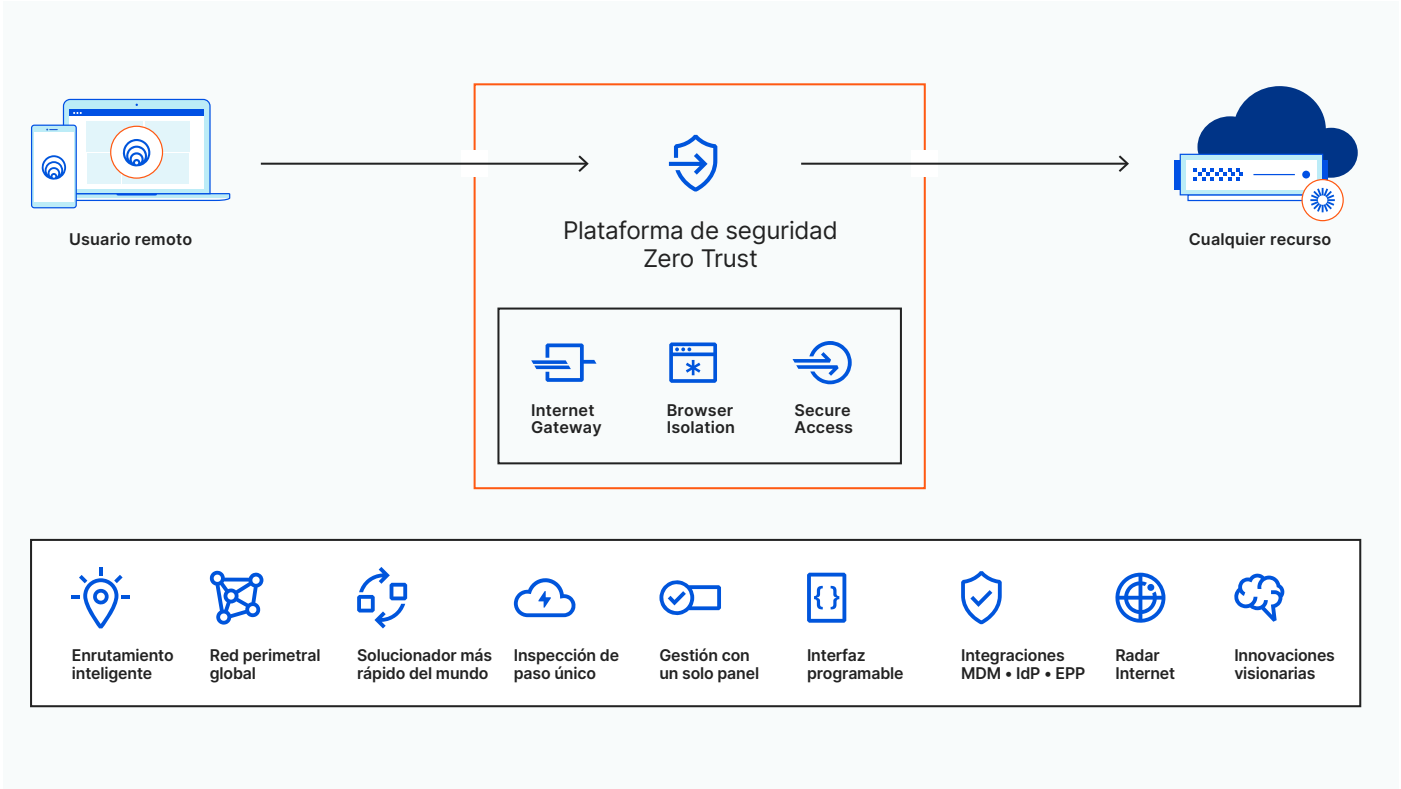
Protección de la conectividad de usuarios remotos a largo plazo con Cloudflare

Cuando la COVID-19 obligó a muchas empresas a implantar el trabajo a distancia de la noche a la mañana, tuvieron que esforzarse por garantizar la conectividad de los empleados. Algunas soluciones eran estratégicas, pero otras no dejaban de ser parches tácticos, p. ej. reforzar las VPN lentas y poco fiables, dividir el tráfico de Internet en túneles y piratear el acceso remoto precipitadamente. Ahora están empezando a aparecer las primeras deficiencias de este enfoque, ya que persisten los desafíos relativos a la visibilidad, la seguridad y la complejidad.

Los fallos de seguridad asociados al trabajo remoto no deberían resolverse en meses o semanas. Con Cloudflare Zero Trust, los administradores pueden abordar más de 20 casos de uso urgentes de seguridad y conectividad de los usuarios en solo 30 minutos.

La solución: Cloudflare Zero Trust



La plataforma de seguridad Zero Trust de Cloudflare aumenta la visibilidad, elimina la complejidad y reduce los riesgos asociados a la conexión de los usuarios remotos 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 el de otros proveedores.

Tres formas de mejorar la seguridad de los usuarios remotos con una plataforma Zero Trust

Reducir riesgos

La dependencia de las VPN ha creado un riesgo de conmutación por error y ha permitido a los atacantes explotar las vulnerabilidades de la infraestructura corporativa. Una vez que un atacante consigue acceso, puede moverse lateralmente a través de varios recursos para robar datos. Pese a hacer todo lo posible para bloquear y abordar las amenazas, los puntos de conexión siguen viéndose afectados por malware no detectado.

Las plataformas de seguridad Zero Trust reducen los riesgos del trabajo remoto porque aplican la identidad y la autenticación basada en contexto en cada solicitud a tus aplicaciones corporativas, lo que apenas deja margen al movimiento lateral. El aislamiento del navegador aísla los puntos de conexión de la actividad del navegación, mitigando así las amenazas conocidas y desconocidas.

Aumentar la visibilidad

Cuando los usuarios trabajaban desde la oficina, era sencillo mantener registros de actividad, pero mantener un registro de auditoría es mucho más difícil cuando los empleados están distribuidos geográficamente y trabajan desde nuevos dispositivos. Las capacidades de registro dentro de las aplicaciones SaaS a menudo son inconsistentes y analizar los registros VPN puede ser complicado.

Las plataformas Zero Trust restauran la visibilidad al interceptar y registrar solicitudes de todos los dispositivos remotos, incluso los dispositivos no administrados. Los administradores pueden supervisar la actividad de los usuarios remotos en las aplicaciones alojadas internamente y SaaS, con un registro de auditoría para investigar incidentes. Los registros están centralizados en un solo panel de control y se envían automáticamente al SIEM elegido.

Eliminar la complejidad

Los parches implementados para conectar a los usuarios remotos están resultando demasiado precarios a largo plazo. Los administradores se ven obligados a administrar políticas de filtrado de tráfico con varias herramientas incompatibles, al tiempo que los usuarios se sienten frustrados por el rendimiento deficiente.

Las plataformas Zero Trust simplifican la forma en que los usuarios se conectan y optimizan el trabajo de los administradores. Con una menor dependencia de las VPN heredadas, los administradores pueden aplicar controles de seguridad estándar a todo el tráfico, independientemente de cómo se inicie esa conexión o dónde se aloja en la red. Y todas las políticas se pueden administrar desde un único panel de control.

Seguridad Zero Trust en acción

En una arquitectura de un solo paso, el tráfico de los usuarios remotos se inspecciona, aísla, registra y protege de las amenazas de Internet, y el rendimiento nunca se ve afectado, ya que los usuarios se conectan a los centros de datos más cercanos.