INFOGRAFÍA

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.[1]

50 %
de todos los datos corporativos se almacena en la nube.[2]

70 %
de las aplicaciones empresariales que las empresas utilizan hoy en día se basan en SaaS.[3]

¿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.

92 %
de las organizaciones sienten que necesitan actualizar su seguridad para proteger mejor a los trabajadores remotos y en la oficina.[4]

El 72 %
de las empresas están dando prioridad a la adopción de un modelo de confianza cero.[5]

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.

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

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

47 %
de las empresas no confían en que sus tecnologías actuales puedan ayudarles a conseguir la confianza cero.[5]

53 %
de las organizaciones cometerán el error de confiar en sus tecnologías existentes y colocarán a los usuarios en la red corporativa.[5]

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

1. *Grady, John. (2021). El estado de las estrategias de seguridad de confianza cero Enterprise Strategy Group. https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies*
2. *Statista. Porcentaje de datos y datos confidenciales almacenados en la nube en todo el mundo. https://www.statista.com/statistics/1202541/sensitive-data-cloud-location*
3. *Better Cloud. (2021). El estado de SaaSOps 2021. https://stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1909514686.1636678142*
4. *Encuesta de IDG Marketpulse. (2021). Enfoques de seguridad de red y razones que justifican la confianza cero. https://info.zscaler.com/industry-report-leading-cxo-and-it-leaders-see-it-future-in-zero-trust-thank-you*
5. *Cybersecurity Insiders. (2021). Informe de riesgo de las VPN. https://info.zscaler.com/resources-industry-reports-vpn-risk-report-cybersecurity-insiders*

©2021 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zscaler Zero Trust Exchange™, Zscaler Internet Access™ y Zscaler Private Access™, ZIA™ y ZPA™ y Zscaler B2B™ son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

Zscaler, Inc.
120 Holger Way
San José, CA 95134
+1 408 533 0288
www.zscaler.es