FICHA DE DATOS

Zscaler Private Access™

Capacite a su personal híbrido con acceso rápido, seguro y confiable a aplicaciones privadas con el primer ZTNA basado en IA del sector

Zscaler Private Access (ZPA) es una solución nativa de la nube que ofrece acceso zero trust para todos los usuarios con conectividad directa a aplicaciones privadas al tiempo que minimiza la superficie de ataque, elimina el movimiento lateral y protege contra ataques sofisticados.

Los enfoques de seguridad de red tradicionales no satisfacen las necesidades de su personal híbrido y de su empresa.
Los cortafuegos y las VPN tradicionales crean una superficie de ataque masiva que los atacantes pueden encontrar y explotar. También colocan a los usuarios directamente en su red, lo que permite la propagación lateral de amenazas. Si las credenciales de su usuario se ven comprometidas, los atacantes tienen fácil acceso a sus datos confidenciales. El uso de una VPN para habilitar a su personal híbrido y el acceso de terceros aumenta el riesgo cibernético, crea malas experiencias de usuario y agrega gastos administrativos. Para brindar acceso seguro a los usuarios desde cualquier dispositivo y ubicación, necesita un enfoque más eficaz.

En 2025, al menos el 70 % de las nuevas implementaciones de acceso remoto se realizarán predominantemente mediante el acceso a la red de confianza cero (ZTNA) en contraposición a los servicios de VPN, frente a menos del 10 % a finales de 2021, según Gartner.

Ventajas:

- **Reemplace las soluciones VPN vulnerables**
  Reduzca la superficie de ataque y elimine el movimiento lateral conectando a los usuarios directamente a las aplicaciones, no a la red, lo que mejora su postura de seguridad.
- **Prevenga ataques cibernéticos**
  Minimice el riesgo de una infracción con protección de aplicaciones privadas contra amenazas web y de identidad, protección avanzada contra amenazas con inspección en línea completa y prevención de pérdida de datos.
- **Empodere a su personal híbrido**
  Amplíe sin inconvenientes el acceso ultrarrápido a aplicaciones privadas entre usuarios, sede central, sucursales y terceros.
- **Reduzca la complejidad operativa**
  Ofrezca acceso seguro y optimizado, sin productos puntuales costosos y complejos, a través de una plataforma ZTNA unificada y nativa de la nube para usuarios, cargas de trabajo y OT/TI

Los atacantes pueden eludir fácilmente los enfoques de seguridad de red heredados aprovechando la confianza inherente y el acceso excesivamente permisivo de las arquitecturas tradicionales de castillo y foso. Así:

- **La arquitectura heredada no puede escalar ni ofrecer una experiencia de usuario rápida y fluida:** las VPN requieren retorno de los datos, lo que introduce costes, complejidad y demasiada latencia para el personal remoto actual
- **Los cortafuegos, VPN, VDI y aplicaciones privadas tradicionales crean una superficie de ataque masiva:** los atacantes pueden descubrir y explotar recursos vulnerables expuestos externamente
- **El acceso a toda la red permite el libre movimiento lateral:** las VPN colocan a los usuarios en su red, brindando a los atacantes un fácil acceso a datos confidenciales
- **Los usuarios comprometidos y las amenazas internas pueden eludir los controles tradicionales:** los atacantes avanzados pueden robar credenciales y subvertir la identidad para acceder a aplicaciones privadas con herramientas de acceso remoto heredadas

Ha llegado el momento de replantearse cómo conectamos a los usuarios con las aplicaciones que necesitan de forma segura y sin fisuras. Es hora de redefinir la seguridad de las aplicaciones privadas con una nueva generación de acceso a la red de zero trust.

Zscaler Private Access™ (ZPA)

Zscaler Private Access (ZPA), el primer ZTNA impulsado por IA de la industria, es una solución nativa de la nube que ofrece acceso zero trust para todos los usuarios con conectividad directa a aplicaciones privadas al tiempo que minimiza la superficie de ataque al ocultar las aplicaciones detrás de Zero Trust Exchange, eliminando el movimiento lateral mediante la segmentación de usuario a aplicación impulsada por IA y protegiendo contra ataques sofisticados con inspección de tráfico integrada, protección de aplicaciones y datos. Al ser un servicio nativo de la nube construido sobre un marco de servicios de seguridad integral (SSE), ZPA puede desplegarse en cuestión de horas para reemplazar las VPN heredadas y las herramientas de acceso remoto a fin de:

- **Minimizar la superficie de ataque:** las aplicaciones se vuelven invisibles para Internet, lo que evita que usuarios y dispositivos no autorizados las descubran. Las conexiones de dentro hacia afuera entre el usuario y la aplicación garantizan que las aplicaciones y las IP nunca queden expuestas
- **Aplicar el acceso con privilegios mínimos:** el acceso a las aplicaciones se determina por la identidad y el contexto, no por una dirección IP. Los usuarios nunca se conectan a la red para acceder.
- **Eliminar el movimiento lateral:** las aplicaciones están segmentadas para que los usuarios sólo puedan acceder a una aplicación específica, lo que ayuda a limitar el movimiento lateral
- **Detener los ciberataques con una inspección completa:** el tráfico de aplicaciones privadas se inspecciona en línea para evitar las técnicas de ataque web más frecuentes
- **Evitar la pérdida de datos:** DLP integrado para aplicaciones privadas, respuesta avanzada a incidentes y clasificación de datos para proteger las aplicaciones más importantes
- **Ofrecer una experiencia de usuario superior:** conectar a los usuarios directamente a aplicaciones privadas elimina el retorno lento y costoso a través de VPN heredadas y, al mismo tiempo, supervisa y resuelve de manera proactiva los problemas de la experiencia del usuario.

En el año 2025, al menos el 70 % de los nuevos despliegues de acceso remoto serán servidos predominantemente por ZTNA en contraposición a los servicios VPN. A finales de 2021, eran menos del 10 %.*

– Gartner

*Gartner, Tecnologías emergentes: Perspectivas de crecimiento de la adopción del acceso a la red de confianza cero, Nat Smith, Mark Wah, Christian Canales. 8 de abril de 2022

Casos de uso clave

Acceso remoto seguro (reemplazo de VPN)
Las VPN basadas en dispositivos o en la nube le dejan expuesto a ataques cibernéticos. Están plagadas de vulnerabilidades y los atacantes las explotan con regularidad. Su diseño centrado en la red reenvía el tráfico, amplía la superficie de ataque y permite el movimiento lateral al colocar a los usuarios directamente en la red, lo que conduce a ataques de ransomware. Las VPN son inseguras, lentas y complejas de administrar.

ZPA resuelve estos desafíos al brindar acceso zero trust para todos los usuarios con conectividad directa a aplicaciones privadas, al tiempo que minimiza la superficie de ataque ocultando las aplicaciones detrás de Zero Trust Exchange, eliminando el movimiento lateral mediante la segmentación de usuario a aplicación impulsada por IA y protegiendo contra ataques sofisticados con inspección de tráfico integrada, protección de aplicaciones y datos. ZPA supera estos desafíos proporcionando acceso rápido y directo a aplicaciones a través de más de 160 puntos de presencia (PoP) distribuidos globalmente sin los riesgos de seguridad inherentes a la VPN. El diseño nativo de la nube de ZPA significa que los equipos de TI pueden eliminar los dispositivos de puerta de enlace entrantes, como equilibradores de carga, concentradores de VPN y otros dispositivos de seguridad, lo que reduce los costes, la complejidad y los gastos generales de administración. ZPA ofrece acceso zero trust a todas las aplicaciones, incluidas las aplicaciones conectadas a la red, como Voz sobre IP (VoIP) y aplicaciones de servidor a cliente, e incluso aplicaciones alojadas por socios comerciales (extranet) en las que los clientes no pueden implementar los conectores de aplicaciones de la solución.

Acceso seguro a aplicaciones para usuarios en la oficina e híbridos
Los trabajadores modernos trabajan desde sus hogares y otras ubicaciones remotas, sucursales y sedes centrales, lo que desafía los paradigmas de seguridad heredados. Las organizaciones necesitan acceso ininterrumpido a las aplicaciones, sin comprometer la seguridad de Zero Trust durante desastres o períodos de acceso degradado a la infraestructura. Se deben cumplir los estándares regulatorios y de cumplimiento para la continuidad del negocio.

ZPA Private Service Edge le permite implementar el poder de la nube en sus instalaciones, aplicando los mismos controles de seguridad que sus usuarios remotos con el mismo alto rendimiento. Al implementar Zscaler Private Service Edges con controladores de nube privada, ZPA admite la conmutación totalmente automatizada al modo de continuidad comercial en caso de detección de una interrupción. Las políticas y la autenticación se aplican incluso si no se puede acceder a ZPA Cloud.

Uso de dispositivo propios y acceso de usuarios de terceros
El acceso tradicional de terceros dependía de soluciones costosas, complejas y arriesgadas como VDI, RDP, SSH o VNC, que colocaban a los usuarios directamente en la red y exponían los sistemas internos a dispositivos no confiables.

Las capacidades de acceso sin cliente de ZPA facilitan el acceso de terceros, reducen costes y minimizan riesgos. Usuarios externos, como contratistas, proveedores y socios, pueden usar cualquier navegador web desde sus propios dispositivos para conectarse a sitios web de intranet, sistemas internos y equipos, sin necesidad de un cliente. Mantiene a los usuarios de terceros y a los dispositivos no administrados aislados de su red y aplicaciones, lo que garantiza que los datos confidenciales estén protegidos contra ataques no autorizados, actividad de copia/pega, impresión y carga/descarga. La integración de ZPA y el navegador Google Chrome Enterprise mejorará la seguridad de los dispositivos no administrados/propios del usuario verificando el navegador Chrome Enterprise e incorporando información de postura adicional en las comprobaciones de políticas de ZPA. Con el acceso sin cliente, TI puede brindar una experiencia mejor y más segura para los usuarios sin incurrir en los costos de administrar VDI heredado. Las fusiones y adquisiciones, y desinversiones plantean desafíos de integración de la red, pero ZPA acelera este proceso de meses a semanas. ZPA ofrece acceso perfecto a aplicaciones privadas, eliminando la necesidad de convergencia de red o equipos adicionales.

Acceso remoto privilegiado para OT/TI
Tanto empleados como proveedores externos necesitan acceder a los activos de OT/TI con regularidad para maximizar el tiempo de actividad de la producción y evitar interrupciones causadas por fallos de equipos y procesos. ZPA permite un acceso rápido, seguro y confiable a entornos OT/TI desde ubicaciones de campo, la fábrica o cualquier otro lugar. ZPA para OT/TI proporciona acceso a escritorio remoto sin cliente y totalmente aislado a sistemas de destino internos RDP, SSH y VNC, sin necesidad de que los usuarios instalen un cliente en su dispositivo utilizando hosts de salto y VPN heredadas.

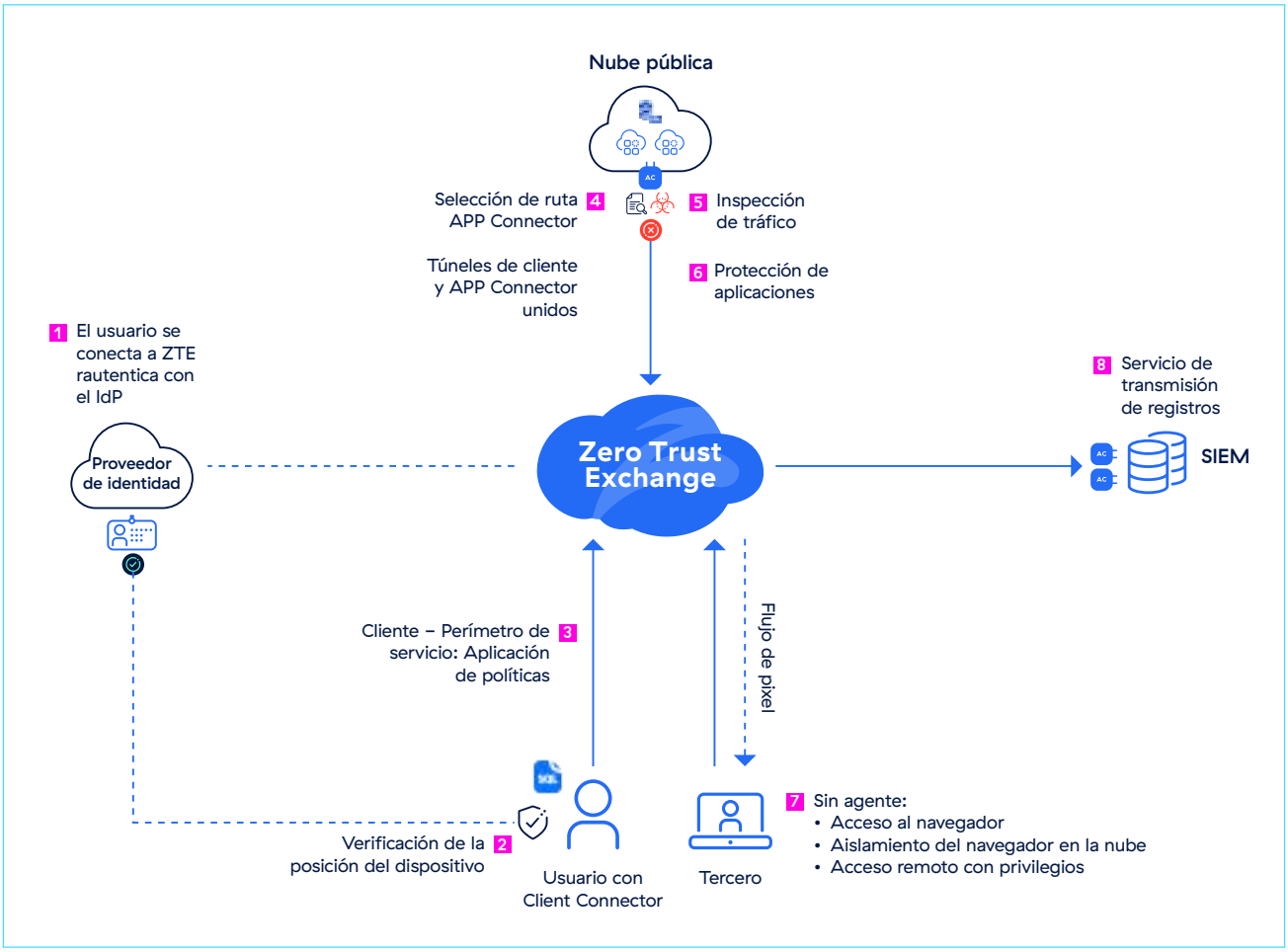
Alternativa a VDI
Los equipos de IT y seguridad carecen de control sobre los dispositivos no administrados, lo que genera riesgos comerciales. Para respaldar el acceso a las aplicaciones en dispositivos no administrados, las organizaciones han utilizado tradicionalmente VDI. Las VDI colocan a los usuarios directamente en la red, lo que expone las aplicaciones internas a terminales no administrados. Además, las VDI son costosas, difíciles de administrar y no escalables. A raíz de la transformación digital, las aplicaciones modernizadas suelen estar basadas en la web o en el navegador, y la transmisión de un escritorio completo a través de VDI no proporciona muy buena experiencia para el usuario final.

ZPA es una alternativa eficaz a VDI que ofrece acceso seguro, sin agentes y basado en navegador en dispositivos no administrados. Los usuarios obtienen acceso rápido y sin inconvenientes a aplicaciones privadas gestionadas por el perímetro de servicio más cercano. La arquitectura ZPA proporciona acceso directo a las aplicaciones, sin colocar al usuario en la red, lo que hace que el acceso a las aplicaciones privadas sea seguro. ZPA Browser Access permite a los usuarios aprovechar un navegador web para la autenticación de usuarios y el acceso a aplicaciones, sin necesidad de tener Zscaler Client Connector instalado en sus dispositivos. ZPA ha integrado el aislamiento del navegador, gracias al cual sólo se transmiten los píxeles al dispositivo del usuario final, en lugar del contenido real; los datos dentro de las aplicaciones permanecen seguros. ZPA permite a los administradores crear políticas de aislamiento para definir cómo un usuario puede interactuar dentro del entorno aislado.

Microsegmentación
Las soluciones de acceso remoto como las VPN otorgan acceso completo a la red, y exponen las IP y las aplicaciones a Internet. Las VPN extienden la red interna a dispositivos remotos y, por diseño, requieren tráfico entrante, lo que expone una superficie de ataque pública. Sin una segmentación de red adecuada, una brecha en un segmento podría comprometer toda la red de la organización. Dicho esto, la implementación de la segmentación requiere reglas de cortafuegos complejas que son difíciles de mantener, a menudo interrumpen las aplicaciones y pueden complicar el acceso para los usuarios de VPN. Dentro de las grandes organizaciones, esto a menudo requiere alta disponibilidad, enrutamiento complejo y enlaces privados caros.

La segmentación de aplicaciones impulsada por IA de Zscaler ofrece una segmentación precisa de usuario a aplicación y una solución sólida para implementar fácilmente políticas uniformes a escala y eliminar el movimiento lateral de amenazas. Le ayuda a descubrir todas las aplicaciones dentro de su organización y proporciona información visual sobre qué usuarios tienen acceso a qué aplicaciones. Genera automáticamente recomendaciones para segmentos de aplicaciones y políticas basadas en modelos de aprendizaje automático, lo que simplifica la implementación.

Cómo funciona ZPA



Cómo funciona

Cuando un usuario (empleado, proveedor, socio o contratista) intenta acceder a una aplicación interna, ZPA proporciona conectividad segura y directa mediante:

1. El usuario se conecta a Zero Trust Exchange con el Client Connector y se autentica con el proveedor de identidad (IdP). Tras una autenticación exitosa, se vuelve a conectar al Public Service Edge y se establece una única conexión TLS permanente con el Service Edge.
2. Tras la autenticación del usuario y el establecimiento del túnel hacia Service Edge, Client Connector descarga su configuración, incluida la verificación de la postura del dispositivo.
3. La aplicación Zscaler reenvía el tráfico del usuario al perímetro de servicio ZPA más cercano (que actúa como agente) donde se verifican las políticas de seguridad y acceso del usuario.
4. Dos túneles salientes, uno de Client Connector en el dispositivo y el otro de App Connector, se unen mediante el perímetro de servicio

5 Una vez que se establece una conexión entre el dispositivo del usuario y la aplicación, App Connector inspecciona automáticamente el tráfico en línea para detectar y detener posibles amenazas procedentes de usuarios o dispositivos que puedan haber sido vulnerados

6 Zscaler AppProtection protege las aplicaciones privadas basadas en la web y la identidad a través de una inspección integral de capa 7, lo que mejora la postura de seguridad general.

7 Los usuarios de terceros pueden conectarse a aplicaciones privadas con acceso integrado basado en el navegador o con Cloud Browser Isolation para un acceso sin agentes en dispositivos no gestionados

8 El servicio de transmisión de registros (LSS) transmite varios registros, incluida la actividad del usuario a SIEM

Un ZPA Service Edge puede ser alojado por Zscaler en la nube (ZPA Public Service Edge) o ejecutarse localmente dentro de su infraestructura (ZPA Private Service Edge), lo que proporciona una ruta más corta a las aplicaciones locales y respalda la planificación de la continuidad del negocio.

Capacidades principales

Motor de políticas basadas en el riesgo	Valide continuamente las políticas de acceso en función de la postura de riesgo del usuario, el dispositivo, el contenido y la aplicación con un potente motor de políticas nativo para garantizar que solo los usuarios válidos y autenticados puedan acceder a las aplicaciones privadas.
Cliente unificado y acceso sin cliente	Elija el método óptimo de protección para su entorno híbrido. El acceso basado en agente garantiza que los usuarios administrados estén protegidos incluso cuando están fuera de la red corporativa a través de un agente ligero, Zscaler Client Connector. El acceso sin agente da a los usuarios no gestionados acceso a aplicaciones sin fricciones desde cualquier dispositivo y navegador web, sin necesidad de cliente.
Acceso de navegador	Permita que los usuarios que usan dispositivos propios y los usuarios de terceros utilicen libremente sus propios dispositivos para acceder de forma segura y sin problemas a las aplicaciones internas aprovechando cualquier navegador web, sin necesidad de clientes.
ZTNA en el campus	Experimente ZTNA para usuarios en el campus y conecte de forma segura a los usuarios a las aplicaciones en sus oficinas. Universal ZTNA garantiza un acceso y políticas uniformes para los usuarios, independientemente de la ubicación de estos y las aplicaciones.
Continuidad empresarial y recuperación ante desastres	Acceso ininterrumpido a aplicaciones esenciales incluso durante un evento de cisne negro con una solución de continuidad comercial controlada por el cliente que crea la ruta de acceso a aplicaciones privadas esenciales a través de ZPA Private Service Edge.
Detección de aplicaciones	Descubra y catalogue automáticamente las aplicaciones mediante nombres de dominio y subredes IP específicos para obtener información detallada de su estado de aplicaciones privadas, así como de su posible superficie de ataque.
Segmentación de aplicaciones mediante IA	Aplique las recomendaciones de segmentación basadas en ML que se le proporcionan automáticamente vía ZPA. De esta manera podrá identificar los segmentos de aplicaciones adecuados y crear las políticas de acceso correctas de forma fácil y rápida. Con la tecnología de modelos de aprendizaje automático, probada continuamente en millones de señales de clientes, y sus patrones únicos de acceso a aplicaciones, la segmentación basada en ML puede ayudarle a minimizar su superficie de ataque interna.
Segmentación de usuario a aplicación	Asegúrese de que cualquier acceso a la aplicación se otorgue según la "necesidad de saber", en base a los privilegios mínimos, con la segmentación de usuario a aplicación. Proporcione a los usuarios autorizados acceso seguro a aplicaciones específicas, sin colocar nunca a los usuarios en la red. Evite la necesidad de una segmentación de red complicada con cortafuegos internos.
Protección de aplicaciones	Proteja las aplicaciones y la infraestructura privadas frente a los ataques más frecuentes con una inspección de seguridad en línea de alto rendimiento de toda la carga útil de la aplicación que expone las amenazas. Identifique y bloquee los riesgos de seguridad web conocidos, como los del OWASP Top 10, y las vulnerabilidades emergentes de día cero que pueden eludir los controles de seguridad de red tradicionales.

Acceso remoto privilegiado	Permita que los administradores y operadores con privilegios se conecten de forma segura a sitios web de intranet, sistemas internos y equipos sin necesidad de VPN, VDI o clientes de escritorio remoto como RDP, SSH y VNC.
Protección de datos y frente a amenazas	Reduzca el riesgo de amenazas con una inspección completa del contenido. Encuentre y controle los datos confidenciales en la conexión entre el usuario y la aplicación.
Identidad e inicio de sesión único (SSO)	Se integra fácilmente con su infraestructura de identidad y autenticación existente, aprovechando el SSO para reducir aún más la complejidad.
Acceso seguro a aplicaciones de red	Habilite el acceso seguro a aplicaciones conectadas a redes heredadas, como VoIP y aplicaciones de servidor a cliente.
Conectividad IPsec	Habilite el acceso zero trust a las aplicaciones de socios comerciales y proveedores (aplicación de extranet) alojadas en sus redes

Ventajas

Minimice la superficie de ataque
Eliminar las VPN vulnerables y hacer que las aplicaciones sean invisibles para Internet hace imposible que usuarios no autorizados las encuentren y ataquen. ZPA crea un segmento de uno entre un usuario autorizado y una aplicación privada específica, eliminando toda la conectividad de dentro hacia afuera y permitiendo exclusivamente conexiones internas a través de microtúneles cifrados a los dispositivos de los usuarios. Los administradores pueden descubrir y segmentar automáticamente aplicaciones, servicios y cargas de trabajo fraudulentas mediante la detección de aplicaciones, lo que reduce aún más la superficie de ataque.

Elimine el movimiento lateral
La conectividad basada en el acceso con privilegios mínimos garantiza que el acceso a las aplicaciones se otorgue de forma individual desde un usuario autorizado a las aplicaciones designadas, en lugar de un acceso total a la red. Por lo tanto, el movimiento lateral entre aplicaciones o a través de la red es imposible. Dado que ZPA no se basa en direcciones IP, se elimina la necesidad de configurar y administrar segmentaciones de red complejas, listas de control de acceso (ACL), políticas de cortafuegos co traducciones de direcciones de red.

Prevenga usuarios comprometidos, amenazas internas y atacantes avanzados
Las capacidades integradas de inspección en línea y DLP minimizan el riesgo de usuarios comprometidos y atacantes activos. ZPA detiene automáticamente los ataques web con cobertura completa para las técnicas más frecuentes, incluido el OWASP Top 10, y soporte completo de firmas personalizadas para la aplicación de revisiones virtuales inmediatas contra vulnerabilidades de día cero. ZPA minimiza los riesgos de terceros y de dispositivos propios con acceso completamente aislado a las aplicaciones que mantiene los datos confidenciales fuera de los dispositivos no administrados mediante el aislamiento del navegador en la nube integrado.

Ofrezca una experiencia de usuario exepcional
Una conectividad consistentemente rápida que no requiere iniciar y cerrar sesión en los clientes VPN brinda a los usuarios remotos una experiencia de acceso más segura y eficiente. Los contratistas, proveedores y socios externos se benefician de un acceso sin fricciones desde cualquier dispositivo y navegador web sin necesidad de instalar un cliente. Los usuarios se inscriben con sus credenciales SSO existentes (Azure AD, Okta, Ping, etc.). Además, los administradores pueden mantener la productividad de los usuarios detectando y resolviendo proactivamente los problemas de rendimiento del usuario final causados por dificultades de acceso a aplicaciones privadas, interrupciones en las rutas de red o congestión de la red.

Una plataforma unificada para el acceso seguro entre aplicaciones, cargas de trabajo y dispositivos
Amplíe zero trust entre aplicaciones privadas y dispositivos OT/IT para simplificar e integrar múltiples herramientas de acceso remoto inconexas, unificando las políticas de seguridad y acceso para detener las infracciones y reducir la complejidad operativa.

Opciones de empaquetado Zscaler Private Access

	Plataforma Zscaler Essentials (PLATAFORMA ZS-ESS)	Plataforma Zscaler Private Access (PLATAFORMA ZS-ZPA)	Plataforma Zscaler (PLATAFORMA ZS)
Servicios de la plataforma de acceso privado	✔ 1 usuario por cada 20 usuarios suscritos (Mín.: 500 usuarios suscritos)	✔	✔
Control de acceso granular por usuario, grupo y puertos			
Servicio de transmisión de registros			
Supervisión continua del estado de todas las aplicaciones			
Anclaje IP de origen			
App Connector	$	Tantos como sean necesarios, hasta el máximo del sistema	Tantos como sean necesarios, hasta el máximo del sistema
ZPA Private Service Edge			
Acceso de terceros	$	✔ PRA para más de 500 usuarios	✔ PRA para más de 500 usuarios
Acceso mediante navegador			
Portal del usuario			
Estándar de acceso remoto privilegiado (PRA)			
Supervisión de la experiencia digital	$	✔	✔
Estándar ZDX			
Seguridad para aplicaciones privadas	$	$	✔ Engaño para más de 500 usuarios
Protección de datos para aplicaciones privadas			
Gestión de riesgos: engaño			
Segmentación	20 segmentos de aplicación (10 recomendaciones/90 días, retrospectiva limitada)	20 segmentos de aplicación (10 recomendaciones/90 días, retrospectiva limitada)	20 segmentos de aplicación (10 recomendaciones/90 días, retrospectiva limitada)
Segmentos de aplicaciones y vista previa de segmentación			
Complemento de segmentación	✔ 100 recomendaciones/14 días Informes semanales a petición, descargue y analice hasta 30 días de datos Importe aplicaciones desde el sistema interno o fuentes de terceros (Qualys, Tenable, ServiceNow)	✔ 100 recomendaciones/14 días Informes semanales a petición, descargue y analice hasta 30 días de datos Importe aplicaciones desde el sistema interno o fuentes de terceros (Qualys, Tenable, ServiceNow)	✔ 100 recomendaciones/14 días Informes semanales a petición, descargue y analice hasta 30 días de datos Importe aplicaciones desde el sistema interno o fuentes de terceros (Qualys, Tenable, ServiceNow)
Segmentos de aplicación ilimitados			
Segmentación impulsada por IA			
Información de segmentación			
Importación de segmentos de aplicaciones (desde archivos de datos estructurados)			
Complemento AppProtection	Complemento	Complemento	Complemento
Visibilidad de ataques a aplicaciones			
Las 10 principales defensas de OWASP: inyección SQL, secuencias de comandos entre sitios, escáneres ambientales y de puertos			
Protección contra amenazas de día cero			
Supervisión de usuarios de alto riesgo			

Diferenciadores clave

Como la primera solución ZTNA impulsada por IA de la industria, ZPA ofrece seguridad superior con una experiencia de usuario inigualable:

- **Creada desde cero para un acceso de privilegios mínimos:**permita que los usuarios autorizados se conecten solo a los recursos aprobados, no a su red, lo cual sería imposible con las VPN heredadas.
- **Las aplicaciones se vuelven invisibles e inaccesibles para los atacantes:** detenga el compromiso de las aplicaciones, el robo de datos y el movimiento lateral haciendo que las aplicaciones, las cargas de trabajo y los dispositivos privados sean invisibles para la Internet pública
- **Inspección completa en línea:** proteja sus aplicaciones identificando y deteniendo la explotación de aplicaciones privadas, previniendo automáticamente los ataques web más frecuentes mientras protege sus datos con DLP líder en el sector
- **Habilite la continuidad empresarial global sin comprometer la seguridad:** minimice el impacto de las interrupciones e implemente el acceso zero trust para cumplir con los estrictos requisitos de cumplimiento incluso cuando la nube de Zscaler no esté disponible
- **Acceso sin cliente:** aproveche el acceso basado en navegador para terceros con DLP integrado
- **Elimine el movimiento lateral con segmentación impulsada por IA:** ofrece una segmentación precisa de usuario a aplicación, visualiza el acceso y ajusta las políticas mediante el aprendizaje automático para minimizar las superficies de ataque y prevenir amenazas laterales.
- **Presencial de perímetro global:** obtenga una seguridad y una experiencia de usuario incomparables con más de 160 ubicaciones en el perímetro de la nube en todo el mundo, así como un perímetro de servicio local opcional para ampliar zero trust a su sede central
- **Fundación nativa de la nube:** aproveche la escalabilidad de una plataforma entregada en la nube sin costosos dispositivos ni complejas infraestructuras locales a medida que su negocio crece
- **Plataforma ZTNA unificada para usuarios, cargas de trabajo y dispositivos:** conéctese de forma segura a aplicaciones, servicios y dispositivos OT privados con la plataforma ZTNA más completa del sector.
- **Parte de una plataforma extensible de confianza cero:** proteja y potencie su negocio con Zero Trust Exchange, creado sobre un marco completo de SSE

**Gartner, Cuadrante mágico para Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15 de abril de 2024

Gartner no avala ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no aconseja a los usuarios de tecnología que seleccionen solo a los proveedores con las calificaciones más altas u otra designación. Las publicaciones de investigación de Gartner recogen las opiniones de la organización de investigación de Gartner y no deben interpretarse como declaraciones de hecho. Gartner renuncia a toda garantía, expresa o implícita, con respecto a este análisis, incluida cualquier garantía de comerciabilidad o adecuación a un fin determinado.

GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en EE. UU. e internacionalmente, y MAGIC QUADRANT es una marca comercial registrada de Gartner, Inc. y/o sus filiales y se utilizan aquí con autorización. Todos los derechos reservados.

Componentes fundamentales

Zscaler Client Connector
Client Connector es una aplicación ligera que se ejecuta en los ordenadores portátiles y dispositivos móviles de los usuarios. Al reenviar automáticamente el tráfico de usuarios al perímetro de servicio de Zscaler más cercano, se garantiza que las políticas de seguridad y acceso se apliquen en todos los dispositivos, las ubicaciones y las aplicaciones.

Acceso sin cliente de Zscaler
Los usuarios pueden conectarse de forma segura a aplicaciones, cargas de trabajo y dispositivos OT a través del acceso integrado basado en navegador (web, RDP, SSH, VNC) o Zscaler Browser Isolation para acceso sin cliente en dispositivos no administrados.

ZPA App Connector
Los App Connectors son máquinas virtuales ligeras que se sitúan delante de aplicaciones privadas implementadas en el centro de datos o en la nube pública, lo que permite la conectividad segura entre un usuario autorizado y una aplicación nominal con una conexión interna que no expone aplicaciones a Internet.

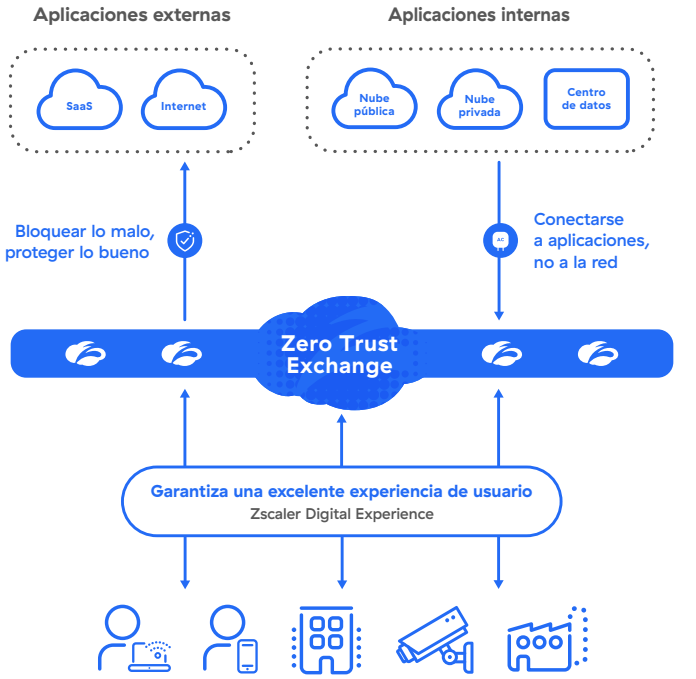
ZPA Service Edges
Los perímetros de servicio aseguran el cumplimiento de políticas de seguridad y acceso, vinculando la conexión den entrada y salida entre un usuario autorizado (a través de Client Connector y Browser Access) y una aplicación privada específica (a través de App Connector). La mayoría de los clientes utilizan nuestros perímetros de servicio públicos, que están alojados en más de 160 intercambios en todo el mundo y manejan millones de usuarios simultáneos para las mayores organizaciones a nivel global. También hay perímetros de servicio privados, administrados por Zscaler, disponibles para alojarse en el sitio y brindar a los usuarios locales la ruta más corta a las aplicaciones locales sin salir de la red local.

ZPA forma parte de la plataforma global Zero Trust Exchange

Zscaler Zero Trust Exchange es una plataforma nativa de la nube que activa un completo perímetro de servicio de seguridad (SSE) para conectar usuarios, cargas de trabajo y dispositivos sin colocarlos en la red corporativa. Reduce los riesgos de seguridad y la complejidad asociada a las soluciones de seguridad basadas en el perímetro que extienden la red, amplían la superficie de ataque, aumentan el riesgo de movimiento lateral de las amenazas y no logran evitar la pérdida de datos.

Cómo Zscaler ofrece zero trust para usuarios, cargas de trabajo y OT/TI

Implementación en semanas para mejorar la protección cibernética y la experiencia del usuario



Cualquier usuario, cualquier dispositivo, cualquier aplicación, cualquier lugar

Especificaciones técnicas

Componente Zscaler	Plataformas y sistemas compatibles	
Client Connector	iOS 9 o posterior Android 5 o posterior Windows 7 o posterior	macOSX 10.10 o posterior CentOS 8 Ubuntu 20.04
Clientless Access	Navegadores web modernos: (compatible con HTML 5)	Chrome Edge Firefox
App Connector	AWS Centos, Oracle y Red hat Microsoft Azure	Microsoft Hyper-V VMware vCenter o vSphere Hypervisor Anfitrión acoplable

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

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