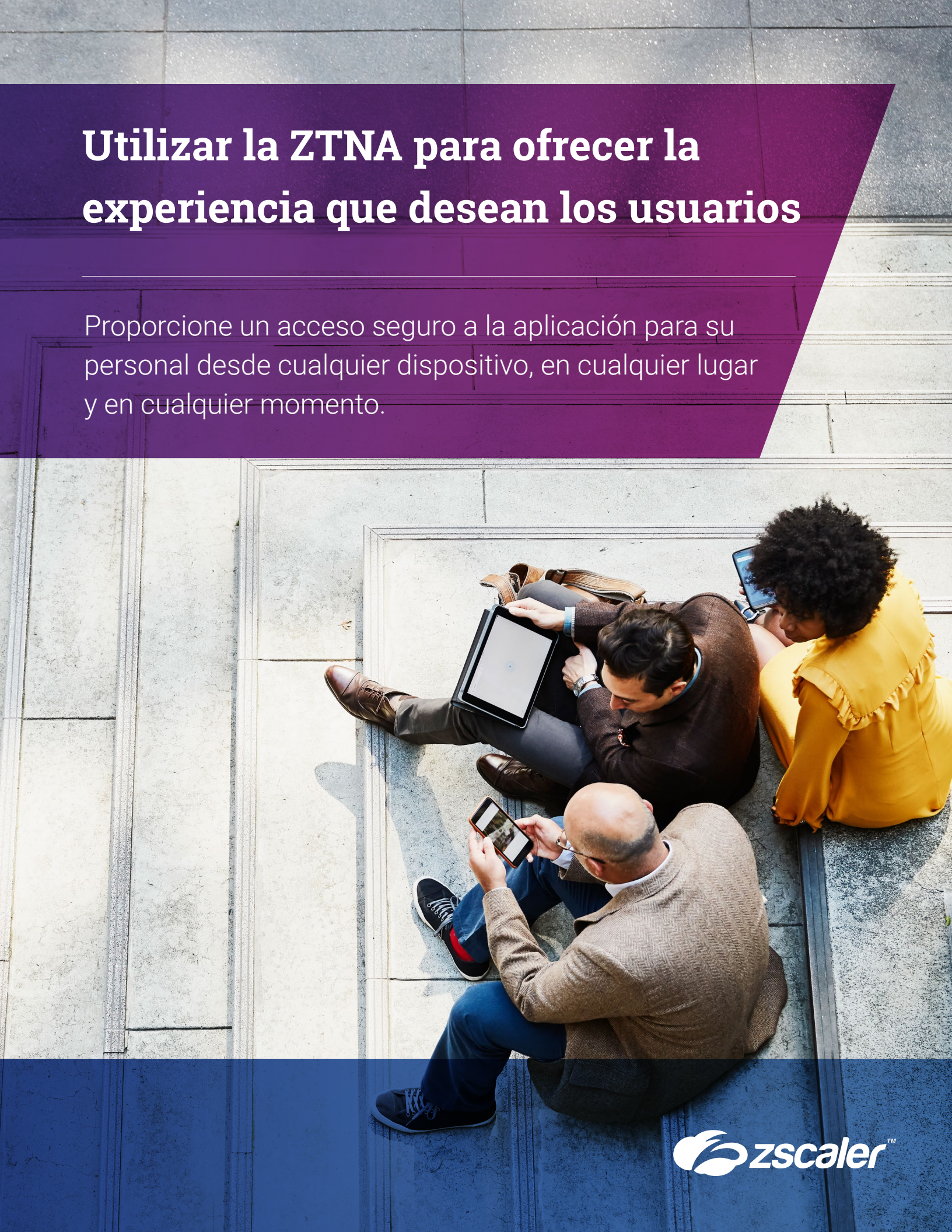
Utilizar la ZTNA para ofrecer la experiencia que desean los usuarios

Proporcione un acceso seguro a la aplicación para su personal desde cualquier dispositivo, en cualquier lugar y en cualquier momento.



zscaler™

"Queremos que la gente no tenga que pensar en cómo acceder a sus aplicaciones y queremos apoyar esa capacidad rápidamente con la menor fricción posible".

- Mike Towers, CSO de Takeda

Su base de usuarios ha evolucionado

Estamos en 2020 y su personal ya no está encerrado en la oficina. Está trabajando desde casa, desde hoteles y desde aeropuertos. Los dispositivos que utiliza ya no son dispositivos BlackBerry gestionados que reciben del equipo de objetivos. Son smartphones, tabletas y portátiles personales BYOD que se utilizan tanto para el ocio como para el trabajo.

Usted es responsable no solo de la seguridad de sus empleados, sino también de la de los terceros contratistas que están en la nómina de la empresa. Todos estos usuarios necesitan un acceso idéntico a las aplicaciones privadas en todos los dispositivos, ubicaciones y tipos de aplicaciones. Proporcionar acceso desde estos dispositivos, sin comprometer la seguridad, se convirtió en una imposibilidad en un momento dado. Ya no lo es.

Un vistazo a su cartera de usuarios

Con una plantilla diversificada y distribuida por todo el mundo, proporcionar un acceso seguro a las aplicaciones privadas se ha convertido en un desafío para los equipos de TI. Aunque la plantilla puede tener un aspecto diferente al de hace 15 años, todavía hay algo que tienen en común: todos sus usuarios necesitan un acceso rápido y fiable a las aplicaciones privadas para que la empresa siga funcionando sin problemas. Su plantilla moderna puede tener un aspecto similar al siguiente:

El viajero

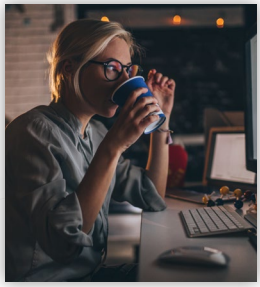
Sam Davis, vicepresidente de ventas

"Probablemente paso alrededor del 75 % de mi tiempo de viaje. La mayoría de las veces, estoy en un aeropuerto, un hotel o en las instalaciones de un cliente, intentando aprovechar los periodos de espera para trabajar. Aunque mi entorno de trabajo cambie constantemente, sigo necesitando acceder a nuestros recursos empresariales rápidamente para poder atender mejor a nuestros clientes".

El local

Danielle Allen, directora financiera

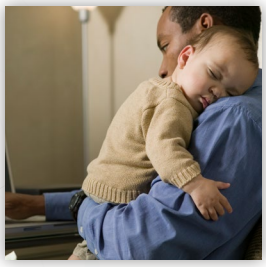
"Trabajo en nuestra sede central en San José, California, y soy principalmente una empleada "de oficina". A diario, otros empleados me solicitan información acerca de sus pagos. Utilizo constantemente nuestras aplicaciones financieras y necesito acceder a ellas rápidamente para poder estar al día con las solicitudes".



El contratista

Elaina Thalin, contratista de desarrollo web

"Llevo aproximadamente 8 meses como contratista con la empresa". Aunque no soy empleada ni trabajo físicamente en la oficina, sigo necesitando acceso a algunas aplicaciones privadas para poder trabajar. Si no puedo acceder a ellas, no puedo hacer mi trabajo".



El trabajador desde casa

Justin Miller, director de marketing

"Vivo en Florida y a menudo me afectan las alertas meteorológicas, incluidos los huracanes. En esos momentos, he tenido que garantizar mi seguridad y la de mi familia sin dejar de cumplir mis responsabilidades laborales".

Independientemente del tipo de usuario o del trabajo que desempeñe, su personal seguirá necesitando poder acceder a sus aplicaciones privadas de forma rápida y segura dondequiera que estén. El departamento de TI debe contar con la tecnología adecuada para que esto sea posible y garantizar que la seguridad no se interponga en la productividad del usuario. Por eso, la VPN no está a la altura de los empleados modernos.

Sus usuarios se merecen algo mejor que una VPN

Debido a que la VPN se desarrolló hace más de 30 años, ya no es adecuada para su uso con el personal actual, ya que su diseño de seguridad defectuoso ofrece una experiencia de usuario deficiente.

Alta latencia, escala limitada y mala experiencia

Las VPN se diseñaron para asegurar el acceso a la red. Esto significa que todo el tráfico de los usuarios se devuelve primero al centro de datos, incluso si las aplicaciones se ejecutan ahora en la nube pública. Esto provoca un tromboning de la red, que a su vez crea latencia para los usuarios. Además, los dispositivos VPN tienen limitaciones de capacidad para los usuarios y pueden desbordarse si demasiados usuarios simultáneos acceden al servidor VPN a la vez.

Inicios de sesión repetitivos y conexiones interrumpidas

Cada vez que hay un cambio o inactividad en la red, la conexión VPN se interrumpe. Para un personal que es ahora móvil, esto puede ocurrir con bastante frecuencia, lo que provoca frustración y pérdida de productividad del usuario.

Confusión acerca de cuándo usar la VPN... o no

A menudo ocurre que los usuarios ni siquiera saben cuál es la diferencia entre sus aplicaciones públicas y privadas. Ahora que aplicaciones están transfiriéndose a la nube, es aún más confuso para el usuario saber cuándo, dónde y cómo debe usar la VPN. Obviamente, la VPN no es perfecta ni intuitiva para sus usuarios.

Al igual que Netflix no se podría haber construido conectando miles de reproductores de DVD, las soluciones de acceso a aplicaciones privadas para el acceso en cualquier momento y lugar deben ser diseñadas específicamente para tal fin. Deben estar siempre disponibles, ser altamente escalables y estar centradas en el usuario. Adaptar los dispositivos VPN en el centro de datos, virtualizarlos o colocarlos en la nube no resolverá los desafíos que supone la experiencia del usuario ni los retos relacionados con la seguridad de la red que genera un mundo móvil. **Se necesita un nuevo enfoque.**

"Para 2023, el 60 % de las empresas eliminarán la mayoría de sus redes privadas virtuales (VPN) de acceso remoto a favor de ZTNA".

Gartner, Guía de mercado para el acceso a la red de confianza cero
Steve Riley, Neil MacDonald, Lawrence Orans, abril de 2019

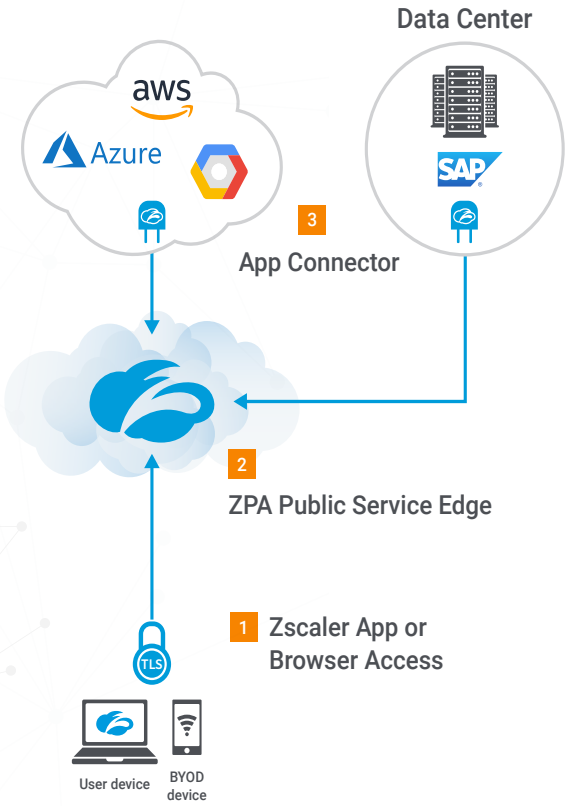
Garantizar la productividad de los usuarios con ZTNA

Tanto si accede a SAP en la nube pública, a SSH, a RDP, a una intranet personalizada o a una aplicación de plantilla de control horario basada en la web, la experiencia de usuario siempre debe ser fluida. Por eso Gartner recomienda a las organizaciones adoptar tecnologías de **acceso a la red de confianza cero (ZTNA)** en sustitución de las VPN de acceso remoto.

En la mayoría de los casos, los servicios de ZTNA están alojados en la nube y utilizan políticas para determinar qué usuarios autorizados tienen acceso a una aplicación privada específica. Estas políticas tienen en cuenta, entre otros criterios, la identidad del usuario, su grupo y la postura del dispositivo.

Dado que muchos servicios de ZTNA se ofrecen íntegramente en la nube, permiten que los usuarios se conecten a uno de los muchos puntos de presencia globales del servicio, que luego redirige la conexión segura a una aplicación privada. Esto proporciona una mayor disponibilidad y una escala mucho mayor que un dispositivo VPN. Los usuarios nunca están realmente en la red, por lo que el tráfico ya no retorna a un centro de datos. Esto significa que el servicio de ZTNA facilita el acceso del usuario final y, al mismo tiempo, le permite a usted minimizar el riesgo para su empresa.

Arquitectura de acceso a la red de confianza cero (ZTNA)



1 Acceso a aplicaciones o el navegador de Zscaler

- Redirige el tráfico al proveedor de IDP para la autenticación
- Client Connector dirige automáticamente el tráfico al Public Service Edge
- El acceso por navegador elimina la necesidad de tener un cliente en el dispositivo para acceder a las aplicaciones basadas en la web

2 ZPA Public Service Edge

- Protege la conexión de usuario a aplicación
- Aplica todas las políticas de administración personalizadas

3 Conector de la app

- Se ajusta a aplicaciones privadas en la nube y/o centro de datos
- Solo responde a solicitudes de ZPA Public Service Edge
- No hay conexiones de entrada. Responde únicamente con conexiones de adentro hacia afuera.



Comience a ofrecer la experiencia que los usuarios desean

Si desea proporcionar a sus usuarios las herramientas para que sean productivos, considere un servicio de ZTNA.

No se olvide de ver el siguiente vídeo en el que se muestra cómo Steve Day, EGM de infraestructura, nube y lugar de trabajo en el Banco Nacional de Australia, permitió a sus usuarios ser productivos.

Vea la historia del Banco Nacional de Australia

¿Y ahora qué? Pruebe nuestro servicio ZTNA.

Inicie una demostración de ZTNA de 7 días

Acerca de Zscaler

Zscaler permite a las organizaciones líderes del mundo transformar de forma segura sus redes y aplicaciones para un mundo móvil y centrado en la nube. Sus servicios insignia, Zscaler Internet Access ™ y Zscaler Private Access ™, crean conexiones rápidas y seguras entre usuarios y aplicaciones, independientemente del dispositivo, la ubicación o la red. Los servicios de Zscaler se entregan al 100 % a través de la nube y ofrecen la simplicidad, la seguridad reforzada y la experiencia de usuario mejorada que los dispositivos tradicionales o las soluciones híbridas no pueden igualar. Utilizado en más de 185 países, Zscaler opera una plataforma de seguridad en la nube distribuida multiusuario que protege a miles de clientes de ataques cibernéticos y pérdida de datos. Obtenga más información en **zscaler.com** o síganos en Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com