

EL BORDE DE CONFIANZA CERO:

UNA RED MÁS SEGURA DESDE EL PRINCIPIO

El trabajo remoto aceleró la migración a la nube. ¿Cuál es tu plan para mejorar el rendimiento de la red y evitar problemas de seguridad? ¿De qué manera necesitas cambiar tu arquitectura?



El 53 % de los nuevos trabajadores remotos quiere seguir trabajando de esa forma.



La nube, el borde y la IoT redefinieron la ubicación de los datos y las aplicaciones.

Integra las redes y la seguridad para aumentar la protección de tus negocios

Las infraestructuras de redes y seguridad fragmentadas ya no son sostenibles



En la nube, hay cada vez más aplicaciones empresariales.



Los usuarios y dispositivos ya dejaron atrás el perímetro empresarial tradicional.

Los modelos de redes y seguridad antiguos ya no sirven

Consecuencias de estructuras de redes y seguridad fragmentadas e inconexas, y de métodos inflexibles centrados en el hardware:



Más complejidad, menos flexibilidad y menor eficacia



Obstáculos en la capacidad de resiliencia y la recuperación ante desastres



Pérdida de oportunidades y posibilidad de quedar atrás de los competidores



Dificultad para cumplir con los requisitos operativos de la nube y respaldar a los teletrabajadores

La importancia del borde de confianza cero (ZTE)

Una solución de borde de confianza cero (Zero Trust Edge, ZTE) utiliza principios de acceso de confianza cero para conectar el tráfico, y transportarlo dentro y fuera de sitios remotos. Para lograrlo, normalmente se usan servicios de redes y seguridad en la nube.

Un servicio de acceso seguro al borde (SASE) es un borde de confianza cero (ZTE). La arquitectura de red SASE usa un modelo de software en la nube para integrar funcionalidades de SD-WAN y seguridad en el "borde de servicios", donde se conectan los dispositivos y las redes.

Forrester 2021

¿Cuáles son los beneficios de ZTE y SASE?

- ✓ Incorporar seguridad en el ADN de las redes
- ✓ Dar prioridad al tráfico de las aplicaciones comerciales más importantes en la WAN de la sucursal
- ✓ Proteger los negocios contra clientes, empleados, contratistas y dispositivos que se conectan a entornos de alto riesgo a través de estructuras WAN
- ✓ Proporcionar acceso seguro a aplicaciones y servicios corporativos para garantizar la seguridad de los trabajadores remotos
- ✓ Proteger a Internet contra todo, desde dispositivos de IoT y del borde hasta socios comerciales
- ✓ Centralizar la gestión, el control y el análisis del conjunto de servicios de redes y seguridad que residen en las soluciones de ZTE

¿Deberías usar ZTE? Tres preguntas para tu empresa

1 ¿Qué nivel de segregación hay en la seguridad y las redes?

2 ¿Tienes dificultades para garantizar la seguridad de los dispositivos y usuarios en el borde?

3 ¿Estás listo para que el 53 % de los trabajadores se queden en casa?

PRESENTAMOS EL MODELO DEL BORDE DE CONFIANZA CERO PARA SERVICIOS DE REDES Y SEGURIDAD:

UN SERVICIO DE ACCESO SEGURO AL BORDE (SASE) ES UN BORDE DE CONFIANZA CERO (ZTE)

Si accedes al informe completo de Forrester, encontrarás las respuestas a estas preguntas:

- ¿Por qué están desapareciendo rápidamente las infraestructuras de redes y seguridad fragmentadas?
- ¿Cuál es el mejor método de ZTE para tu empresa?
- ¿Cómo se deben evaluar las opciones de uno o varios proveedores?



Leer el informe [→](#)