenamiento y de proceso.

No es ninguna sorpresa que la integración de sus soluciones de seguridad complementarias no sea tan fluida como debería con otros proveedores de nube. Además, presentan también otros inconvenientes, como documentación menos detallada y errores. Esta dependencia de un conjunto de productos y servicios tecnológicos complica el trabajo de los equipos de seguridad de la información.

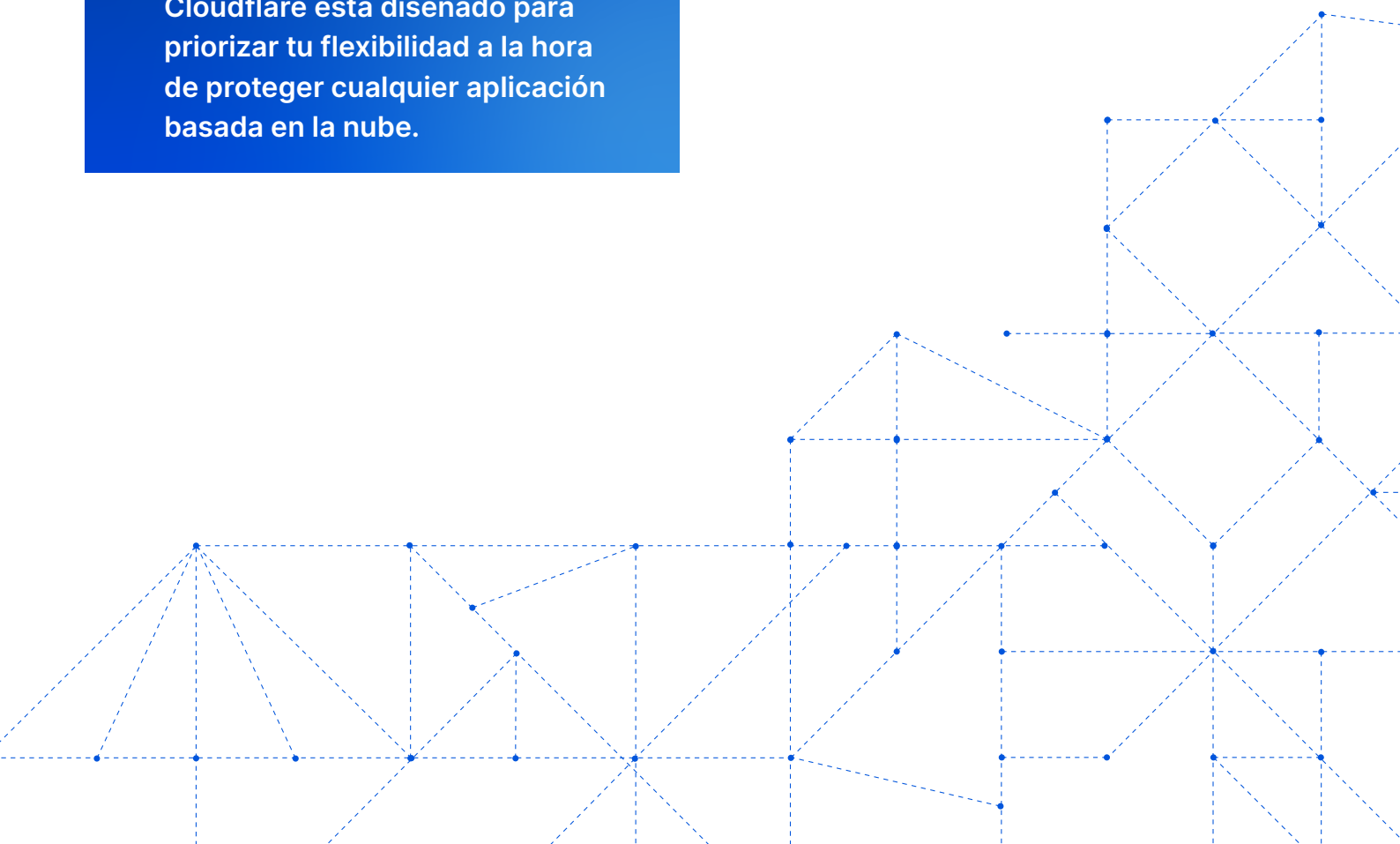
Solución

Por el contrario, nuestro foco estratégico es tu seguridad, no tu consumo de la nube. Cloudflare es independiente de la nube: protegemos el acceso a cualquier recurso en cualquier entorno de nube pública, privada o SaaS.

Cloudflare está diseñado para priorizar tu flexibilidad a la hora de proteger cualquier aplicación basada en la nube.

Funciones clave

- Acceso Zero Trust en los entornos de nubes públicas, privadas y SaaS
- Sin dependencia del proveedor para destinos de almacenamiento o proceso en la nube
- Conectores de aplicaciones, socios de acceso a la red e integraciones de almacenamiento que te facilitan la interacción con las aplicaciones en cualquier nube



Capacidad de Cloudflare

Amplía las conexiones a las aplicaciones en cualquier nube

Nuestro ligero conector de aplicaciones funciona en cualquier nube

- Ejecuta la herramienta de la línea de comandos en Linux y en otros sistemas operativos
- Integrado como un contenedor Docker
- Compatible con la réplica para entornos Kubernetes modernos
- Tunnel se puede configurar y supervisar mediante la interfaz de usuario

Amplias interconexiones con proveedores de nube

- Rápidas conexiones para los usuarios gracias a 11 000 interconexiones entre nuestra red y otros proveedores de nube, 50 de los cuales son interconexiones privadas con centros de datos de Microsoft, Amazon y Google

Diversos socios de acceso a la red que no son específicos de la nube

- Conecta fácilmente cualquier entorno de nube pública o privada a nuestra red mediante tu método de enrutamiento SD-WAN actual (p. ej., VMware) o realiza una interconexión privada en más de 1600 ubicaciones de proveedor de colo (p. ej., Equinix)

Envía datos de registro a cualquier nube

Los datos de registro se pueden almacenar en las nubes o bien enviar directamente a los proveedores de análisis

- Soporte integrado para uno o más destinos de almacenamiento al mismo tiempo, incluidos AWS, Azure, Google Cloud y cualquier API compatible con S3 (p. ej., Digital Ocean Spaces)
- Integraciones incluidas con herramientas de análisis y SIEM como Sumo Logic, Splunk y Datadog

Seguridad en cualquier nube pública o privada

Socios de integración Zero Trust

Con el tiempo, Cloudflare agregará señales para un mayor número de tus proveedores preferidos, con el respaldo de la información de nuestra plataforma Zero Trust y nuestra red global.

Proveedores de identidad

Proveedores de soluciones de inicio de sesión corporativos

- Centrify
- Citrix ADC
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- Ping Identity

Identidades sociales

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Código abierto

- OIDC
- SAML 2.0

Proveedores de puntos finales

Proveedores de protección de puntos finales

(para la postura de seguridad de los dispositivo)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

Proveedores de soluciones de gestión de puntos finales

(para una implementación de cliente)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

Socios de soluciones de acceso a la red

Socios de soluciones de interconexión física

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Socios de soluciones de interconexión de estructura de redes

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

Proveedores de nube

Destinos de almacenamiento en la nube

- AWS S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- Otros proveedores con una API compatible con S3

Socios de análisis en la nube y SIEM

- Azure Sentinel
- Datadog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

Para obtener más información sobre Cloudflare Zero Trust y solicitar una demostración o prueba de concepto a un representante de ventas, visita: https://www.cloudflare.com/es-es/products/zero-trust/.

CLOUDFLARE

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-3795.26SEP2022