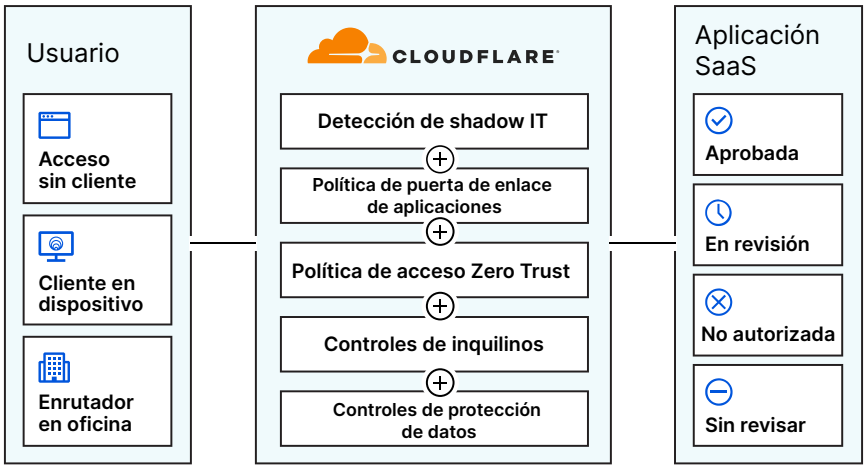
RESUMEN DE LA SOLUCIÓN

CLOUDFLARE

Visibilidad y control Zero Trust de las aplicaciones SaaS

Las aplicaciones SaaS ceden mayor control que antes a tus equipos de trabajo, pero la flexibilidad y la libertad que les ofrecen también plantean riesgos de seguridad, problemas de visibilidad y obstáculos de control de acceso para tu organización.

Cloudflare te ofrece las herramientas que necesitas para proteger tus datos y usuarios, al tiempo que les permite utilizar las herramientas que les facilitan el trabajo.



Detección y administración de Shadow IT

Sin visibilidad de las aplicaciones que utilizan tus usuarios, no puedes controlar cómo se almacenan, comparten o exponen los datos confidenciales a terceros. Cloudflare te ayuda a detectar, clasificar y controlar todas las aplicaciones autorizadas y no autorizadas dentro de tu organización, al tiempo que registra cada conexión y solicitud en una ubicación centralizada.

Adopción de una política de acceso Zero Trust

Las aplicaciones SaaS se alojan fuera de la red corporativa, lo que limita la capacidad de tus equipos de seguridad para controlar cómo los usuarios acceden a esas aplicaciones y trasladan los datos dentro y fuera de ellas. Cloudflare aplica medidas de seguridad Zero Trust por capas delante de tus aplicaciones SaaS, autenticando a los usuarios legítimos e impidiendo que los usuarios no autorizados o los dispositivos de riesgo accedan a tus archivos y datos.

Implementación de controles de protección de datos e inquilinos

Cuando los empleados acceden a la instancia incorrecta de las aplicaciones, pueden compartir y almacenar tus datos en lugares equivocados, lo que abre la puerta a posibles fugas de datos y otros riesgos de seguridad. Cloudflare te ayuda a controlar el uso compartido y el almacenamiento de tus datos, ya sea en tránsito por nuestra red o en uso dentro de nuestro navegador remoto. Ahora puedes crear e implementar políticas de navegación Zero Trust para proteger los datos que se alojan dentro de cualquier inquilino de SaaS, a la vez que evitas que tus empleados accedan a aplicaciones o inquilinos equivocados de aplicaciones autorizadas.

Detección y administración de Shadow IT

Evalúa las aplicaciones que utilizan tus usuarios

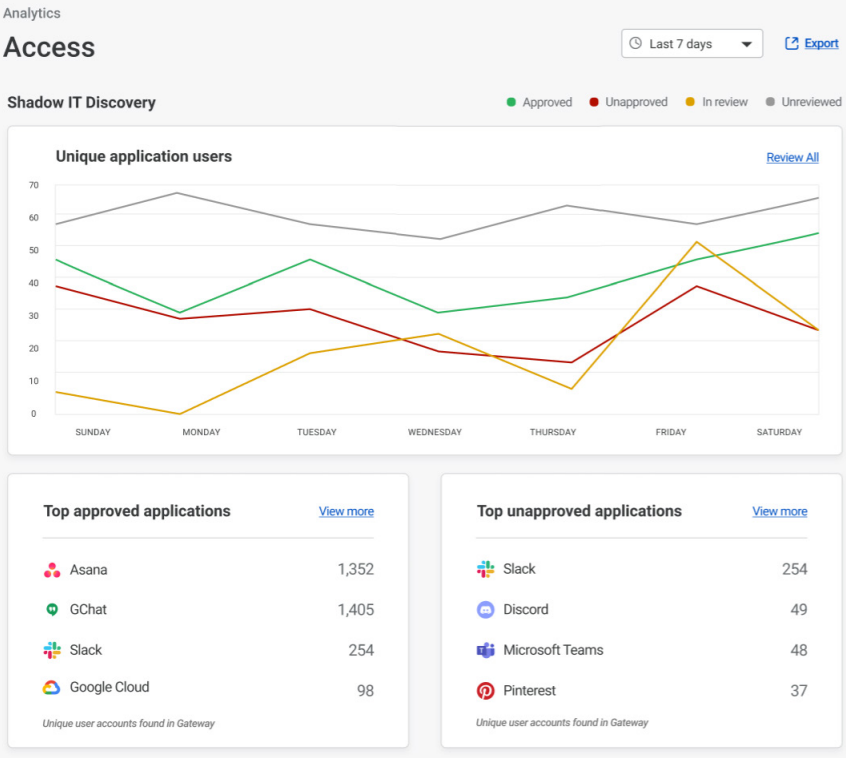
Cuando los informáticos no puede ver las aplicaciones que utilizan tus equipos de trabajo, pierden el control de lo que ocurre con los datos dentro de esas aplicaciones. Cloudflare añade y clasifica de forma automática todas las solicitudes HTTP en nuestro registro de actividad por tipo de aplicación. A partir de ahí, puedes establecer el estado y hacer un seguimiento del uso de las aplicaciones autorizadas y no autorizadas en tu organización.

Registra cada conexión y solicitud

Cloudflare ayuda a mitigar los riesgos que enfrenta tu organización cuando los usuarios acceden a aplicaciones no autorizadas o utilizan dispositivos no gestionados para acceder a información confidencial. Todas las conexiones y solicitudes se registran en una ubicación central, para que puedas ver qué aplicaciones se están utilizando y qué acciones están realizando los usuarios en ellas. Los administradores también tienen la capacidad de bloquear y permitir las solicitudes a las aplicaciones SaaS, evitando que los usuarios omitan importantes controles de seguridad y obtengan acceso no autorizado a aplicaciones, recursos y datos de tu organización.

Funciones principales

- Controla de forma automática las aplicaciones que ya cuentan con la protección de Cloudflare.
- Conserva los registros durante un máximo de 6 meses en la red de Cloudflare.
- Envía los registros a uno o más de tus servicios de almacenamiento de registros en la nube y SIEM.



Adopción de una política de acceso Zero Trust para tus aplicaciones SaaS

Ofrece acceso seguro a SaaS a través del proxy de identidad de Cloudflare

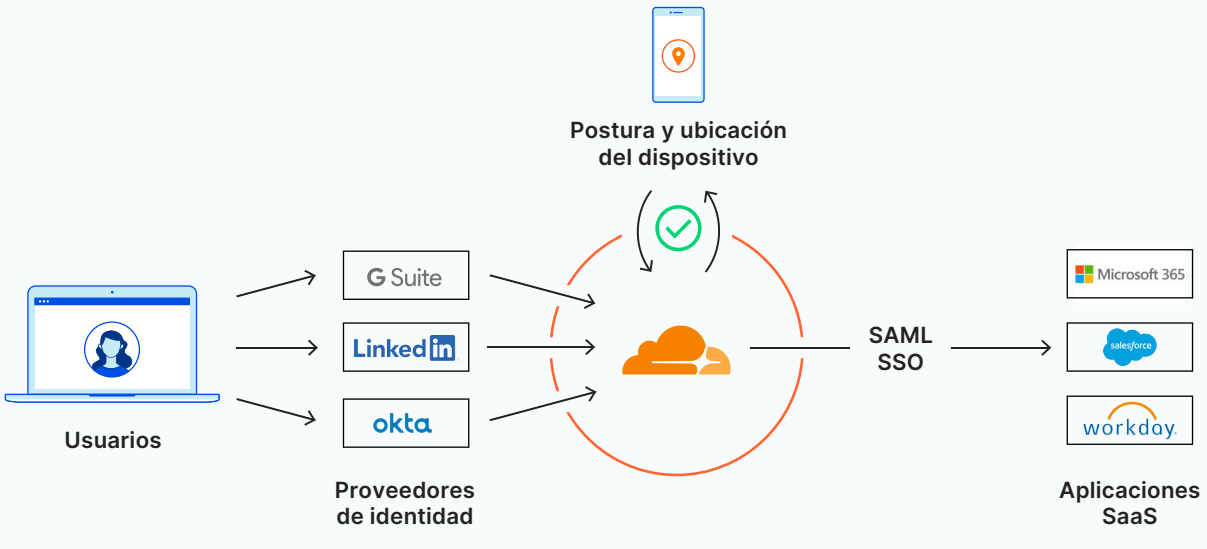
Las aplicaciones SaaS se encuentran alojadas en servidores de terceros y suelen estar gestionadas por unidades de negocio, lo que significa que tu departamento de informática a menudo tiene poco que decir sobre cómo los usuarios acceden a esas aplicaciones. Cloudflare se sitúa entre tu proveedor de identidad y tus aplicaciones SaaS, lo que te permite crear y aplicar reglas de Zero Trust basadas en el contexto y con reconocimiento de identidad para el proceso de inicio de sesión, todo ello sin interrumpir la experiencia del usuario final.

Define los permisos de las aplicaciones para los dispositivos de los usuarios

Tu equipo informático necesita un control detallado sobre el modo en que los dispositivos gestionados por la empresa inician sesión en las aplicaciones SaaS. Cloudflare incluye reglas de Zero Trust en el proceso de inicio de sesión único para todas las aplicaciones que admiten la autenticación SAML. Los usuarios se autentican primero con tu proveedor de identidad. A continuación, Cloudflare comprueba la solicitud con la postura y la ubicación del dispositivo antes de autorizar el acceso a cualquier aplicación SaaS, con una gestión de sesiones flexible para una verificación continua. Los administradores de seguridad también pueden crear políticas específicas para cada dispositivo, de modo que los usuarios solo puedan acceder a las aplicaciones a través de dispositivos que cumplan los requisitos de seguridad preestablecidos, incluidos los certificados mTLS.

Funciones principales

- Integra varios proveedores de identidad o varias instancias del mismo proveedor.
- Verifica la identidad del usuario con reglas por aplicación (p. ej. la autenticación multifactor requiere una clave segura).
- Verifica la postura del dispositivo con reglas por aplicación (p. ej. aplicación de políticas de puerta de enlace web segura, instalación de EPP, activación de un certificado mTLS o de cifrado de discos) y ubicación.
- El portal del iniciador de aplicaciones de Cloudflare permite a los usuarios ver y acceder a todas sus aplicaciones SaaS autorizadas.



Implementación de controles de protección de datos e inquilinos para cualquier aplicación SaaS

Restringe el acceso a las instancias no corporativas de las aplicaciones

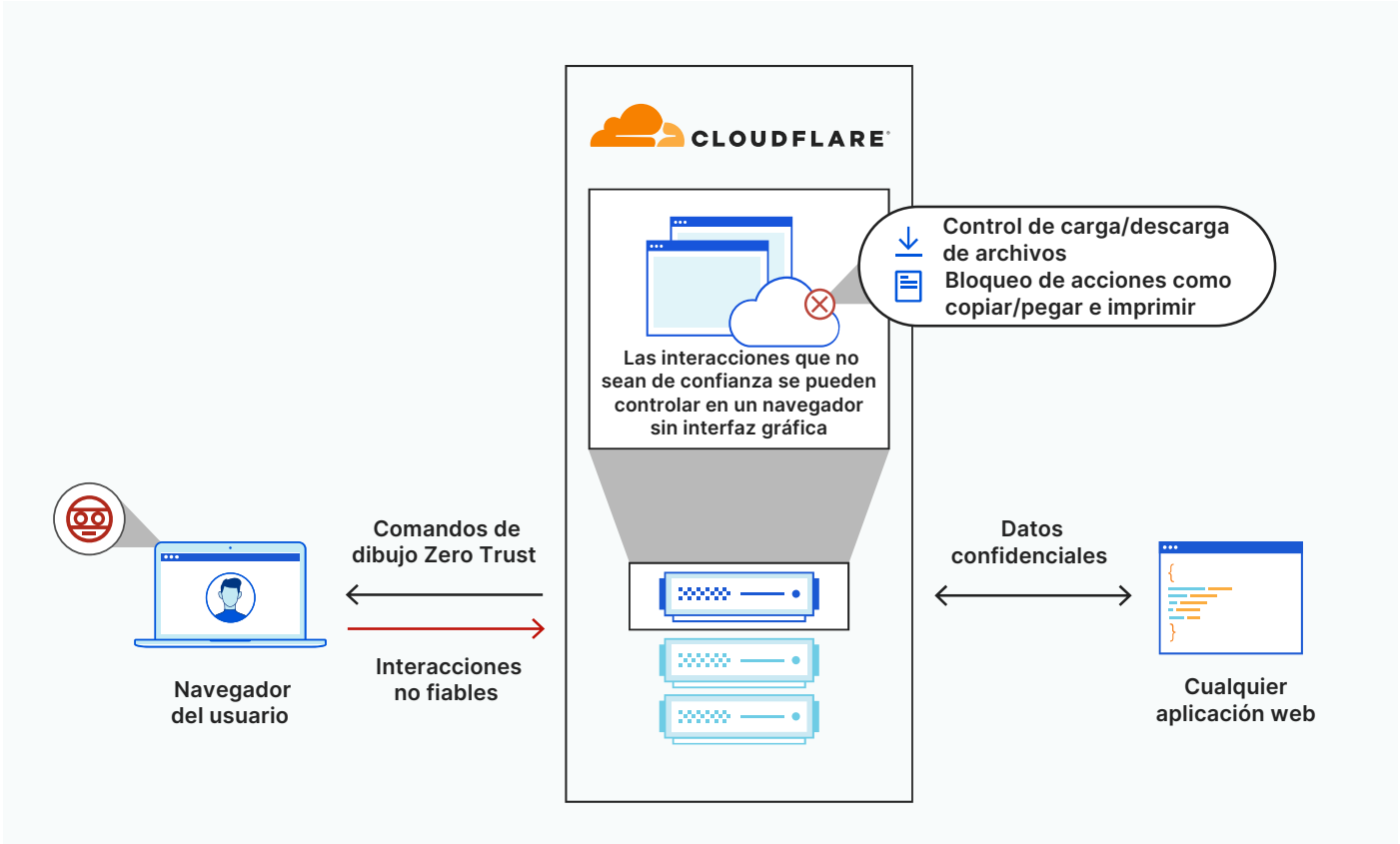
Cloudflare permite el control de inquilinos a través de políticas de puerta de enlace HTTP, que se pueden configurar para evitar que los usuarios accedan a las versiones para consumidores de aplicaciones. En lugar de aplicar estas políticas utilizando servidores proxy locales a través de VPN corporativas, Cloudflare filtra e inspecciona todo el tráfico y las solicitudes a través de una amplia red global de centros de datos, para que tus usuarios nunca experimenten un aumento de la latencia o el rendimiento se vea afectado.

Evita que los datos corporativos salgan de tus inquilinos

Cloudflare facilita la creación e implementación de políticas de navegación de Zero Trust para controlar y proteger los datos que se alojan dentro de tus aplicaciones web. Todo el código de la aplicación se ejecuta en un navegador seguro sin interfaz gráfica que funciona de forma remota a través de nuestra red global masiva, en lugar de los dispositivos de punto de conexión, por lo que los datos confidenciales están protegidos de los dispositivos vulnerables o que no son de confianza, así como de las amenazas de día cero. Además, los administradores mantienen el control sobre el modo en que los usuarios acceden a los datos y los comparten, por lo que se puede minimizar el riesgo de pérdida accidental de datos o de fugas más importantes.

Funciones principales

- Permite o bloquea los comportamientos del navegador en función de varios criterios, como la aplicación, el tipo de aplicación, el nombre del servidor, la identidad del usuario y el riesgo de seguridad.
- Controla las acciones del usuario dentro del navegador: funciones de descarga, carga, copia y pega, entrada del teclado e impresión.



La diferencia de Cloudflare

Alcance de nuestra plataforma

Cloudflare usa controles de acceso Zero Trust (ZTNA), puerta de enlace web segura (SWG) y aislamiento remoto del navegador (RBI) delante de tus aplicaciones SaaS, sin necesidad de que tu equipo informático configure y opere un producto CASB (agente de seguridad de acceso a la nube) dedicado.

Diseño de servicios desde cero

Las capacidades de CASB de Cloudflare se integran de forma eficaz con nuestros servicios de ZTNA, SWG y RBI, ya que todos se han diseñado desde cero, lo que elimina la necesidad de compaginar varios productos específicos para proteger tus aplicaciones y equipos.

Panel de control único

Cloudflare permite a las organizaciones establecer políticas y gestionar el acceso y el uso de las aplicaciones desde un único panel de control, para que puedas supervisar todas las solicitudes y los permisos a simple vista.

Cloudflare ayuda a los equipos de trabajo a supervisar, proteger y controlar las aplicaciones SaaS a través de un conjunto de capacidades de seguridad Zero Trust integradas de forma nativa.

Más información