CLOUDFLARE

RESUMEN DE PRODUCTO

Cloudflare Zero Trust

La plataforma de acceso a aplicaciones y navegación Zero Trust más rápida del mundo

Riesgos fuera del perímetro

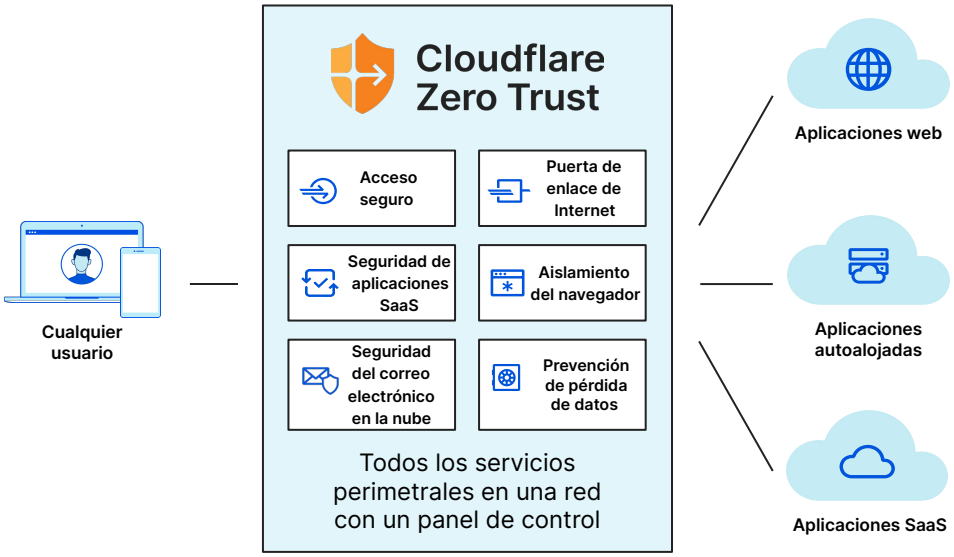
La exposición de las aplicaciones y los usuarios fuera del perímetro corporativo obligó a los equipos de seguridad a alcanzar un compromiso sobre cómo mantener la seguridad de los datos. Los métodos basados en la ubicación para proteger el tráfico (como las VPN, los firewalls y los proxies web) han sucumbido a la presión, limitando así la visibilidad de las organizaciones, complicando las configuraciones y exponiendo a las organizaciones a un riesgo excesivo.

Los riesgos están presentes en todas partes, y para adaptarse, las organizaciones están recurriendo a un modelo de seguridad Zero Trust en la nube.

Implementa una arquitectura Zero Trust nativa de Internet

Cloudflare Zero Trust es una plataforma de seguridad que aumenta la visibilidad, elimina la complejidad y reduce riesgos cuando los usuarios remotos y presenciales se conectan a aplicaciones y a Internet. Con una arquitectura de un solo paso, el tráfico se verifica, filtra, inspecciona y aísla de las amenazas.

Se ejecuta en una de las redes Anycast más rápidas del mundo que abarca más de 275 ciudades en más de 100 países para acelerar las implementaciones y el rendimiento frente a otros proveedores.



Acceso seguro
Simplifica y protege el acceso entre usuarios y aplicaciones, en cualquier dispositivo, en cualquier lugar.

Protección contra amenazas
Garantiza la protección de los usuarios y los datos frente a las amenazas web, del correo electrónico y multicanal.

Protección con Microsoft
Visibilidad y control de todas las suites SaaS de Microsoft, Google y más.

Trabajo híbrido seguro
Mejora la productividad de los equipos, reduce el riesgo cibernético y aumenta la eficiencia tecnológica.

Beneficios para empresas

Reduce el exceso de confianza

Protege las aplicaciones con reglas Zero Trust basadas en la identidad y el contexto. Bloquea el phishing, el ransomware y otras amenazas en línea. Aísla los puntos finales de los riesgos alejando de los dispositivos y los datos, el código y la actividad de los usuarios no fiables.

Elimina la complejidad

Reduce la dependencia de los productos específicos heredados y aplica controles de seguridad estándar a todo el tráfico, independientemente de cómo se inicie la conexión o en qué parte de la pila de la red se aloje.

Restablece la visibilidad

Registros exhaustivos de DNS, HTTP, SSH, red y actividad de Shadow IT. Supervisa la actividad de los usuarios en todas las aplicaciones. Envía los registros a varias de tus herramientas de almacenamiento y análisis en la nube preferidas.

Acceso seguro (ZTNA)

Una forma más rápida, fácil y segura de conectar a los usuarios con las aplicaciones

Desafío: acceso lento, complejo y peligroso

Los controles de acceso tradicionales basados en el perímetro (como las VPN) son cada vez un mayor inconveniente. El mal rendimiento perjudica la productividad del usuario final, los administradores tienen dificultades con las configuraciones complejas y es difícil frenar el movimiento lateral.

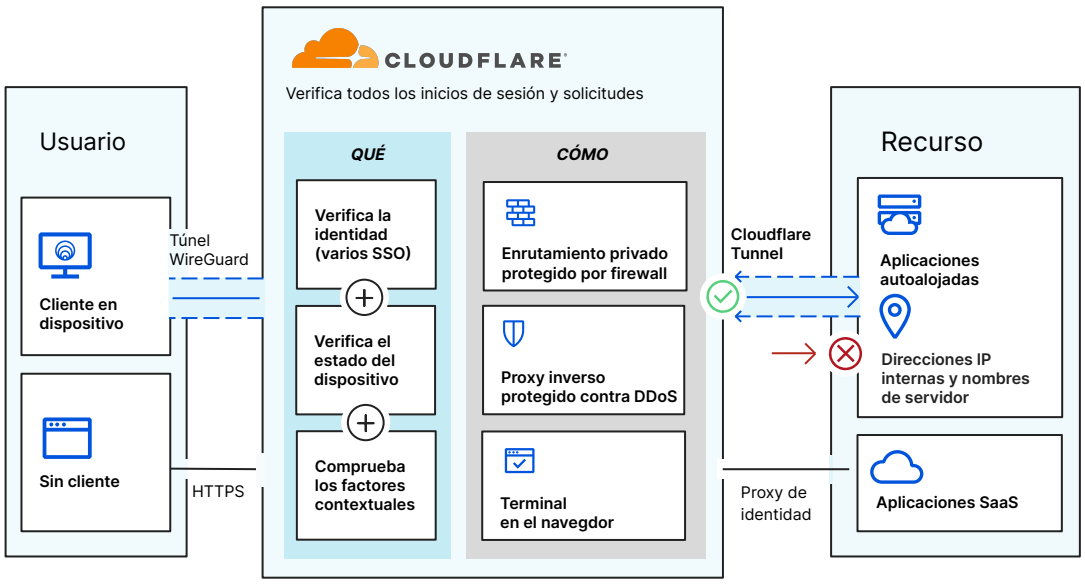
La implementación acelerada de la nube y el trabajo híbrido ha acentuado todavía más estas deficiencias e intensificado la vulnerabilidad de las VPN.

Acceso a la red Zero Trust (ZTNA)

Access, el servicio ZTNA de Cloudflare, mejora o sustituye los clientes VPN protegiendo cualquier aplicación, en cualquier entorno de red local, nube pública o SaaS.

ZTNA de Cloudflare trabaja con tus proveedores de identidad y plataformas de protección de puntos finales para aplicar reglas Zero Trust por defecto que limitan el acceso a las aplicaciones corporativas, los espacios IP privados y los nombres de servidor.

Cómo funciona



Implementación sin cliente para aplicaciones autoalojadas basadas en web, SSH o VNC accesibles a través de un navegador.

Implementación con el cliente en dispositivo de Cloudflare para conectarse a las direcciones IP internas, nombres de servidor y aplicaciones no web.

Casos de uso clave

Promover el teletrabajo e iniciativas de BYOD

Verifica el acceso de todos los usuarios, estén donde estén, en función de la identidad, el estado del dispositivo, el método de autenticación y otros factores contextuales.

Aplica estas políticas Zero Trust para el acceso de tus usuarios híbridos. Promueve iniciativas de "usa tu propio dispositivo" (BYOD) protegiendo dispositivos administrados y no administrados.

Agilizar el acceso de terceros con flexibilidad

Agiliza la configuración del acceso para contratistas, proveedores, agencias, colaboradores, etc.

Incorpora varios proveedores de identidad (IDP) a la vez. Configura reglas de mínimo privilegio basadas en los IDP que ya utilizas.

Evita la acumulación de licencias SSO, la implementación de VPN o la creación de permisos únicos.

Simplificar la configuración administrativa y el soporte

Añade nuevos usuarios, proveedores de identidad o reglas Zero Trust en cuestión de minutos.

Promueve la productividad reduciendo el tiempo de incorporación de los usuarios (eTeacher Group) y dejando atrás la configuración de acceso basada en IP (BlockFi). Sin necesidad de contratar equipos dedicados a la gestión de las VPN (ezCater).

Protección contra amenazas (SWG y RBI)

Filtra, inspecciona y aísla el tráfico de Internet

Desafío: El panorama de las amenazas en constante evolución

Aumentar la seguridad y mantener la productividad de los usuarios nunca ha sido tan difícil. El teletrabajo implica más dispositivos no administrados que almacenan más datos confidenciales a nivel local. Mientras tanto, el ransomware, el phishing, el Shadow IT y otras amenazas web han aumentado en volumen y sofisticación.

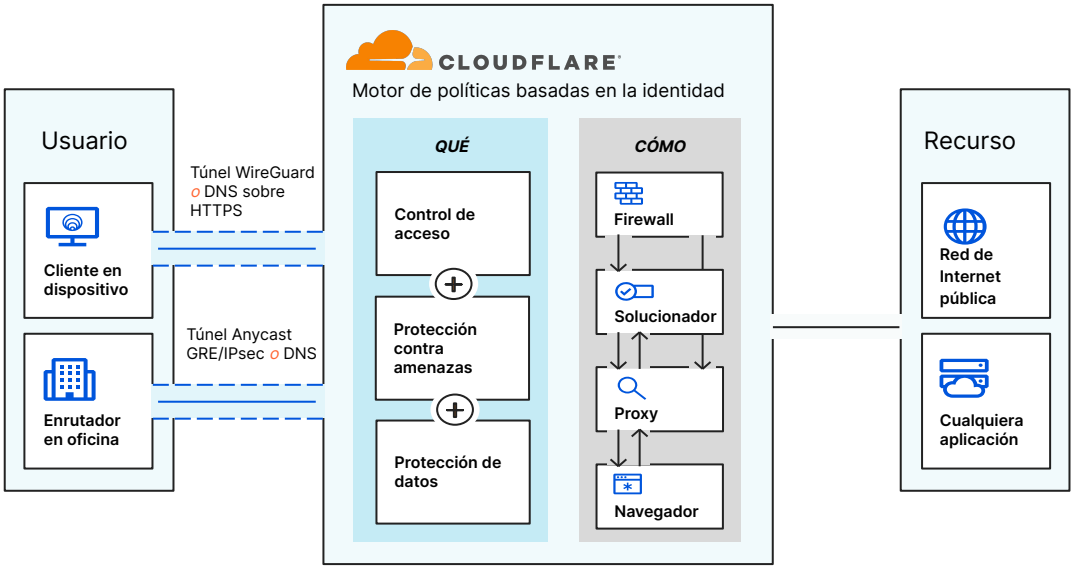
Confiar en soluciones específicas heredadas y en las copias de seguridad de los datos es una estrategia arriesgada para protegerse de las amenazas multicanal.

SWG con navegación Zero Trust

Cloudflare Gateway, nuestra puerta de enlace web segura, protege a los usuarios con un filtrado web basado en la identidad, además de un aislamiento remoto del navegador (RBI) integrado de forma nativa.

Empieza con el filtrado de DNS para conseguir una rentabilidad asequible y rápida para los usuarios que trabajan en remoto o presencialmente. A continuación, aplica un método de inspección HTTPS más exhaustivo y, por último, amplía los controles RBI para implementar Zero Trust para toda la actividad en Internet.

Cómo funciona



Sin redireccionamiento. Envía el tráfico de las capas 4 y 7 a través de Cloudflare en lugar de utilizar dispositivos heredados.

Se puede filtrar, inspeccionar y aislar tanto el tráfico de los recursos internos como de Internet.

Casos de uso clave

Evitar el ransomware

Bloquea los sitios y dominios de ransomware gracias a nuestra información de red global. Aísla la navegación en sitios peligrosos para reforzar la protección.

Combina el filtrado SWG y RBI con la denegación por defecto, ZTNA para mitigar el riesgo de propagación lateral de la infección de ransomware y la escalada de privilegios a través de tu red.

Bloquear el phishing

Filtra los dominios de phishing conocidos y "nuevos"/"recién vistos". Aísla la navegación para impedir que las cargas útiles peligrosas se ejecuten localmente. Evita el envío de información confidencial en sitios de phishing sospechosos mediante los controles de entrada de teclado del aislamiento remoto del navegador (RBI).

Además, próximamente, los administradores podrán activar el filtrado de correo electrónico con un solo clic, con la tecnología de Area 1.

Evitar la fuga de datos

Implementa la prevención de la pérdida de datos (DLP) con controles que impiden que los usuarios carguen archivos a los sitios.

Implementa la navegación Zero Trust para controlar y proteger los datos que se alojan dentro de las aplicaciones basadas en la web. Controla las acciones del usuario dentro del navegador, como las funciones de descarga, carga, copia y pega, entrada de teclado e impresión.

Protección con Microsoft (CASB)

Optimiza la seguridad de SaaS para obtener más visibilidad y control, con menos gastos generales

Desafío: Proliferación de aplicaciones SaaS

Los equipos de trabajo modernos dependen más que nunca de las aplicaciones SaaS, como Microsoft 365. Pero cada aplicación SaaS requiere diferentes consideraciones de seguridad, y opera fuera de las salvaguardas del perímetro tradicional.

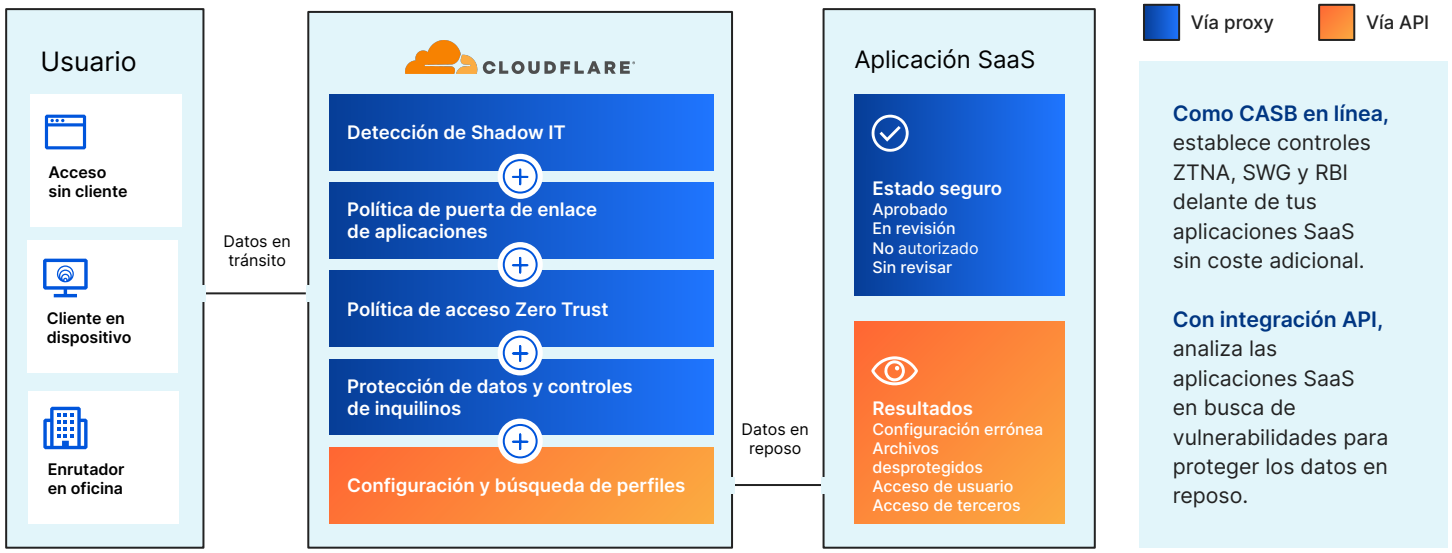
Conforme las organizaciones adoptan docenas de aplicaciones SaaS, resulta cada vez más difícil mantener la seguridad, la visibilidad y el rendimiento consistentes.

Agente de seguridad de acceso a la nube (CASB)

El servicio CASB de Cloudflare ofrece visibilidad y control completos de las aplicaciones SaaS, para que puedas evitar fácilmente las fugas de datos y el incumplimiento de la normativa.

Bloquea las amenazas internas, el intercambio de datos de riesgo y los infiltrados. Registra cada solicitud HTTP para revelar las aplicaciones SaaS no autorizadas. Analiza las aplicaciones SaaS para detectar configuraciones erróneas y actividades sospechosas.

Cómo funciona



Como CASB en línea, establece controles ZTNA, SWG y RBI delante de tus aplicaciones SaaS sin coste adicional.

Con integración API, analiza las aplicaciones SaaS en busca de vulnerabilidades para proteger los datos en reposo.

Casos de uso clave

Implementación de controles de protección de datos e inquilinos

Aplica el control de inquilinos a través de las políticas de puerta de enlace HTTP para evitar que los usuarios accedan y almacenen datos en las versiones incorrectas de las aplicaciones SaaS más populares, ya sea de forma involuntaria o maliciosa.

Controla las acciones de los usuarios (p. ej. copia/pega, descargas, impresión, etc.) dentro de las aplicaciones SaaS basadas en la web para minimizar el riesgo de pérdida de datos.

Mitigar y controlar elementos de Shadow IT

Minimiza los riesgos planteados por las aplicaciones SaaS no autorizadas.

Cloudflare añade y clasifica automáticamente todas las solicitudes HTTP en nuestro registro de actividad por tipo de aplicación. Los administradores pueden configurar el estado y hacer un seguimiento del uso de las aplicaciones autorizadas y no autorizadas en toda la organización.

Identificar nuevas amenazas y configuraciones erróneas

Conéctate a aplicaciones SaaS populares (Google Workspace, Microsoft 365, etc.) a través de la API y analiza los riesgos.

Otorga a tus equipos informáticos y de seguridad visibilidad sobre los permisos, configuraciones erróneas, accesos indebidos y problemas de control que podrían poner en peligro tus datos y a tus usuarios.

Protección contra el phishing (CES)

Amplía la seguridad Zero Trust al correo electrónico para conseguir una protección integral contra las amenazas

Desafío: El correo electrónico es el vector de amenaza n.º 1

El correo electrónico es la forma de comunicación n.º 1 entre usuarios, pero también la primera vía de entrada de los ciberdelincuentes. De hecho, un estudio reciente reveló que el 91 % de todos los ciberataques comienzan con un correo electrónico de phishing.

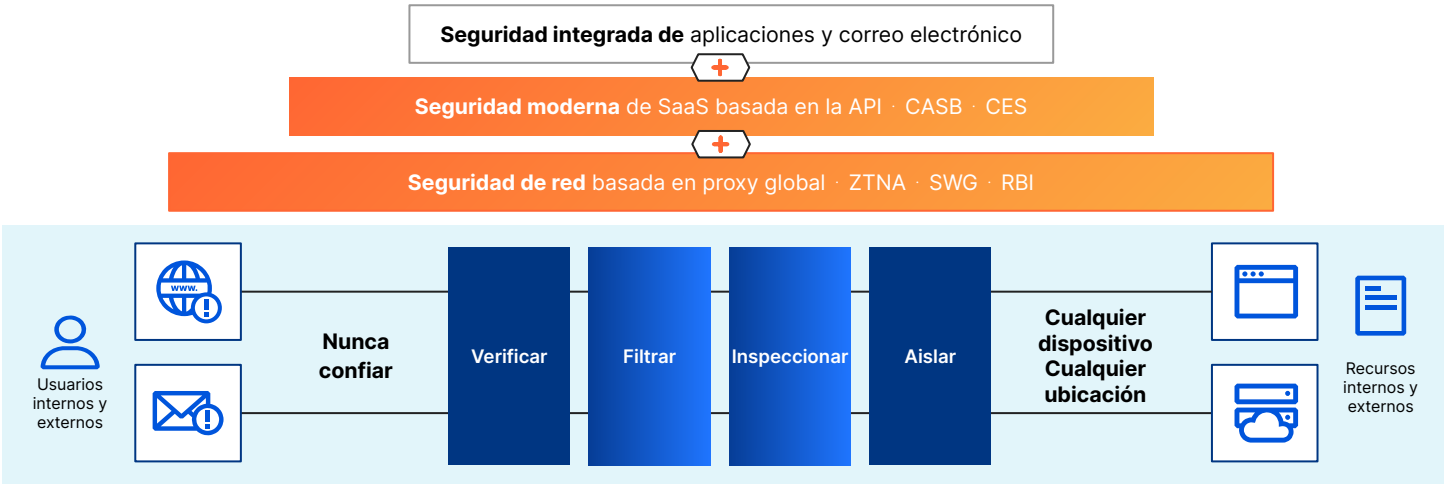
Los atacantes se dirigen con frecuencia y explotan con éxito el alto nivel de confianza que se suele otorgar a la comunicación por correo electrónico.

Integración de la seguridad del correo electrónico nativa en la nube

La incorporación de la seguridad del correo electrónico en la nube (CES) de Area 1 como parte de una estrategia integral Zero Trust elimina la confianza implícita en el correo electrónico para detener preventivamente los ataques de phishing y las amenazas del correo electrónico corporativo (BEC).

Todo el tráfico de los usuarios, incluido el correo electrónico, se verifica, se filtra, se inspecciona y se aísla de las amenazas conocidas y desconocidas. Area 1 ayuda a los clientes a bloquear las amenazas del correo electrónico, a adoptar una postura de seguridad proactiva y a reducir un 90 % el tiempo de respuesta a los incidentes de phishing.

Cómo funciona: Zero Trust para todo el tráfico del correo electrónico, web y red



Casos de uso clave

Evitar las amenazas al correo electrónico corporativo y el fraude por correo electrónico

Evita los sofisticados ataques al correo electrónico corporativo y la apropiación de cuentas de proveedores mediante el análisis de sentimientos, los gráficos sociales de los socios, la clasificación de los mensajes y el análisis del origen de las campañas.

Bloquea automáticamente, pon en cuarentena y escala las comunicaciones financieras fraudulentas.

Proteger contra los ataques multicanal

Bloquea fácilmente las campañas de ataque que se dirigen a los usuarios a través de varios canales de comunicación, como el correo electrónico y la web, permitiendo a los usuarios cargar de forma segura enlaces sospechosos o desconocidos en un navegador remoto y aislado.

Detecta los ataques de phishing diferido que incluyen enlaces peligrosos después del envío con la clasificación de enlaces en el momento de hacer clic.

Acelerar la evaluación del phishing y la respuesta

Permite los ciclos de investigación de seguridad, obtén información útil sobre tu entorno de correo electrónico y reduce los tiempos de respuesta con recursos dedicados que mejoran la capacidad de tu equipo actual para neutralizar rápidamente las amenazas de phishing.

Consigue soporte adicional y experiencia en seguridad con los servicios administrados de seguridad del correo electrónico.

Trabajo híbrido seguro: la diferencia de Cloudflare

Seguridad moderna para equipos modernos

Fácil implementación

Cloudflare ofrece una plataforma uniforme y modular para facilitar la configuración y las operaciones. Los conectores de software y las integraciones únicas permiten que nuestros accesos directos y servicios perimetrales funcionen en conjunto.

Esta ventaja mejora la experiencia para tu equipo de informática y usuarios finales.

Resistencia de red

Nuestra automatización del tráfico de un extremo a otro garantiza una conectividad de red fiable y escalable con una protección permanente desde cualquier lugar.

Con Cloudflare, cada servicio del perímetro se ha desarrollado para ejecutarse en cada ubicación de red, disponible para cada cliente, a diferencia de otros proveedores de soluciones de seguridad.

Velocidad de innovación

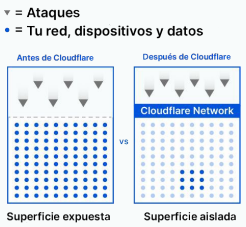
Nuestra arquitectura con garantía ante el futuro nos ayuda a desarrollar y entregar nuevas soluciones de seguridad y red a buen ritmo.

Tanto si se trata de nuestra rápida capacidad de implementación de nuevos estándares de Internet y seguridad como de la creación de casos de uso pensados para el cliente, nuestra trayectoria de proezas técnicas habla por sí sola, y nuestro fundamento brinda una mayor capacidad de elección.

5 formas para ahorrar tiempo y dinero a tu empresa con Zero Trust

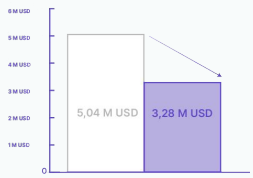
Disminuye la superficie de ataque en un

91 %↓



Rebaja los costes de fuga en un

35 %↓



Acelera la incorporación de usuarios en un

60 %↑

Reduce la carga de las incidencias informáticas en un

80 %↓

Reduce la latencia de los usuarios en un

39 %↓

Seguridad optimizada para proporcionar la máxima facilidad de uso

Una interfaz de gestión

Simplifica la configuración con un panel de control creado de forma nativa para las políticas de acceso a las aplicaciones e Internet.

Utiliza un panel de control que integre los proveedores de identidad, las protecciones de puntos finales y los accesos directos de red.

Una plataforma consolidada

Sustituye distintos clientes VPN, firewalls locales y otras soluciones de seguridad específicas por una plataforma y un plano de control.

Reduce los costes y la complejidad conforme migras la seguridad al perímetro.

Experiencia de usuario inigualable

Cloudflare se sitúa más cerca de tus usuarios y servicios y enruta las solicitudes con mayor rapidez utilizando un enrutamiento optimizado y basado en la información a través de nuestra amplia red Anycast, con más de 275 ubicaciones en más de 100 países de todo el mundo.

Acelera tu recorrido Zero Trust — Probar ahora — Te ayudamos