CLOUDFLARE

IMPACTO SOBRE EL NEGOCIO

Cómo Zero Trust reduce el riesgo y mejora la eficiencia de la tecnología

Protege más con menos gasto

Cuantificar el impacto en las finanzas y la seguridad de las prácticas recomendadas Zero Trust

Reduce el riesgo cibernético

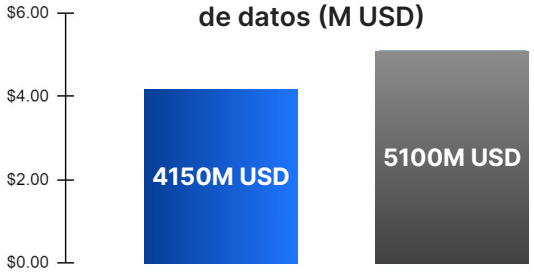
95 % reducción de la superficie de ataque con una arquitectura SASE, que incluye los principios Zero Trust integrados [1]

72 % de los responsables de TI declaran que la razón principal de su adopción de Zero Trust fue "reforzar la seguridad de los datos" [2]

61 % de profesionales de TI/seguridad señalan como una ventaja la "autenticación más eficaz utilizando la postura de riesgo e identidad" [3]

↓23 % reducción del coste medio de una fuga de datos en las organizaciones con Zero Trust implementado vs. sin Zero Trust [4]

Coste medio de una fuga de datos (M USD)



Mejora la eficiencia de la tecnología

7M USD reducción media del gasto en la seguridad heredada adoptando Zero Trust en las cinco organizaciones [5]

20 USD/ FTE al mes ahorrado al reemplazar servicios de seguridad redundantes con una plataforma Zero Trust basada en la nube [5]

↓80 % reducción del esfuerzo necesario para suministrar y proteger la nueva infraestructura [5]

39 % de tecnologías de la seguridad que utilizan las organizaciones están obsoletas y se pueden modernizar con Zero Trust [6]

Consecuencias principales de la complejidad de la ciberseguridad [7]

N.° 1 Pérdidas financieras debido a fugas de datos o ciberataques que han tenido éxito

N.° 2 Incapacidad de innovar tan rápido como requieren las oportunidades del mercado

N.° 3 Falta de resiliencia operativa

Motores

- Reducir el exceso de confianza con controles basados en la identidad y el contexto para cada solicitud
- Mejorar la visibilidad para todos los usuarios, aplicaciones y dispositivos para una corrección más rápida
- Reducir el movimiento lateral de las amenazas

Motores

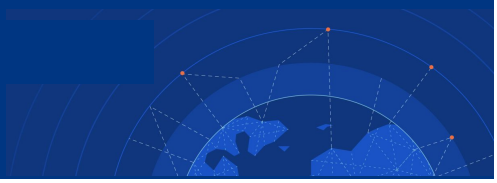
- Reducir la complejidad consolidando soluciones puntuales heredadas en una única plataforma en la nube
- Simplificar los flujos de trabajo de la seguridad sin redireccionamientos a través de los dispositivos locales
- Políticas coherentes para tus usuarios híbridos

Zero Trust es un cambio de mentalidad estratégico para tu organización

Seguridad de TI heredada: El perímetro determina la confianza		Zero Trust: Sin perímetro, verificar siempre
Perímetro protegido, seguro dentro de la red (es decir, seguridad perimetral)	Protección	Asumir el riesgo, reducir el impacto (encriptar, inspeccionar, microsegmentar)
Registrar solo inicio de sesión en el perímetro	Visibilidad	Registrar todos los inicios de sesión y solicitudes, en cualquier ubicación
Permitir por defecto, acceso estático en función de la ubicación de la red	Control	Denegar por defecto, privilegio mínimo en función de la identidad y el contexto

Empieza a reducir el ciberriesgo con Zero Trust

Solicitar una reunión



¿Aún no estás preparado para realizar tu consulta?

- Descubre cómo Zero Trust mejora la productividad del equipo: leer el resumen
- Más información acerca de cómo organizaciones similares abordan el trabajo híbrido: leer el resumen
- Explora una hoja de ruta independiente de proveedores para lograr Zero Trust: leer el documento técnico

1. Basado en experiencias de clientes de Cloudflare
2. "Capterra's 2022 Zero Trust Survey", agosto de 2022 (enlace)
3. "Global Study on Zero Trust Security for the Cloud", Ponemon Institute LLC, julio de 2022 (enlace)
4. "The Cost of a Data Breach Report", IBM, 2022 (enlace)
5. "The Total Economic Impact ™ of Zero Trust Solutions from Microsoft", Forrester Research, diciembre de 2021 (enlace)
6. "Security Outcomes Study", Cisco, diciembre de 2021 (enlace)
7. "2022 Global Digital Trust Insights", PWC, septiembre de 2022 (enlace)