# AWS y Zscaler: una solución unificada para una seguridad en la nube sólida que escala

aws

zscaler™

# Índice



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

*Las VPN y otras prácticas de seguridad basadas en el perímetro no pueden seguir el ritmo de los desafíos modernos de la nube. Así que, ¿cuáles son las opciones?*

En 2020, más de la mitad de las empresas migraron sus cargas de trabajo a la nube y el 76 % de ellas eligieron Amazon Web Services (AWS). 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 retos: la gestión del acceso y las operaciones en medio del creciente cambio a estructuras de trabajo remotas e híbridas, así como al malware y el ransomware, amenazas cada vez más sofisticadas.

Históricamente, implementar un entorno seguro requería una VPN centrada en la red, que sacrificaba la velocidad, la facilidad de uso y la flexibilidad para el control. Hoy en día, a medida que las empresas migran a la nube y el volumen de las operaciones de TI aumenta, las desventajas de usar una VPN superan a los beneficios.

En su base, la VPN no está diseñada para proporcionar un acceso a Internet intrínsecamente seguro y hace que el peso de tener una conexión a Internet sólida y medidas de seguridad actualizadas recaiga en el personal. A medida que las empresas que se trasladan a la nube contratan a usuarios que trabajan desde cualquier lugar, las conexiones entrantes han aumentado, lo que amplía la oportunidad de ataques DDoS. Esto, a su vez, aumenta la complejidad de la segmentación del acceso cuando ya hay un problema: una visibilidad reducida de quién está haciendo qué en la red. En última instancia, estos obstáculos limitan la escalabilidad, aumentan los costes, perjudican la productividad y merman la calidad de la experiencia de los empleados. En algunos casos, también afectan al usuario final: el cliente.

Estos obstáculos son el motivo por el que Zscaler, un intercambio de confianza cero líder que ha revolucionado el sector de la red y la seguridad, funciona tan bien con AWS. Como socio tecnológico avanzado de AWS, Zscaler proporciona seguridad como servicio basada en un modelo de confianza cero para ayudar a las empresas a lograr una verdadera transformación en la nube, de forma segura y simple, ahora y en el futuro.

# La solución moderna, integral y que prioriza la nube de Zscaler

*Un paquete de productos configurables para simplificar el acceso y fortalecer la seguridad, diseñados para la complejidad de la nube múltiple*

Tanto si una empresa quiere trasladar las cargas de trabajo a la nube o simplemente dejar atrás la VPN, la solución está en el emparejamiento de Zscaler y AWS, que ofrece una seguridad de primer nivel y una gran experiencia de usuario a través de tecnología de vanguardia y un modelo de confianza cero.

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 Internet Access** (ZIA) es una pila de seguridad completa entregada en la nube que mitiga el coste y la complejidad de los enfoques tradicionales de puerta de enlace web segura.

**Zscaler Digital Experience Monitoring** (ZDX) es una plataforma de supervisión multiusuario basada en la nube que sondea, compara y mide las experiencias digitales de cada usuario dentro de una organización.

Juntos, Zscaler y AWS ayudan a las organizaciones a acceder a las puertas del futuro con:

- Acceso permanente que mejora la experiencia del usuario final
- Enrutamiento más eficiente que reduce la latencia y se traduce en un tiempo de producción más rápido
- 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
- Disminución de los costes para liberar fondos que estarían mejor destinados en 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 gran parte de los quebraderos de cabeza 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 la preocupación o la demora de crear o trasladar redes.

## Zscaler en cifras

Cada día, Zscaler:

Bloquea
**7000 millones**
de amenazas

Procesa
**más de 200 000 millones**
de solicitudes

Proporciona
**más de 200 000**
actualizaciones de seguridad únicas

# ZPA: una solución de acceso de confianza cero sin fisuras y que prioriza la nube para aplicaciones privadas

*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*

En su día, las VPN fueron la mejor opción para el acceso privado, pero ahora se han vuelto engorrosas y vulnerables en un mundo basado en la nube, ya que básicamente enrutan a un usuario a una red solo para volverlo a sacar de ella. 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, la VPN requiere que los usuarios entiendan qué perfil deben utilizar y qué recursos les permitirán acceder a la red, algo que no es la mejor experiencia para el usuario, especialmente para los empleados menos expertos en tecnología.

## Mantenga sus oficinas satélite en órbita

ZPA proporciona acceso remoto seguro a las aplicaciones sin una VPN, sin tener que acceder a la red y sin depender de dispositivos físicos o virtuales centrados en la IP. Gestiona el acceso de los usuarios autorizados antes, durante y después de la migración de aplicaciones a AWS utilizando una vía mucho más eficiente y segura: una solución de perímetro definido por software (SDP) de confianza cero que aprovecha una conexión interna establecida desde un conector de aplicaciones de AWS en la nube de seguridad global de Zscaler. Además, es gratuito para los grupos de seguridad nativos de AWS, así como de AWS Direct Connect. Independientemente de dónde intente conectarse un usuario a aplicaciones internas, ZPA se traduce en migración de aplicaciones más rápida, costes reducidos y en dejar de ser objetivo de amenazas (incluso para las empresas que siguen confiando en un centro de datos privado). Todo esto es perfecto para asociar escalabilidad con agilidad.

## ZPA Northstar: cómo GROWMARK hace que no pare la producción de alimentos

GROWMARK, una empresa agrícola norteamericana que ofrece diversos materiales y servicios para apoyar el crecimiento de los cultivos, cuenta con empleados de más de 500 ubicaciones rurales, por lo que la empresa está familiarizada con los desafíos de la baja fiabilidad de Internet Cuando llegó la pandemia de la COVID-19 y la cadena de suministro se vio afectada, era más importante que nunca que las operaciones se desarrollaran sin problemas. En sus esfuerzos por modernizarse, GROWMARK trasladó cientos de aplicaciones a AWS, pero también alojó algunas en sus instalaciones, y necesitaba una solución que pudiera funcionar con su estructura híbrida. Después de seleccionar a ZPA, GROWMARK pudo proporcionar a los empleados una conexión más fiable y, al mismo tiempo, eliminar las interfaces públicas de su entorno privado, lo que, en última instancia, redujo su superficie de ataque. En el momento álgido de la pandemia, el 98 % de la plantilla de GROWMARK se conectaba a ZPA sin apenas problemas.

# ZIA: una pila fiable de seguridad en la nube como servicio

*Reduzca el riesgo y los costes de red al pasar de la seguridad perimetral obsoleta a la protección en la nube de confianza cero*

Las empresas que operan en centros de datos y modelos de seguridad basados en el perímetro están descubriendo que la transición a la nube conlleva cambiar a enfoques de pasarela web más seguros.

Pasar de un centro de datos a la nube hace que las aplicaciones estén en "un nuevo hogar"; las puertas de enlace centralizadas que simplificaban el acceso y reducían los costes en el pasado ya no abordan las nuevas vulnerabilidades resultantes del tráfico de los usuarios que van directamente a la nube. Esto hace que el marco del perímetro de seguridad heredado sea un lastre. Si a todo esto le añadimos el ataque que suponen los nuevos dispositivos de seguridad que sobrecargan una puerta de enlace ya saturada, el departamento de TI todavía tiene más dificultades para mantenerse al día.

## En el espacio, no hay margen de error

Zscaler y AWS operan con confianza cero para que nunca baje su guardia en territorio desconocido. De acuerdo con Forrester, esto ya sitúa a las empresas a la vanguardia y la confianza cero se está convirtiendo rápidamente en la arquitectura de seguridad más elegida.

Con ZIA, las empresas pueden brindar una conexión más segura a las soluciones de software como servicio (SaaS), proporcionando visibilidad de toda la actividad en Internet de los usuarios de una empresa, a la vez que se mantiene el acceso remoto a las aplicaciones internas en AWS de forma sencilla y segura.

A través de la estructura y los servicios de Zscaler, los usuarios disfrutan de una reducción en la superficie de ataque, mejoran el control de acceso y fortalecen la protección de datos, lo que hace posible la aplicación de políticas granulares a escala.

## ZIA Northstar: cómo MAN Energy Systems adoptó ZIA

La empresa alemana de fabricación y servicios de transporte MAN Energy Systems suministra productos y servicios de alto impacto que mantienen al mundo en funcionamiento, como motores diésel y turbomaquinaria. Para seguir siendo competitiva, la empresa migró cargas de trabajo a AWS, pero el creciente número de equipos distribuidos en todo el mundo de MAN requería cada vez más acceso móvil a aplicaciones y herramientas empresariales personalizadas. Esto suponía un elevado riesgo para la seguridad y frustraba a los empleados debido al largo y complicado proceso de autenticación y acceso que se requería a nivel individual para una larga lista de aplicaciones. Junto con la eliminación de la VPN, la directiva adoptó ZIA para que solo los usuarios de confianza pudieran acceder a aplicaciones de confianza. Así, pudieron conectar siempre de forma segura a sus trabajadores móviles a las aplicaciones SaaS de MAN, desde cualquier ubicación.

# 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 magnífica calidad, hasta el punto de que una interrupción temporal de las redes sociales es noticia. Mientras que las empresas estaban empezando a dominar la experiencia del usuario con la tecnología en la oficina, los cuellos de botella se han vuelto más comunes a medida que los equipos remotos e híbridos se enfrentan a obstáculos como una mala conexión a Internet y diferentes dispositivos móviles personales (a veces anticuados). Cuando esto sucede en forma de tiempos de espera y reconexiones constantes, los tickets de ayuda se acumulan y el trabajo no sale adelante, lo que pone a TI en una situación de gran presión para averiguar la causa (y la resolución) de problemas únicos.

## Permita a todos los usuarios finales viajar hacia un trabajo sin frustraciones

ZDX es una plataforma de supervisión multiusuario basada en la nube que sondea, compara y mide las experiencias digitales de cada uno de los usuarios de su organización, sin importar dónde se encuentren. En tiempo real, ZDX evaluará lo que está causando un problema (por ejemplo, la conexión a Internet frente al proveedor de ISP) y luego implementará sus capacidades de resolución remota de problemas. Los análisis miden el rendimiento a lo largo del tiempo por ubicación, usuario y departamento para identificar tendencias e informar sobre las mejoras. ¿El resultado? Una auténtica arquitectura de perímetro de servidor de acceso seguro (SASE) que se materializa en una experiencia superior para el usuario (y muchos menos tickets de TI).

## ZDX Northstar: cómo Liberty Mutual mejoró la experiencia de sus empleados

Liberty Mutual Insurance podía garantizar sus centros de datos y ancho de banda ISP, pero no el funcionamiento de Internet para los empleados que trabajaban desde casa, algo que todos experimentaron en masa en 2020. Empezando con 100 usuarios para proporcionar una prueba de concepto, el equipo de seguridad de Liberty comenzó a implementar ZDX para los usuarios con problemas a largo plazo como casos de uso iniciales, lo que hizo posible pasar problemas al equipo de soporte técnico de nivel 2, que podía resolver fácilmente los problemas de los usuarios con sus redes domésticas. Ahora que han integrado ZDX en toda la organización, han detectado y eliminado problemas de latencia de los proveedores de servicios, problemas de enrutadores inalámbricos, fugas de memoria en ordenadores de escritorio y problemas de ISP en torno al tiempo de recuperación de páginas, entre otros.

# Una solución conjunta de fácil despliegue y rápidamente operativa

*Con un proceso de implementación diseñado para conseguir velocidad y Zscaler Client Connector que administra el acceso, sus equipos pueden ponerse en marcha en cuestión de minutos*

Pasar a una nueva plataforma e infraestructura de TI puede ser un proceso complejo y prolongado, por lo que Zscaler diseñó el proceso de adopción teniendo en cuenta la velocidad y la simplicidad. Hay todo el tiempo operaciones seguras basadas en la nube y transiciones fluidas para las personas adecuadas, algo fácil de hacer con Zscaler y AWS.

Aunque ZPA, ZIA y ZDX pueden funcionar por separado, lo mejor es utilizarlos conjuntamente para conseguir un marco de trabajo bien diseñado. En el eje de sus procesos está Zscaler Client Connector (ZCC).

ZPA utiliza Client Connector para conectar a los usuarios a aplicaciones privadas mediante un enfoque de confianza cero, pero Browser Access también está disponible para aplicaciones privadas solo por Internet.

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 un sondeo sintético a la aplicación de software como servicio (SaaS) o servicio basado en Internet (por ejemplo, Salesforce, Zoom, etc.) que se desee.

## Despídase de las VPN

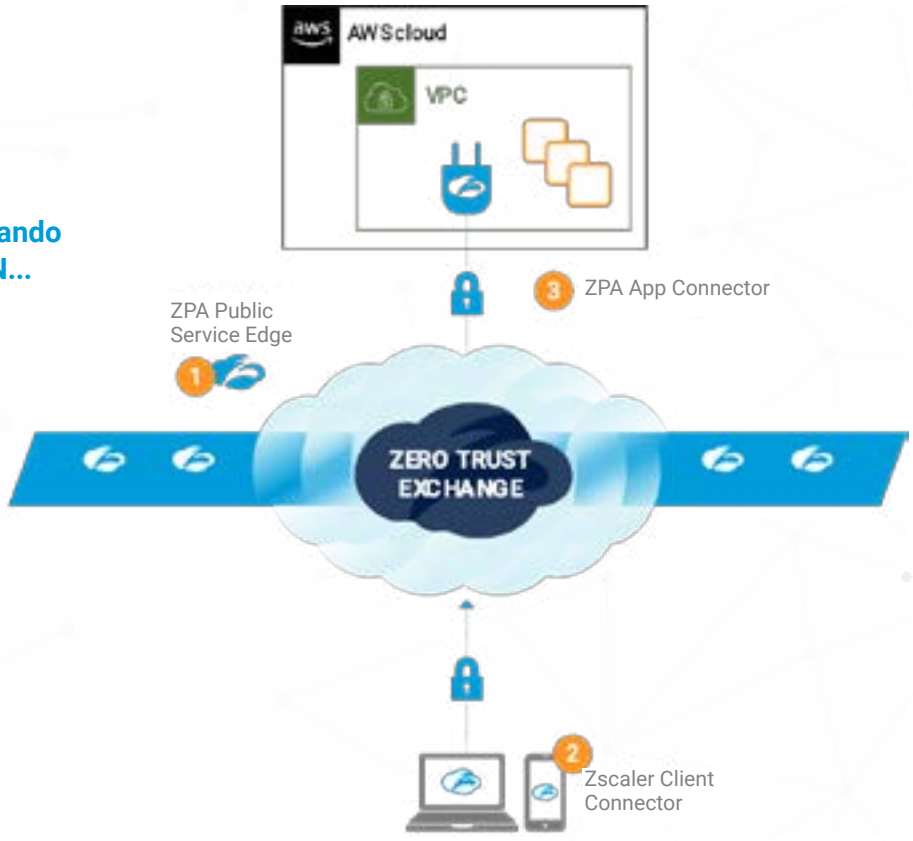
Nuestros clientes están dejando las VPN atrás para siempre con la instalación rápida y sin complicaciones de Zscaler.

1. 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 tendrán que acceder.
2. En el portal ZPA, defina aplicaciones y conectores y asígnelos a grupos de servidores
3. 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.**

## Los clientes de Zscaler se están alejando de forma rápida y segura de sus VPN... para siempre. Veamos cómo.

1. **ZPA Public Service Edge** alberga el motor de políticas e intermedia en las conexiones
2. **Zscaler Client Connector** es un agente de punto final que reenvía el tráfico a la nube de Zscaler
3. **ZPA App Connector** conecta a aplicaciones privadas y descubre nuevas aplicaciones



# ¿Listo para transformar su seguridad en la nube?

Zscaler y AWS han allanado el camino para superar la última frontera en el acceso de los usuarios, y hay mucho que descubrir. Encuentre soluciones de Zscaler en AWS Marketplace.

Pruebe una demostración gratuita de 7 días de ZPA alojada

En tan solo unos clics, Zscaler preparará un informe que proporcionará una evaluación detallada de su postura de seguridad en la nube, que le mostrará dónde se encuentran sus vulnerabilidades en Internet. Comience su análisis de exposición a amenazas de Internet.