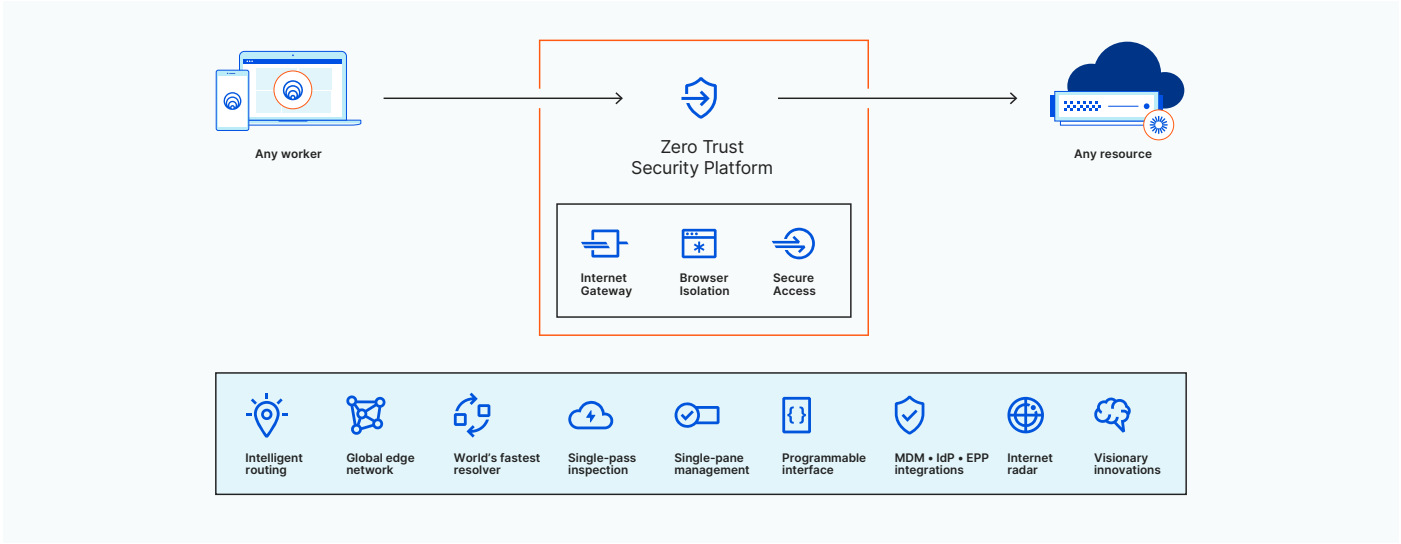
Cloudflare for Teams

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

La dispersión de las aplicaciones y los usuarios fuera de la zona de control de las redes empresariales obligó a los equipos de seguridad a alcanzar un compromiso sobre cómo mantener la seguridad de los datos. Los métodos centrados en la ubicación que implementaron para proteger el tráfico de los empleados, como las VPN, las listas de control de acceso y las listas de direcciones IP permitidas han sucumbido a la presión, limitando la visibilidad de las empresas, complicando las configuraciones y exponiendo a las organizaciones a un riesgo excesivo.

La plataforma de seguridad Zero Trust de Cloudflare aumenta la visibilidad, elimina la complejidad y minimiza los riesgos cuando los empleados se conectan a las aplicaciones e Internet. Se ejecuta en la red perimetral más rápida del mundo, lo que acelera el ritmo de implementación y ofrece un rendimiento mejor que otros proveedores.

Verifica, filtra, inspecciona y aísla el tráfico de los empleados con una inspección de paso único ultrarrápida



Beneficios

Reduce el exceso de confianza

Protege las aplicaciones corporativas con reglas de Zero Trust basadas en la identidad y el contexto, y aísla los puntos de conexión de los riesgos ejecutando el código web que no es de confianza lejos de los dispositivos.

Elimina la complejidad

Al reducir la dependencia de las VPN heredadas y de productos de seguridad específicos, los administradores pueden aplicar controles de seguridad estándar a todo el tráfico, independientemente de cómo se inicie esa conexión o del lugar de la pila de la red en el que se encuentre.

Restablece la visibilidad

Aumenta la visibilidad con registros detallados de DNS, HTTP, inicio de sesión y actividad dentro de las aplicaciones. Los administradores pueden monitorizar la actividad de los usuarios en las aplicaciones autohospedadas y SaaS, con una traza de auditoría para investigar incidentes.

Resultados de la implementación

80 %↓

menos tiempo dedicado a resolver incidencias informáticas y la postura de seguridad de los empleados.

91 %↓

reducción de la superficie de ataque al situar a Cloudflare delante del acceso a las aplicaciones y la navegación por Internet.

30 min

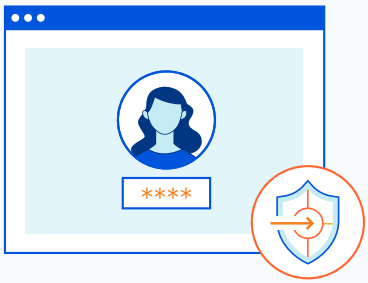
de tiempo de configuración para permitir un acceso más rápido y seguro a las aplicaciones e Internet.

Acceso a la red Zero Trust con enrutamiento privado

- Protege las aplicaciones con reglas basadas en la identidad, la postura y el contexto.
- Aplica controles de acceso y visibilidad coherentes en aplicaciones locales, en la nube y SaaS.
- Usa métodos de autenticación sólidos incluso en las aplicaciones heredadas con reglas de firewall de red y Zero Trust.

Puerta de enlace web segura con navegación Zero Trust

- Bloquea el phishing y el malware con la información de nuestro firewall de red y reglas de Zero Trust.
- Aísla la actividad de navegación de los puntos de conexión corporativos, mitigando el impacto de las fugas.
- Impide que los datos salgan de las aplicaciones corporativas y consigue visibilidad de Shadow IT.



La diferencia de Cloudflare

Una interfaz de gestión

Ofrece una mayor facilidad de uso a los administradores con un panel de control diseñado de forma nativa para el acceso a las aplicaciones e Internet que incluye integraciones con proveedores de identidad, protecciones de puntos de conexión y soluciones de acceso de red.

Una plataforma consolidada

Reduce la complejidad con una plataforma fácil de gestionar que consolida soluciones de puerta de enlace web segura, acceso a la red Zero Trust, filtrado de DNS, agente de seguridad de acceso a la nube (CASB) y prevención de pérdida de datos en un plano de control optimizado. Sustituye los clientes VPN, los firewall locales y otras soluciones de seguridad heredadas a medida y migra la seguridad y la conectividad al perímetro.

Experiencia inigualable para el usuario final

Cloudflare enruta las solicitudes más rápido utilizando un enrutamiento optimizado y basado en información a través de nuestra amplia red Anycast, con más de 200 ubicaciones en más de 100 países de todo el mundo.

De media, se accede a las aplicaciones web un 30 % más rápido y el tiempo de recorrido de ida y vuelta de las conexiones TCP se reduce un 17 %.

Funciones de Cloudflare for Teams

Soporte	
Canales de comunicación	**Soporte ininterrumpido por vía telefónica** **Soporte ininterrumpido por chat** **Correo electrónico**
Tiempo promedio de respuesta a correos electrónicos	**Menos de 1 hora**

Reducción de riesgos	
Acceso a la red Zero Trust	✔
Puerta de enlace web segura	✔
→ *Filtros de DNS recursivos*	✔
→ *Filtros de firewall en capa 4*	✔
→ *Filtros de firewall en capa 7*	✔
→ *Inspección antivirus*	✔
→ *CASB*	✔
→ *Aislamiento remoto del navegador*	**Complemento (integrado de forma nativa)**

Aumento de visibilidad	
Retención de registros de actividad	**6 meses**
Grupos de aplicaciones para visibilidad de Shadow IT	✔
Vistas detalladas del país, estado y dispositivo en función de la identidad	✔
Envío de registros al almacenamiento en la nube o SIEM	✔

Política coherente	
Políticas personalizadas de acceso a aplicaciones, redes privadas e Internet	**Sin límite**
Autenticación a través de proveedores de identidad corporativos y sociales	✔
Categorías de seguridad (13) mediante aprendizaje automático y fuentes de inteligencia	✔
Categorías de contenidos (más de 100) para uso aceptable	✔
Listas personalizadas de bloqueo, permiso o descifrado	✔
Reglas granulares HTTP y URL	✔
Controles de tipo de archivo	✔
Postura del dispositivo con integraciones de terceros y Cloudflare	✔
Importación masiva de listas basada en CSV	✔

Conexión segura	
Conexiones cifradas del cliente a Internet (cliente WARP)	**Win, Mac, iOS, Android**
Acceso seguro sin cliente a aplicaciones autohospedadas y SaaS	✔
Conexiones privadas para aplicaciones autohospedadas, direcciones IP y nombres de servidor (Cloudflare Tunnel)	✔
Seguridad a nivel de red para ubicaciones físicas	**50**
Ubicaciones de red IP editables	✔

Interoperabilidad sencilla	
Integraciones de gestión de puntos de conexión y movilidad	✔
Túnel dividido para conectividad local o VPN	✔
Autoinscripción de clientes para dispositivos no administrados	✔
Autenticación que admite varios proveedores de identidad simultáneamente	✔
Iniciador de aplicaciones personalizable	✔
Conectores genéricos y personalizados que admiten SAML y OIDC	✔
Autenticación basada en tokens para servicios automatizados	✔
Autorización basada en certificados para IoT y otros casos de uso de mTLS	✔

Sin afectar al rendimiento	
SLA de tiempo activo	**100 %**
Red perimetral a nivel global más rápida (más de 200 PoP)	✔
Actualizaciones de políticas globales más rápidas (<500 ms segundos)	✔
Enrutamiento IP inteligente más rápido (< 100 ms)	✔
Solucionador de DNS privado más rápido (7-31 ms)	✔
Navegador remoto más rápido y seguro (el doble de velocidad que otros)	**Complemento**

¿Quieres probar Cloudflare for Teams? Visita www.cloudflare.com/teams/ hoy mismo