Acceso a la red Zero Trust

Cloudflare Zero Trust, en concreto Access, mejora la productividad de los equipos de trabajo y minimiza los riesgos, ya que todos los usuarios acceden a tus aplicaciones autoalojadas, SaaS o no web, sin necesidad de una VPN.

Acceso sencillo y seguro para el trabajo híbrido

Acceso a la red Zero Trust (ZTNA) nativa de Internet

El entorno de trabajo descentralizado actual exige un enfoque distribuido de la seguridad. El "perímetro" ya no existe, y las soluciones tradicionales de acceso remoto, como las VPN, no pueden responder a las expectativas modernas de seguridad o rendimiento.

El acceso a la red Zero Trust (ZTNA) proporciona acceso sencillo y seguro entre usuarios y aplicaciones, en cualquier dispositivo y en cualquier lugar, ya que comprueba continuamente el contexto granular, como la identidad y el estado del dispositivo, recurso por recurso. Con un enfoque totalmente nuevo, ya no hay que "equilibrar" la seguridad y la experiencia del usuario. ZTNA garantiza ambos aspectos, contribuyendo al éxito de tu negocio.

También permite a las organizaciones ser más ágiles y más capaces de entender el cambio, ya sea la migración a la nube, la actividad de fusiones y adquisiciones, o la capacidad de innovar y escalar rápidamente. Cloudflare es la clave de una estrategia Zero Trust o de modernización de la seguridad, ya que ofrece ZTNA en nuestra conectividad cloud global programable.

80 % Reducción en el tiempo promedio dedicado a resolver incidencias de soporte de acceso remoto relacionadas con el uso de una VPN [1]

72 % Tiempo ahorrado en la configuración mensual de políticas en comparación con proveedores anteriores [1]

68 % Porcentaje que vio un impacto significativo en la optimización de las experiencias de autenticación para usuarios y proveedores [1]

Ofrece a tu empresa acceso renovado

Refuerza la experiencia del usuario

Mejora la productividad de los equipos con seguridad modernizada que hace que las aplicaciones locales parezcan aplicaciones SaaS. Sin VPN engorrosas y lentas ni quejas de los empleados.

Elimina el movimiento lateral

Disminuye el riesgo cibernético y reduce la superficie de ataque otorgando un acceso de privilegio mínimo por recurso, basado en el contexto, en lugar del acceso a nivel de red.

Escala fácilmente Zero Trust

Mejora la eficiencia tecnológica protegiendo primero las aplicaciones esenciales o los grupos de usuarios más expuestos al riesgo, y luego ampliando el ZTNA nativo de Internet a toda tu empresa.

Principales casos de uso de Access

Implementa Zero Trust y un trabajo híbrido seguro

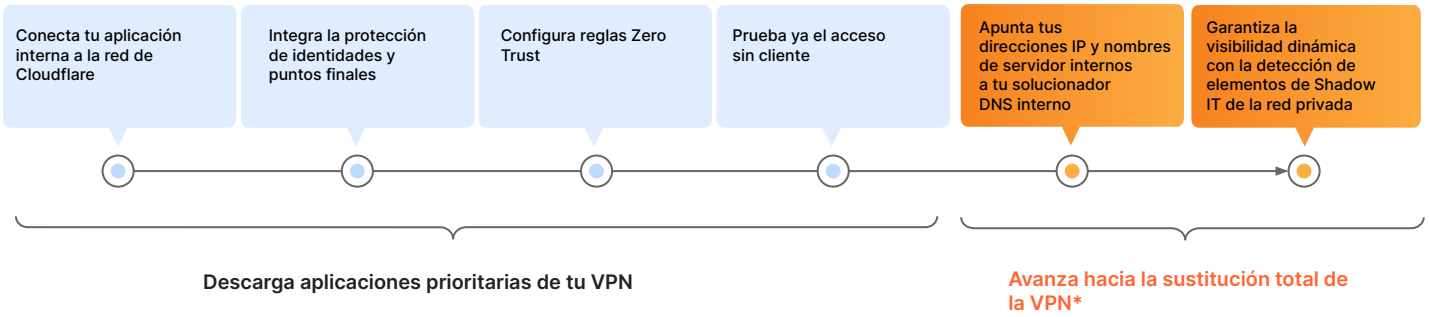
- ★ **Mejora y sustitución de VPN** — Access es más rápido y seguro que las VPN tradicionales. Empieza a descargar aplicaciones esenciales para mejorar la seguridad y la experiencia del usuario final.
- ★ **Acceso para proveedores** — Autentica a usuarios de terceros, como proveedores con opciones sin cliente, proveedores de identidad de redes sociales, etc.
- **Acceso para desarrolladores** — Proporciona a los usuarios técnicos acceso seguro a la infraestructura esencial sin desventajas en el rendimiento.

Facilita la modernización digital

- **Acelera los procesos de fusión y adquisición** — Evita por completo una fusión de red tradicional. Permite una integración con varios proveedores de identidad y acceso interno por aplicación durante los procesos de fusión y adquisición.
- **Autenticación multifactor (MFA) resistente al phishing**— Implementa una autenticación eficaz, como las claves de seguridad compatibles con FIDO2, a nivel global.
- **Protege los flujos de trabajo de desarrollo y operaciones** — Protege los flujos de trabajo de servicio a servicio con conectividad de malla/punto a punto, compatible con el tráfico bidireccional.

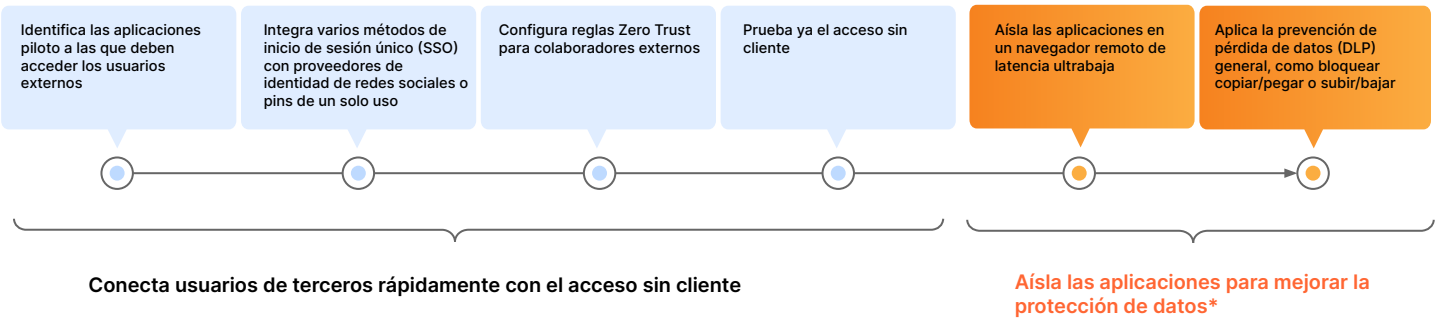
Primeros pasos: mejora y sustitución de la VPN

Prioriza las aplicaciones esenciales o los usuarios más expuestos al riesgo cuando pruebes una solución ZTNA para mejorar tu VPN. Utiliza el acceso sin cliente para aplicaciones web o SSH en el navegador a fin de agilizar las pruebas. Implementa funciones avanzadas con el tiempo para avanzar hacia la sustitución total de la VPN y mantener una visibilidad dinámica a medida que cambia tu red.



Primeros pasos: acceso de proveedores (terceros)

Ofrece experiencias de usuario fáciles y al mismo tiempo mitiga el riesgo de los dispositivos no administrados. Configura opciones de autenticación sencillas para los proveedores, sin necesidad de software de usuario final. Incorpora funciones avanzadas con el tiempo para implementar una mayor protección de los datos.



**Utilización de funciones de otros componentes de la plataforma Zero Trust*

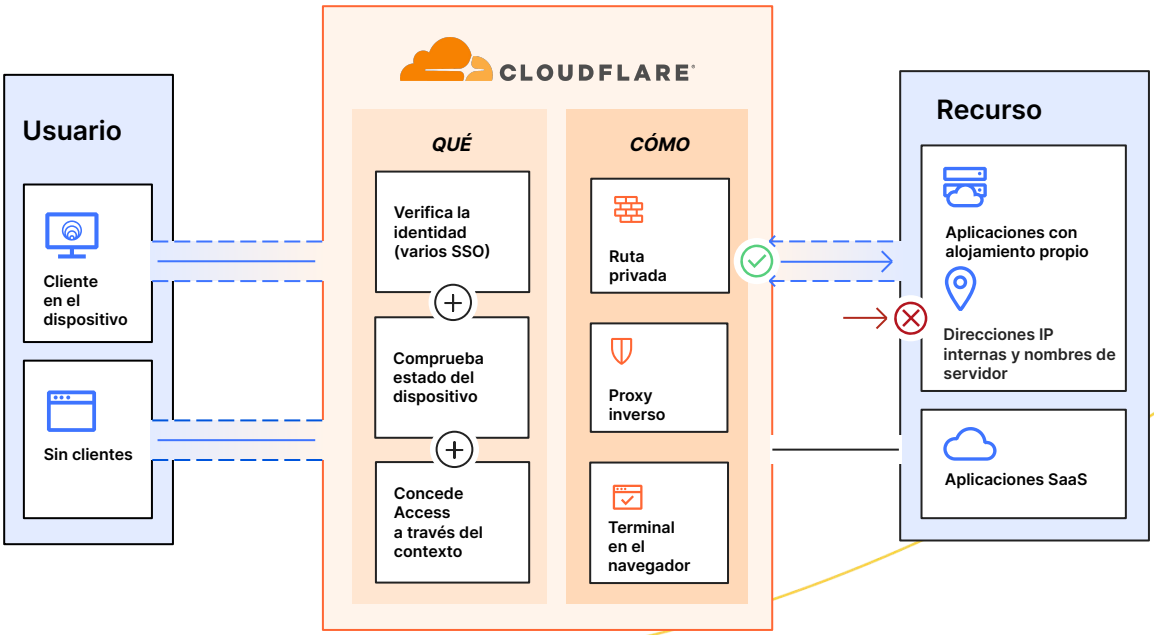
Cómo funciona Access

Cloudflare Access es una capa de agregación flexible que verifica continuamente el contexto granular, como la identidad y el estado del dispositivo, para proporcionar un acceso sencillo y seguro a todos los recursos de una organización de forma individual, creando un perímetro definido por software. Cuando un usuario se autentica y cumple todos los criterios de la política de acceso, Access emite un token web JSON firmado válido para una duración de sesión determinada. Realizamos una inspección de paso único en todas las solicitudes de los usuarios a través de nuestra plataforma modular, y nuestra experiencia de administración centralizada de políticas propaga los cambios de políticas globalmente en segundos gracias a nuestra exclusiva arquitectura de red Anycast.

El funcionamiento unificado sin cliente y basado en el cliente gestiona todos los tipos de dispositivos. Utilizamos un cliente de dispositivo para todos los servicios Zero Trust que encripta el tráfico a nuestra red para mantener la privacidad de los datos de nuestros clientes. También brindamos acceso sencillo y seguro a dispositivos fuera de la empresa mediante nuestra configuración sin cliente. Nuestros servicios de ZTNA, DNS, WAF y protección DDoS, líderes del mercado, trabajan juntos para crear y proteger nombres de host públicos accesibles a usuarios de terceros y equipos híbridos en cualquier dispositivo. Nuestras opciones de autenticación sin usuario (tokens o certificados mTLS) también abordan casos de uso de servicios automatizados y dispositivos IoT.

Para los controles Zero Trust, los recursos utilizan nombres de host públicos para proxy inverso a aplicaciones autoalojadas (en la nube/locales) o SSH/VNC en el navegador, proxy de identidad a aplicaciones SaaS, o enrutamiento privado basado en cliente/túnel mediante proxy de reenvío de capas 4-7 a cualquier recurso web o no web (p. ej., TCP/UDP arbitrario) dentro de una subred privada. Nuestra red global y el software de conectores de aplicaciones combinados admiten cualquier entorno informático, nube pública, incluidos Kubernetes y contenedores, o recursos de red locales heredados, sin necesidad de infraestructura de máquinas virtuales y sin limitaciones de rendimiento, a diferencia de otros proveedores de Zero Trust.

Las herramientas de identidad, punto final, acceso a la red, registro/análisis y SIEM de terceros están integradas en nuestro panel junto con opciones nativas para nuestro cliente de dispositivo y análisis, lo que garantiza la agilidad de la actividad de los administradores y el trabajo de desarrollo con las herramientas que ya utilizan.



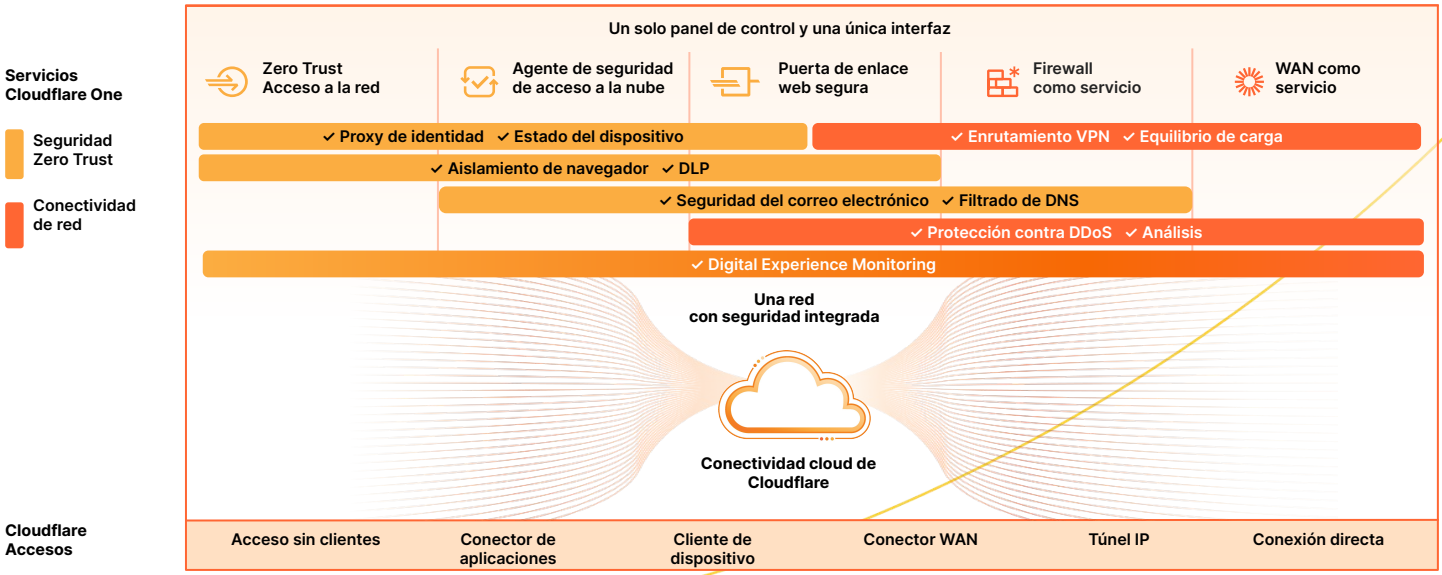
Access, parte de la plataforma SSE y SASE de Cloudflare

Mientras que SSE y SASE a menudo implican una trayectoria estratégica de varios años, Cloudflare ve con frecuencia que las organizaciones empiezan con ZTNA porque implica medidas prácticas y accesibles para los equipos informáticos, al tiempo que demuestra un importante valor empresarial a corto plazo. Los líderes informáticos tratan de proteger el trabajo híbrido, defenderse de las amenazas y salvaguardar sus datos en su camino hacia la consolidación, y suelen recurrir cada vez más a Cloudflare como socio de confianza.

La flexibilidad de implementación y la arquitectura modular de Cloudflare permiten a cualquier organización proteger y acelerar el rendimiento de dispositivos, aplicaciones y redes enteras para garantizar la protección y la productividad del trabajo híbrido. Para ello, admitimos la incorporación sin agente para los usuarios finales, el aislamiento web sin cliente para contener el tráfico peligroso y un panel de gestión unificado que permite la visibilidad de todos los servicios de seguridad y red, independientemente del lugar desde el que se conecten los administradores o los usuarios. La amplitud de la red global de Cloudflare permite que la seguridad se aplique más cerca de los usuarios finales, minimizando la latencia y ofreciendo experiencias ágiles a los usuarios. Nuestra arquitectura Anycast ayuda a sortear las interrupciones de Internet, manteniendo a los equipos en línea y ayudando a garantizar la continuidad operativa.

Con nuestra plataforma unificada SSE y SASE, el contexto compartido entre nuestras políticas ZTNA, CASB, DLP y SWG ayuda a reforzar la postura de seguridad al tiempo que simplifica la implementación mediante un flujo de trabajo de administración uniforme. Los mismos atributos de identidad y estado del dispositivo pueden informar tanto de las políticas de acceso para ZTNA y CASB como de las políticas de SWG, lo que simplifica la gestión de políticas en todas las organizaciones.

ZTNA, RBI y la seguridad del correo electrónico también se pueden utilizar conjuntamente para brindar acceso condicional a los recursos, aislando al mismo tiempo a los usuarios del contenido malicioso (enlaces, archivos adjuntos) al que están expuestos a través del correo electrónico y las herramientas de colaboración. A los proveedores y usuarios de dispositivos no gestionados se les puede brindar un acceso limitado a los recursos corporativos con interacciones de usuario (p. ej. cargar/descargar, copiar/pegar, entrada de datos con el teclado) deshabilitadas para evitar que se pongan en peligro los datos, y se pueden aplicar otras políticas de DLP de capa 7 para detectar datos confidenciales.



Qué dicen nuestros clientes

"Cloudflare Access es una gran alternativa a las VPN tradicionales. Los usuarios simplemente abren sus navegadores e inician sesión, sin tener que descargar o configurar ningún software adicional".

— **Platzi**, jefe de ingeniería de la nube

"Cloudflare Access llegó justo a tiempo para evitar que tuviéramos que sufrir la molestia de implementar una VPN. Fue una elección fácil para nosotros, y su implementación fue sorprendentemente sencilla".

— **ezCater**, jefe de seguridad

"Access es mucho más sencillo y seguro que una VPN para limitar el acceso a los activos internos. Solo tenemos que activarlo y agregar usuarios. Simplemente funciona".

— **Bitpanda**, director técnico y cofundador

"Antes de contar con Cloudflare, preparar una aplicación para su segura implementación implicaba un proyecto de 2 a 4 semanas. Con Zero Trust de Cloudflare, nos ahorramos aproximadamente el 90 % de ese tiempo".

— **Creditas**, responsable del equipo de ingeniería de redes

Lo que dicen los analistas

Cloudflare, nombrada empresa líder en el informe "2023 IDC MarketScape for Zero Trust Network Access (ZTNA)"

IDC cita la "enérgica estrategia de producto de Cloudflare para satisfacer las necesidades de seguridad empresarial". Creemos que este reconocimiento valida nuestro enfoque para ayudar a las empresas de cualquier tamaño a empezar a usar Zero Trust y a proteger el acceso de cualquier usuario a cualquier recurso, sin VPN.

Cloudflare es nombrada empresa "líder" en el informe "2022 KuppingerCole Leadership Compass for ZTNA"

En sus análisis del mercado de ZTNA de 2024, KuppingerCole Analysts AG citó varios puntos fuertes de Cloudflare. Entre ellos, nuestra plataforma de seguridad desarrollada de forma orgánica y completamente integrada, nuestra amplia infraestructura de nube global y nuestra vasta presencia en el mercado.

Funciones de Access

Creación/edición de políticas Zero Trust para garantizar acceso seguro	
Políticas de acceso granulares y personalizadas	Experiencia de administración de políticas centralizada. Las aplicaciones de capa 7 están protegidas a nivel de subdominio y ruta, con soporte para comodines y numerosos nombres de host, y admiten solicitudes CORS. Los cambios de política se propagan globalmente en segundos. Incluye comprobador de políticas.
Amplitud de recursos: qué podemos proteger y cómo	Los recursos utilizan nombres de host públicos para el proxy inverso a aplicaciones autoalojadas (en la nube/local) o SSH/VNC en el navegador, proxy de identidad a aplicaciones SaaS, o enrutamiento privado basado en cliente/túnel mediante proxy de reenvío de capas 4-7* a cualquier recurso web/no web (TCP/UDP arbitrario) dentro de una subred privada. También admite recursos/flujos de trabajo con tráfico bidireccional, por ejemplo, VoIP/SIP o canales de integración y distribución continuas (CI/CD).
Identidad	Autentica a través de los principales proveedores de identidad (IdP) corporativa y de redes sociales, incluidos varios IdP simultáneamente. También puede utilizar conectores genéricos SAML y OIDC. Admite (y puede aplicar) cualquier método de autenticación proporcionado por el IdP, autenticación temporal, justificación del propósito, intervalos de reautenticación en base a la sesión global o por aplicación, y opción de revocación inmediata de la sesión por aplicación o por usuario.
Estado del dispositivo	Verifica el estado del dispositivo utilizando integraciones de cliente de dispositivo y proveedor de protección de puntos finales (EPP) de terceros. Utiliza las integraciones de servicio a servicio para extraer las puntuaciones de riesgo del EPP en las políticas Zero Trust.
Señales contextuales para políticas	Configura señales como grupo de correo electrónico, rangos de IP, geolocalización, método de inicio de sesión (p. ej., tipo de autenticación multifactor, tipo de IdP), certificado mTLS o SSH válido, token de servicio, lista de números de serie, atributos de postura del dispositivo, cliente de dispositivo instalado, duración de la sesión, aplicación de reglas SWG o señales de llamadas API externas. También puede hacer referencia directa a las políticas de acceso condicional de Microsoft Entra ID (Azure AD).
Otro soporte relacionado	• **SCIM:** altas/bajas automáticas de usuarios para aplicaciones autoalojadas y SaaS (ejemplos para Okta y Azure AD). • **DNS interno:** configura el dominio de reserva local y resuelve las solicitudes de la red privada. • **División de túneles:** incluye/excluye direcciones IP para redes privadas o que funcionan junto a una VPN. • **Autenticación mTLS:** autenticación basada en certificados para IoT y otros casos de uso de mTLS. • **Aislamiento de aplicaciones:** con una sola casilla de verificación, aísla aplicaciones en nuestro navegador remoto ultrarrápido.*
Acceso de entrada y salida	
Conector de aplicaciones	La sencilla orquestación de nuestro conector ligero de aplicaciones (Cloudflare Tunnel) agiliza la conexión de recursos a Cloudflare, sin necesidad de infraestructura de máquinas virtuales y sin limitaciones de rendimiento. Incluye supervisión, redes virtuales (para solapamientos de direcciones IP) y funciones de redundancia y conmutación por error.
Cliente de dispositivo: Cuándo se utiliza	• **Sin cliente:** amplía las políticas Zero Trust a usuarios de terceros en dispositivos no gestionados. También combina bien con las políticas RBI y DLP de capa 7* sin cliente. El acceso sin cliente admite aplicaciones web y SSH/VNC en el navegador. • **Basado en cliente:** nuestro cliente de dispositivo (Cloudflare WARP) amplía el acceso seguro a redes privadas, permite integraciones de estado de dispositivo de servicio a servicio, y detecta la ubicación para aplicar políticas personalizadas para usuarios locales. También puede conectar dos o más dispositivos que ejecuten WARP para crear redes privadas. Los usuarios se pueden inscribir por su cuenta o hacer la implementación a través de MDM.
Extensibilidad y visibilidad	
Personalización de páginas	Sube HTML personalizado para que las pantallas de bloqueo y de inicio de aplicaciones se adapten a tu marca o transmitan instrucciones de acceso específicas para agilizar la experiencia del usuario final.
Registro	Registro completo de todas las solicitudes, usuarios y dispositivos. Puede utilizar logpush o API para la integración con las herramientas SIEM, orquestación y análisis existentes. En cuanto a los activos desconocidos, nuestra Shadow IT para infraestructura interna cataloga pasivamente el tráfico único de todos los orígenes.
Automatización	API intuitivas y proveedor Terraform disponibles para gestionar mediante programación todos los aspectos de una implementación Zero Trust. También ofrece soporte de token de servicio sin usuario para servicios automatizados.

**Utilización de funciones de otros componentes de la plataforma Zero Trust*

¿Por qué Cloudflare?

Fácil de configurar y gestionar

Simplifica significativamente la configuración y el funcionamiento del tráfico de acceso a los recursos privados con software de conector de aplicaciones y orquestación de túnel.

Experiencia fluida y siempre disponible

Consigue el máximo rendimiento de los usuarios finales y resiliencia a las interrupciones de la red con la tecnología Anycast global de Cloudflare, y garantiza así la fiabilidad.

Innovación rápida para los nuevos usuarios

Sigue el ritmo de la evolución de la propia red de Internet con un proveedor que está innovando constantemente, más que la competencia, para que el acceso a las aplicaciones sea más rápido y seguro.

Hablemos del acceso sencillo y seguro para tu organización

Solicitar seminario

CLOUDFLARE

¿Necesitas más tiempo?

Sigue leyendo en nuestra arquitectura de referencia SASE.

1. Estudio 2023: techvalidate.com/product-research/cloudflare/charts