El desafío de la nube: expandirse de forma rápida pero segura

Extienda la protección Zero Trust
a toda su inversión en la nube de AWS



LIBRO ELECTRÓNICO

©2026 Zscaler, Inc. Todos los derechos reservados.

Índice

El reto de la nube: expandirse con rapidez y seguridad 3

La solución moderna e integral de Zscaler, diseñada para la nube 4

ZPA: una solución fluida de acceso Zero Trust a aplicaciones privadas, diseñada para la nube 5

Zero Trust Cloud: una solución superior de seguridad para cargas de trabajo en la nube 6

ZDX: experiencias rápidas y fluidas para los usuarios finales 7

Una solución conjunta fácil de implementar y que se pone en marcha rápidamente 8

¿Está preparado para transformar la seguridad de su nube? 9



©2026 Zscaler, Inc. Todos los derechos reservados.

El desafío de la nube: expandirse de forma rápida pero segura

Los sistemas de control de acceso basados en redes tradicionales, como las VPN, no son ideales para los entornos de nube modernos. Entonces, ¿cuáles son las alternativas?

Más del 94–96 %[1] de las empresas globales han adoptado servicios en la nube, y la cuota de mercado de AWS representa actualmente el 30 %[2] del mercado global de infraestructura en la nube. Los beneficios de la adopción de la nube son innegables, desde el ahorro de costes hasta la escalabilidad ágil. Las empresas que operan en la nube se enfrentan a dos nuevos desafíos: gestionar el acceso y las operaciones en medio del creciente cambio hacia estructuras de trabajo remotas e híbridas, y la amenaza cada vez más sofisticada que representan el malware y el ransomware.

Tradicionalmente, implementar un entorno seguro requería una red privada virtual (VPN) centrada en la red, que sacrificaba la velocidad, la facilidad de uso y la flexibilidad en favor del control. Hoy en día, a medida que las empresas migran a la nube y la escala de las operaciones de TI crece, las desventajas de usar una VPN se vuelven más significativas.

En su esencia, una VPN no está diseñada para proporcionar un acceso a Internet intrínsecamente seguro. Esto obliga a los trabajadores remotos a contar con una conexión a internet estable y medidas de seguridad actualizadas. A medida que las empresas que migran a la nube emplean a usuarios que trabajan desde cualquier lugar, las conexiones entrantes se han expandido, lo que aumenta las oportunidades para los ataques DDoS. Esto, a su vez, aumenta la complejidad de la segmentación del acceso en un contexto de visibilidad reducida sobre quién hace qué en la red. En definitiva, estos obstáculos limitan la escalabilidad, aumentan los costes, dificultan la productividad y perjudican la experiencia de los empleados. En algunos casos, esto también afecta al usuario final: el cliente.

Estas dificultades explican por qué Zscaler, una plataforma líder de Zero Trust Exchange que está revolucionando el sector de las redes y la seguridad, funciona tan bien con AWS. Como socio tecnológico avanzado de AWS, Zscaler proporciona seguridad como servicio basada en un modelo Zero Trust para ayudar a las empresas a lograr una verdadera transformación en la nube, de forma segura y sencilla, ahora y en el futuro.



©2026 Zscaler, Inc. Todos los derechos reservados.

Zscaler en cifras

CADA DÍA, ZSCALER:

Bloquea
más de 9000 millones
de amenazas

Procesa
más de 750 000 millones
de transacciones

Proporciona
más de 250 000
actualizaciones de seguridad únicas

La solución moderna e integral de Zscaler, diseñada para la nube

Un conjunto de productos configurables para simplificar el acceso y reforzar la seguridad, diseñado para la complejidad de la nube híbrida

Tanto si una empresa busca trasladar sus cargas de trabajo a la nube como si simplemente quiere dejar de utilizar una VPN, la conclusión es clara: combinar Zscaler y AWS ofrece una seguridad de primer nivel y una excelente experiencia de usuario mediante tecnología de vanguardia y un modelo Zero Trust.

Los servicios de seguridad centrados en aplicaciones de Zscaler están construidos en la nube desde el principio y sustituyen las tradicionales puertas de enlace de entrada/salida por un enfoque más moderno (ideal para las empresas que funcionan con AWS). Son tres los servicios centrales que ayudan a los clientes de AWS a aprovechar al máximo sus operaciones en la nube:

Zscaler Private Access (ZPA) hace que la VPN quede obsoleta al conectar a los usuarios a las aplicaciones (no a las redes) eliminando las aplicaciones de Internet para conseguir un entorno más seguro y reducir la complejidad del backend (gestión más sencilla de las herramientas y operaciones entre bastidores con las que los usuarios no interactúan).

Zscaler Zero Trust Cloud (ZTC) centraliza y estandariza la gestión de la seguridad de las cargas de trabajo en todas las nubes mediante un marco único y coherente, lo que permite la segmentación basada en la identidad, la aplicación coherente de políticas y la visibilidad unificada en entornos híbridos y multinube.

Zscaler Digital Experience Monitoring (ZDX) es una plataforma de supervisión multiinquilino basada en la nube que realiza sondeos, establece referencias y mide las experiencias digitales de cada usuario de una organización.

Juntos, Zscaler y AWS ayudan a las organizaciones a acercarse al futuro con:

- Acceso permanente que mejora la experiencia del usuario final
- Un enrutamiento más eficiente que reduce la latencia y se traduce en una puesta en producción más rápida
- Postura de seguridad más sólida y completa para eliminar amenazas
- Migración de aplicaciones más rápida para lograr un tiempo de inactividad mínimo
- Mayor agilidad empresarial para disfrutar de una ventaja competitiva
- Una reducción de costes que libera fondos para destinarlos a otras áreas de la empresa

Aunque estas herramientas ayudan a cualquier empresa a estar preparada para el futuro, demuestran un valor especial en los casos de uso de alto riesgo. Por ejemplo, Zscaler elimina muchos de los problemas técnicos a los que se enfrentan los equipos de TI durante las fusiones y adquisiciones. Proporcionando un proceso de integración mucho menos complejo a la vez que aplica las mejores prácticas de seguridad, Zscaler ha ayudado a las empresas a reducir su proceso de configuración técnica de meses a semanas. Las empresas fusionadas pueden conectar a los empleados directamente a las aplicaciones sin las dificultades ni las demoras que supone crear o trasladar redes.

©2026 Zscaler, Inc. Todos los derechos reservados.

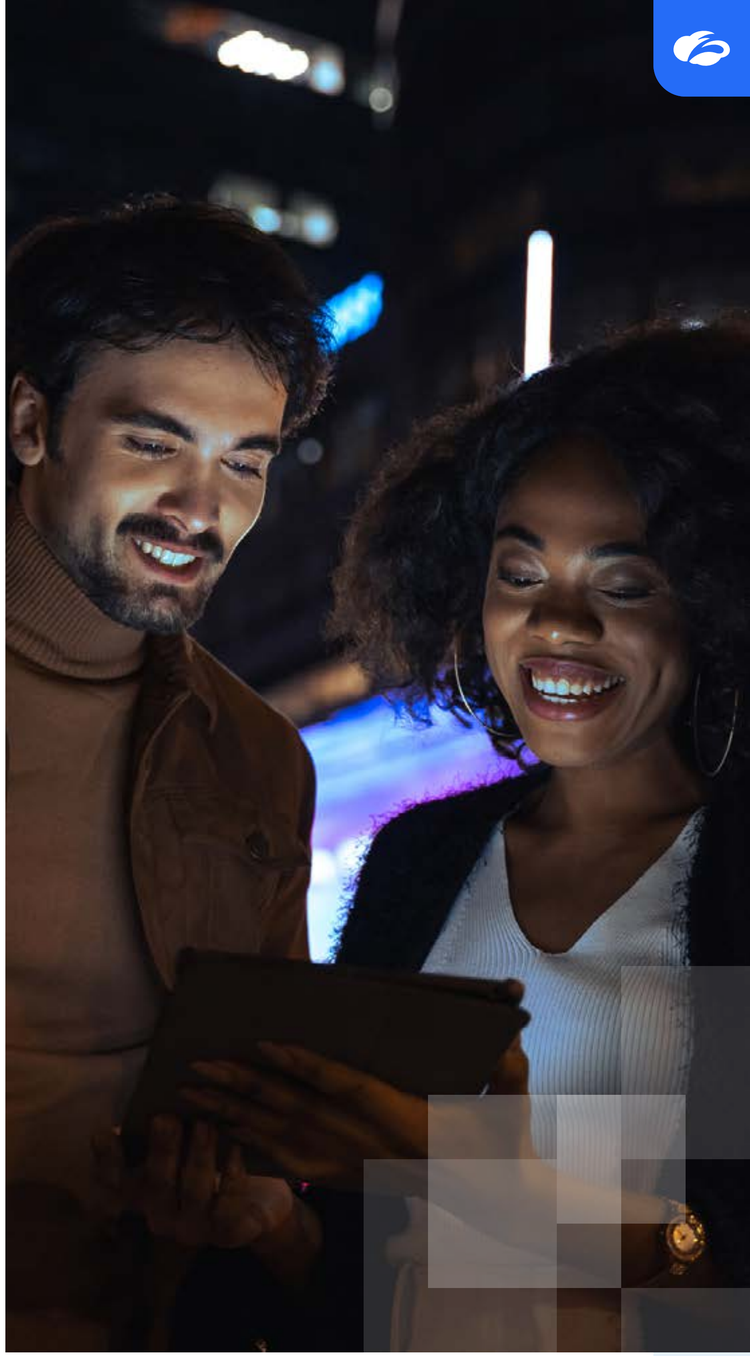
ZPA: una solución fluida de acceso Zero Trust a aplicaciones privadas, diseñada para la nube

Sustituya las engorrosas VPN por un acceso sin fricciones que mantenga las aplicaciones privadas aisladas de Internet y que sea invisible para los actores de las amenazas externos

Si bien en su momento fueron la mejor opción para el acceso privado, las VPN han demostrado ser menos efectivas en un mundo basado en la nube, ya que básicamente enrutan al usuario a una red solo para enviarlo de vuelta fuera. Al atravesar el mundo para pasar por varios puntos de contacto, desde cortafuegos hasta equilibradores de carga, conectarse a las aplicaciones les supone aún más pasos a los trabajadores remotos. Además, las VPN requieren que los usuarios sepan qué perfil deben utilizar y qué recursos les permitirán conectarse a la red, lo que no ofrece una experiencia de usuario ideal, especialmente para los empleados con menos conocimientos técnicos.

Mantenga sus oficinas satélite en órbita.
ZPA proporciona acceso remoto seguro a las aplicaciones sin una VPN, completamente al margen de la red y sin depender de dispositivos físicos o virtuales centrados en IP. Gestiona el acceso de los usuarios autorizados antes, durante y después de la migración de las aplicaciones a AWS mediante una vía mucho más eficiente y segura: una solución de perímetro definido por software (SDP) basada en Zero Trust que aprovecha una conexión de dentro hacia fuera establecida desde un AWS App Connector en la nube de seguridad global de Zscaler. Además, complementa los grupos de seguridad de AWS y AWS Direct Connect. Independientemente de dónde se encuentre el usuario que intenta conectarse a las aplicaciones internas, ZPA permite migrar las aplicaciones con mayor rapidez, reducir los costes y disminuir la exposición a las amenazas, incluso en empresas que siguen dependiendo de un centro de datos privado.

ZPA Northstar: cómo GROWMARK mantiene la producción de alimentos.
GROWMARK, una empresa agrícola norteamericana que proporciona diversos materiales y servicios para favorecer el crecimiento de los cultivos, cuenta con empleados en más de 500 ubicaciones rurales, por lo que conoce bien los retos de las conexiones a internet poco fiables. Con la llegada de la pandemia de COVID-19 y su impacto en la cadena de suministro, era más importante que nunca que las operaciones se desarrollaran sin problemas. Como parte de su modernización, GROWMARK trasladó cientos de aplicaciones a AWS, aunque mantuvo otras en sus propias instalaciones, y necesitaba una solución compatible con su estructura híbrida. Tras elegir ZPA, GROWMARK pudo ofrecer a sus empleados una conexión más fiable y eliminar las interfaces públicas de su entorno privado, reduciendo así su superficie de ataque. En el momento álgido de la pandemia, el 98 % de la plantilla de GROWMARK se conectaba a ZPA prácticamente sin problemas.



©2026 Zscaler, Inc. Todos los derechos reservados.



Una solución unificada para una seguridad sólida y escalable en la nube

Zero Trust Cloud: una solución superior de seguridad para cargas de trabajo en la nube

Transforme la seguridad de su carga de trabajo de cortafuegos a zero trust

Las empresas que operan en entornos híbridos y multinube están descubriendo que los modelos de seguridad tradicionales centrados en la red no son eficaces para proteger las cargas de trabajo modernas. A medida que las aplicaciones y los servicios se mueven entre centros de datos, nubes privadas y entornos de nube pública, los controles tradicionales que antes ayudaban a segmentar y proteger el tráfico se vuelven más difíciles de gestionar y escalar. Las reglas estáticas basadas en IP, los modelos de políticas inconsistentes y las herramientas de seguridad desconectadas generan complejidad, reducen la visibilidad y aumentan el riesgo de movimientos laterales. A esto se suma la carga de garantizar la seguridad del tráfico este-oeste, de entrada y de salida de forma consistente, lo que dificulta que los equipos de TI y seguridad puedan mantenerse al día.

En la nube, no hay margen de error.
Zscaler Zero Trust Cloud aplica principios Zero Trust para que las cargas de trabajo de AWS nunca se consideren de confianza implícita en función de su ubicación en la red. Esto ya sitúa a las empresas a la vanguardia, ya que las organizaciones buscan cada vez más modernizar la seguridad de las aplicaciones e infraestructuras distribuidas. Con ZTC, las empresas pueden centralizar y estandarizar la gestión de la seguridad de las cargas de trabajo en entornos híbridos y multinube, lo que proporciona visibilidad unificada y una aplicación coherente de las políticas para las cargas de trabajo, independientemente de dónde se ejecuten.

ZTC Northstar: cómo FICO protege las cargas de trabajo de producción en la nube.
La empresa de software de análisis FICO está avanzando en su transformación a la nube sin dejar de dar soporte a las aplicaciones que aún residen en centros de datos. A medida que más cargas de trabajo de producción se trasladan a AWS, la empresa necesitaba una forma consistente de extender los controles de seguridad a través de entornos de nube sin depender de enfoques fragmentados. Para respaldar este cambio, FICO adoptó Zscaler Cloud Connectors para conectar de forma segura las cuentas de AWS con los servicios de Zscaler, extendiendo las mismas protecciones utilizadas para los usuarios y el acceso a aplicaciones privadas a las cargas de trabajo en la nube. Con las cargas de trabajo segmentadas por zona y cuenta de AWS, FICO ahora avanza hacia una segmentación más granular a medida que expande su presencia en la nube y fortalece el control sobre la gestión de la seguridad de las cargas de trabajo.

©2026 Zscaler, Inc. Todos los derechos reservados.

ZDX: experiencias rápidas y fluidas para los usuarios finales

Obtenga información estratégica profunda y procesable sobre su experiencia de usuario basada en una vista unificada de métricas de rendimiento de aplicaciones, puntos finales y CloudPath

Como consumidores, nos hemos acostumbrado a una experiencia de usuario de primer nivel, hasta el punto de que una interrupción temporal de las redes sociales aparece en los titulares. Mientras las empresas empezaban a dominar la experiencia de usuario con la tecnología de oficina, los cuellos de botella se han vuelto más habituales a medida que los equipos remotos e híbridos se enfrentan a obstáculos como conexiones a internet deficientes y una variedad de dispositivos móviles personales, a veces obsoletos. Cuando esto se traduce en tiempos de espera agotados y reconexiones constantes, las incidencias de soporte se acumulan y el trabajo queda sin hacer, lo que somete a los equipos de TI a una enorme presión para determinar la causa y la solución de problemas específicos.

Ofrezca una experiencia sin frustraciones a todos los usuarios finales.
ZDX es una plataforma de supervisión multiinquilino basada en la nube que realiza sondeos, establece referencias y mide las experiencias digitales de cada usuario de su organización, esté donde esté. En tiempo real, ZDX determina la causa del problema, por ejemplo, si se debe a la conexión a internet o al proveedor de servicios de internet, y después utiliza sus funciones de resolución remota de problemas. Sus funciones de análisis miden el rendimiento a lo largo del tiempo por ubicación, usuario y departamento para identificar tendencias y orientar las mejoras. ¿El resultado? Una auténtica arquitectura de perímetro de servicio de acceso seguro (SASE) que se traduce en una experiencia de usuario superior y muchas menos incidencias de TI.

ZDX Northstar: cómo Liberty Mutual mejoró la experiencia de los empleados.
Liberty Mutual Insurance podía garantizar el funcionamiento de sus centros de datos y el ancho de banda de su proveedor de servicios de internet, pero no la calidad de la conexión a internet de los empleados que trabajaban desde casa, algo que todo el mundo experimentó de forma generalizada en 2020. El equipo de seguridad de Liberty comenzó con 100 usuarios para demostrar la viabilidad de la solución y, como primer caso de uso, empezó a implementar ZDX entre los usuarios con problemas persistentes. Esto permitió derivar las incidencias al equipo de soporte de nivel 2, que podía resolver fácilmente los problemas de los usuarios con sus redes domésticas. Desde entonces, han integrado ZDX en toda la organización, identificando y eliminando problemas de latencia de los proveedores de servicios, problemas con los routers inalámbricos, fugas de memoria en los ordenadores de sobremesa y problemas de los proveedores de servicios de internet relacionados con el tiempo de carga de las páginas, entre otros.



©2026 Zscaler, Inc. Todos los derechos reservados.

Una solución conjunta fácil de implementar y que se pone en marcha rápidamente

Con un proceso de implementación diseñado para ser rápido y Zscaler Client Connector gestionando el acceso, sus equipos pueden estar operativos en cuestión de minutos

Migrar a una nueva plataforma e infraestructura de TI puede ser complejo y prolongado. Para abordar esta cuestión, Zscaler diseñó el proceso de adopción en torno a la velocidad y la simplicidad, facilitando las operaciones seguras basadas en la nube y las transiciones fluidas con Zscaler y AWS.

Aunque **ZPA, ZIA** y **ZDX** pueden funcionar de forma independiente, ofrecen los mejores resultados cuando se utilizan juntos para desarrollar el acceso a las aplicaciones sobre la base de un marco bien diseñado. En el centro de sus procesos se encuentra Zscaler Client Connector (ZCC).

ZPA utiliza Client Connector para conectar a los usuarios con aplicaciones privadas mediante un enfoque Zero Trust, aunque Browser Access también está disponible para aplicaciones privadas exclusivamente web.

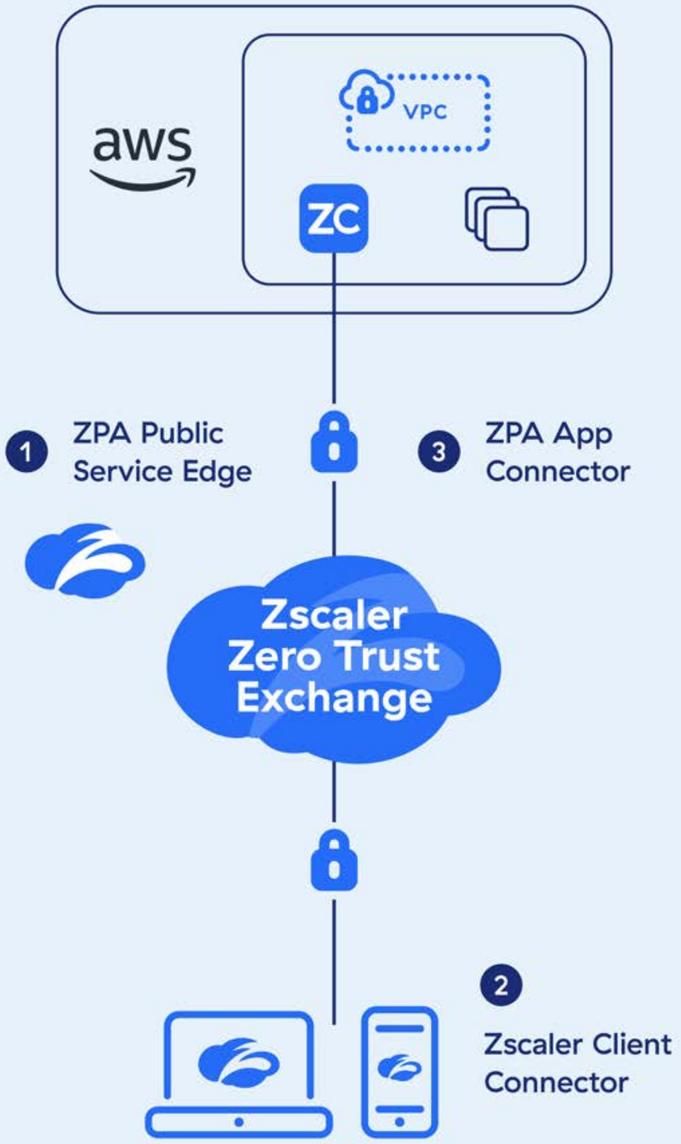
ZIA utiliza Client Connector para proteger a los usuarios fuera de la red corporativa, reenviando el tráfico de internet a través del servicio de Zscaler para garantizar una política de seguridad granular.

ZDX utiliza Client Connector para realizar sondeos sintéticos de la aplicación de software como servicio (SaaS) o del servicio de internet deseado, como Salesforce o Zoom.

Los clientes de Zscaler están dejando atrás sus VPN de forma rápida y segura... para siempre. Veamos cómo.

- **ZPA Public Service Edge** aloja el motor de políticas y actúa como intermediario de las conexiones
- **Zscaler Client Connector** es un agente de punto de conexión que reenvía el tráfico a la nube de Zscaler
- **ZPA App Connector** se conecta a aplicaciones privadas y descubre nuevas aplicaciones. Diga adiós a las VPN. Nuestros clientes están dejando de usar VPN definitivamente gracias a la instalación rápida y sencilla de Zscaler.
- El equipo de TI instala los conectores de aplicaciones en AWS, donde residen las aplicaciones, para que Zscaler pueda llegar a las aplicaciones a las que los usuarios necesitarán acceder.
- En el portal de ZPA, los usuarios definen aplicaciones y conectores y los asignan a grupos de servidores
- Una vez instalado, Client Connector puede servir para múltiples propósitos: decidir a dónde se dirigen las solicitudes, dónde deben ir y dónde conectar a los usuarios.

Más información sobre la configuración de Client Connector.



©2026 Zscaler, Inc. Todos los derechos reservados.



¿Listo para transformar su seguridad en la nube?

Zscaler y AWS han allanado el camino hacia la última frontera en el acceso de los usuarios, y hay sitio de sobra a bordo.

aws marketplace

Encuentre soluciones de Zscaler en AWS Marketplace para simplificar la facturación y la implementación directamente en AWS.

Pruebe una demo alojada de ZPA gratuita durante 7 días

Con solo unos clics, Zscaler preparará un informe con una evaluación exhaustiva de su postura de seguridad en la nube, que le mostrará dónde se encuentran sus vulnerabilidades en internet.

Inicie su análisis de exposición a amenazas de internet.

©2026 Zscaler, Inc. Todos los derechos reservados.

Actúe con rapidez. Manténgase seguro.

©2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

Disponible en AWS Marketplace

Acerca de Zscaler

Zscaler (NASDAQ: ZS) es pionera y líder mundial en seguridad Zero Trust. Las mayores empresas del mundo, organizaciones de infraestructuras críticas y organismos gubernamentales confían en Zscaler para proteger usuarios, sucursales, aplicaciones, datos y dispositivos, y para acelerar sus iniciativas de transformación digital. Distribuida en más de 160 centros de datos en todo el mundo, la plataforma Zscaler Zero Trust Exchange™, combinada con IA avanzada, combate cada día miles de millones de ciberamenazas e infracciones de políticas y ayuda a las empresas modernas a aumentar la productividad reduciendo los costes y la complejidad.

© 2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**