



# Por qué los directores de TI deberían tener en cuenta el Zero Trust Network Access



SECURE ACCESS TO THE MODERN CLOUD ERA

## Una solución para un entorno de TI cambiante

Aunque hace mucho que se considera que la tecnología es un motor necesario para que siga evolucionando la empresa, ahora es reconocida como verdadero impulsor de negocio, capaz de crear nuevas eficiencias, capacidades y oportunidades que antes no estaban al alcance de la mayoría de las empresas. El papel del director de TI ha evolucionado de una manera similar. Así, los CISOs, CIOs y CTOs ya forman parte de la cúpula directiva gracias al nuevo enfoque estratégico de la tecnología.

Los principales factores de este cambio han sido la explosión de la adopción de la nube pública empresarial, incluyendo Azure y AWS, y el amplio uso de dispositivos móviles pertenecientes a empleados para trabajar (BYOD). Las empresas están aprovechando dichas tecnologías para optimizar los procesos empresariales y ofrecer productos y servicios más rápidamente y a menor coste global. ¿Pero, qué riesgo entrañan?

Debido al auge de la nube y de la movilidad, el perímetro de seguridad tradicional que antes protegía a los usuarios y los servicios internos dentro de la red corporativa, en gran medida ya no existe.

Ha llegado el momento de que la seguridad evolucione, trasladando las protecciones más cerca del usuario y poniendo un nuevo énfasis en la comodidad, flexibilidad y fiabilidad.

**“De aquí a 2023, un 60% de las empresas habrá quitado la mayoría de sus Redes Privadas Virtuales (VPNs) en favor del Zero Trust Network Access (ZTNA).”<sup>1</sup>**

– Gartner

<sup>1</sup> Riley, Steve, Macdonald, Neil and Orans, Lawrence: “Market Guide for Zero Trust Network Access”, Gartner, Abril 2019.

## Retos que los directores de TI tienen que superar

Para promover las iniciativas empresariales y cubrir la diferencia entre las necesidades empresariales y las capacidades de las TI, los directores de TI tienen que elegir una tecnología que les permita:

- 1. Resolver la falta de experiencia en TI**, permitiendo a las empresas sacar el mayor partido al talento del que disponen
- 2. Ofrecer una experiencia de usuario superior** para los empleados y los "stakeholders" clave de la empresa
- 3. Adaptarse y ser ágil** para fortalecer un negocio que cambia dinámicamente
- 4. Reducir los riesgos** que puedan amenazar la productividad, la propiedad intelectual y la reputación de la empresa
- 5. Acelerar la adopción** de tecnologías nuevas y habilitantes

Identificar las tecnologías que alcanzarán dichos objetivos es una difícil tarea ya que los objetivos pueden parecer contradictorios. La decisión de adoptar los servicios cloud y las tecnologías móviles, por ejemplo, cumple el objetivo de una experiencia de usuario simplificada, pero ¿qué pasa con el objetivo de minimizar la posibilidad de un ataque de seguridad? Los directores de TI tienen que encontrar un equilibrio cuidadoso entre acelerar la adopción de tecnologías nuevas y habilitantes, y asegurar la seguridad de datos sensibles. Elegir la tecnología adecuada en el momento justo es crucial.

**“Los directores de seguridad deberían desplegar una tecnología que facilite el acceso digital empresarial a aplicaciones protegiéndolas a la vez contra muchos tipos de ataques predominantes que son comunes en el pozo negro que es la internet moderna.”<sup>1</sup>**

– Gartner

<sup>1</sup> Riley, Steve; MacDonald, Neil; and Young, Greg, "It's Time to Isolate Your Services From the Internet Cesspool," Gartner, Septiembre 2016.

## El Zero Trust Network Access permite el éxito de la empresa

El ZTNA (Zero Trust Network Access), también conocido sobre la denominación SDP (Software-Defined Perimeter), crea una identidad y una política de acceso inteligente para una aplicación o un grupo de aplicaciones. Siguen escondidas, y el acceso es restringido vía un trust bróker para un conjunto de entidades determinadas. El bróker verifica la identidad, el contexto y la política asociada a un grupo de usuarios específicos antes de autorizar el acceso. La visibilidad de las aplicaciones así no sigue pública, permitiendo una reducción significativa de la superficie de ataque.

Más arriba hemos comentado los cinco factores clave que los directores de TI tienen que tener en cuenta a la hora de adoptar nuevas tecnologías. Veamos el papel que juega el ZTNA en posibilitar cada uno de ellos.

- 1. Resuelve la falta de experiencia en TI** – Una de las dificultades con la innovación es que a menudo existe una falta de expertos disponibles para ayudar a entenderla e implementarla. La sencillez del ZTNA—todo software, sin hardware—hace que sean fáciles de implementar sin la necesidad de emplear a nuevos especialistas. Esta sencillez permite a los directores de TI adoptar la tecnología que permite un acceso seguro a aplicaciones que se trasladan a la nube, incluso desde dispositivos móviles no gestionados, maximizando a la vez la productividad del personal de TI.
- 2. Ofrece una experiencia de usuario superior** – Los usuarios están teniendo un papel cada vez mayor a la hora de elegir la tecnología empresarial. Ofrecer una experiencia de usuario positiva es uno de los beneficios más importantes del ZTNA. Permite a los usuarios acceder a aplicaciones de forma transparente, sin que importe que la aplicación esté ejecutándose en una nube o en un centro de datos. Una experiencia de usuario parecida a la de la nube se ha convertido en el nuevo estándar, y el ZTNA la proporciona.
- 3. Ofrece agilidad y escala** – El número de aplicaciones empresariales, usuarios y dispositivos de usuarios no para de cambiar constantemente, junto con las necesidades de la empresa. Al utilizar internet y la nube para ofrecer a los usuarios acceso a las aplicaciones, los ZTNAs ofrecen un nivel de agilidad y escala que ninguna tecnología tradicional iguala. Solo imagine lo difícil que sería escalar el número de las pilas de hardware en múltiples centros de datos en todo el mundo. Ahora, compárelo con la escala de internet. Internet gana de lejos.

**4. Reduce los riesgos** – La seguridad es a menudo una de las mayores barreras para la adopción de la nube y del uso de dispositivos móviles personales, ya que dichas tecnologías pueden significar mayores riesgos para la empresa. Los ZTNAs ofrecen un acceso remoto seguro a aplicaciones basado en políticas y comprueban tanto la actitud como la identidad del dispositivo antes de permitir el acceso. Solo los usuarios autorizados pueden acceder a una aplicación. Con el SDP, los directores de TI pueden asegurar que incluso cuando las aplicaciones se trasladen a plataformas IaaS de terceros, sigan siendo seguras. Además, los usuarios podrían utilizar su propio dispositivo sin que éste sirva de conducto para una actividad maligna o sea responsable de la propagación de malware en la red corporativa. Al fin y al cabo, con los ZTNAs, los usuarios nunca se colocan en la red.

**5. Acelera la adopción de la nube y de la movilidad** – Hoy en día, la nube y la movilidad son prioridades para los equipos de la empresa, pero su implementación segura y para una base de usuarios globales puede tardar meses o incluso años. Esto se debe parcialmente a la complejidad que supone el uso de una red y tecnologías de seguridad tradicionales para proporcionar acceso a aplicaciones en la nube desde dispositivos de usuarios no gestionados. Los ZTNAs emplean software para reducir la complejidad, por lo tanto, reduce el tiempo de implementación de meses o años a tan solo unas horas. Con el ZTNA, las organizaciones pueden conseguir más rápidamente los beneficios de la nube y de la movilidad.

**“Con el SDP, las organizaciones pueden mantener los recursos cloud completamente ocultos a los usuarios no autorizados. Esto elimina totalmente muchos vectores de ataque incluyendo los ataques de fuerza bruta; los ataques de inundación de red, así como las vulnerabilidades TLS como Heartbleed y Poodle.”<sup>2</sup>**

– The SDP Working Group, Cloud Security Alliance

<sup>2</sup> Software Defined Perimeter for Infrastructure as a Service, The SDP Working Group, Cloud Security Alliance, 2017.

Infórmese  
sobre ZTNA,  
ofrecido como  
un servicio por  
Zscaler

El Zero Trust Network Access es una herramienta valiosa para los directores de TI empresariales. En Zscaler hemos desarrollado un servicio de ZTNA denominado **Zscaler Private Access (ZPA™)**. El servicio utiliza la nube para ofrecer un acceso remoto seguro y transparente a aplicaciones internas.

Para más información sobre ZPA, visite [zscaler.com/products/zscaler-private-access](https://zscaler.com/products/zscaler-private-access) o contacte el departamento comercial en [sales@zscaler.com](mailto:sales@zscaler.com)

