

# Los cortafuegos y las VPN no son adecuados para la confianza cero

La habilitación y protección de su personal distribuido requiere un nuevo enfoque de la seguridad.

## La forma de trabajar ha cambiado.

Usuarios, datos y aplicaciones están en todas partes.

**300 %**

de aumento en el porcentaje del total de empleados que son usuarios remotos.<sup>1</sup>

**50 %**

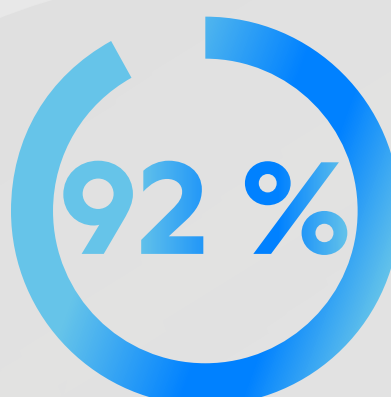
de todos los datos corporativos se almacena en la nube.<sup>2</sup>

**70 %**

de las aplicaciones empresariales que las empresas utilizan hoy en día se basan en SaaS.<sup>3</sup>

## ¿No debería cambiar también la seguridad?

Proteger el perímetro y confiar en lo que hay en la red funcionaba bien en entornos exclusivamente locales. Pero en la actualidad, el perímetro ha desaparecido y las antiguas formas de proteger la red simplemente ya no funcionan.



de las organizaciones sienten que necesitan actualizar su seguridad para proteger mejor a los trabajadores remotos y en la oficina.<sup>4</sup>



de las empresas están dando prioridad a la adopción de un modelo de confianza cero.<sup>5</sup>

## La solución es la confianza cero.

Para que las empresas habiliten a su personal actual y sigan siendo ágiles y competitivas, las arquitecturas de seguridad deben evolucionar. Ha llegado el momento de pasar a una solución que autorice las conexiones basándose en el contexto y la política para cada sesión de cada usuario a cada aplicación, en cualquier lugar.

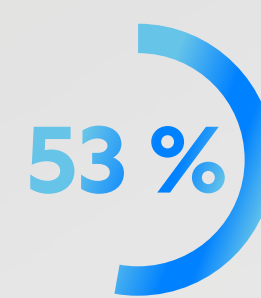
## Pero los cortafuegos y las VPN no son compatibles con la confianza cero. ¿Por qué?

Las amenazas pueden acceder y desplazarse fácilmente por la red, porque los cortafuegos siguen requiriendo la conexión de usuarios y dispositivos a la red para acceder a las aplicaciones.



de las empresas no confían en que sus tecnologías actuales puedan ayudarles a conseguir la confianza cero.<sup>5</sup>

Las aplicaciones se publican en Internet, lo que aumenta su superficie de ataque.



de las organizaciones cometerán el error de confiar en sus tecnologías existentes y colocarán a los usuarios en la red corporativa.<sup>5</sup>

Las arquitecturas de paso de cortafuegos limitan la capacidad de inspeccionar el tráfico y proteger los datos.

## La confianza cero requiere un enfoque fundamentalmente diferente.

A diferencia de los enfoques tradicionales que confían en todo lo que se encuentra dentro del perímetro de la red, la confianza cero parte del principio de acceso con privilegios mínimos y la idea de que ningún usuario o aplicación debe ser inherentemente confiable. Una verdadera solución de confianza cero conecta de forma segura las aplicaciones y los usuarios a través de Internet basándose en las políticas empresariales para:



### Elimine el movimiento lateral

Conectar directamente usuarios y dispositivos a aplicaciones, nunca a la red.



### Minimizar la superficie de ataque

Hacer que los usuarios y las aplicaciones sean invisibles en lo referente a Internet. Si no se pueden detectar, no hay superficie de ataque que atacar.



### Detenga las amenazas y la pérdida de datos

Ofrece una inspección completa, incluido el tráfico cifrado, para una protección eficaz contra las amenazas cibernéticas y la pérdida de datos.

## Zscaler: el líder en confianza cero.

Construido en la mayor nube de seguridad del planeta, Zscaler Zero Trust Exchange ayuda a los equipos de TI a adoptar la confianza cero para reducir el riesgo, aumentar la agilidad del negocio y ofrecer una gran experiencia de usuario.

Todos los días Zscaler Zero Trust Exchange:

**ASEGURA MÁS DE 200 MIL MILLONES** de transacciones

**PREVIENE MÁS DE 7 MILLONES** de incidentes de seguridad y violaciones de la política.

**PROCESA MÁS DE 200 000** actualizaciones de seguridad exclusivas

## Comience su travesía de confianza cero con Zscaler.

Zscaler ha ayudado a más de 5000 empresas a transformarse de forma segura utilizando la confianza cero.

Y también podemos ayudarle a usted.

Descubra cómo

