FICHA DE DATOS

Zscaler Private Access™

Proporcione a sus empleados un acceso rápido, seguro y confiable a aplicaciones privadas con el primer ZTNA del sector potenciado por IA.

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.

Las estrategias de seguridad de red heredadas no satisfacen las necesidades de su fuerza de trabajo híbrida ni de su empresa.
Los firewalls y las VPN tradicionales crean una enorme superficie de ataque que los atacantes pueden encontrar y explotar. Además, conectan a los usuarios directamente a su red, lo que permite la propagación lateral de amenazas. Si las credenciales de sus usuarios se ven comprometidas, los atacantes tienen fácil acceso a sus datos confidenciales. Usar una VPN para habilitar el acceso de su fuerza de trabajo híbrida y externa aumenta el ciberriesgo, genera malas experiencias de usuario y aumenta la carga administrativa. Para proporcionar acceso seguro a los usuarios desde cualquier dispositivo y ubicación, necesita un enfoque más eficaz.

Según el Informe de riesgo de VPN de ThreatLabz 2025, el 92 % de los encuestados comparte la preocupación de que las deficiencias de una VPN sin parchear conducen directamente a incidentes de ransomware, lo que destaca lo difícil que es aplicar parches a las VPN de manera continua y a tiempo.

Ventajas:

- **Sustituya las soluciones de VPN vulnerables**
  Reduzca la superficie de ataque y elimine el movimiento lateral conectando a los usuarios directamente a las aplicaciones, no a la red, elevando su postura de seguridad.
- **Evite los ciberataques**
  Minimice el riesgo de una violación 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 fuerza de trabajo híbrida**
  Amplíe a la perfección el acceso ultrarrápido a aplicaciones privadas entre usuarios, la sede central, las sucursales y terceros.
- **Reduzca la complejidad operativa**
  Ofrezca un 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 e IoT/OT.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Los atacantes pueden burlar fácilmente los modelos de seguridad de red heredados aprovechando la confianza inherente y el acceso excesivamente permisivo de las arquitecturas castle–and–moat tradicionales, lo cual incluye:

- **La arquitectura heredada no puede escalar ni ofrecer una experiencia de usuario rápida y sin interrupciones:** Las VPN requieren redes de retorno, lo que introduce costos, complejidad y demasiada latencia para el personal remoto de la actualidad.
- **Los firewalls tradicionales, las VPN, la VDI y las aplicaciones privadas crean una enorme superficie de ataque:** 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, lo que facilita a los atacantes el acceso a los 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

Es hora de replantearse cómo conectamos de manera segura y fluida a los usuarios con las aplicaciones que necesitan y redefinir la seguridad de las aplicaciones privadas con una solución de acceso a la red Zero Trust (ZTNA).

Zscaler Private Access™ (ZPA)

Zscaler Private Access (ZPA), el primer ZTNA de la industria impulsado por la IA, es una solución nativa en 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 ocultando las aplicaciones tras el Zero Trust Exchange, eliminando el movimiento lateral mediante la segmentación de usuario a aplicación impulsada por la IA y protegiendo contra ataques sofisticados con inspección de tráfico integrada y protección de aplicaciones y datos. ZPA es un servicio resiliente nativo en la nube basado en un marco integral de Security Service Edge (SSE) que se puede implementar en cuestión de horas para reemplazar las VPN heredadas y las herramientas de acceso a distancia para:

- **Minimizar la superficie de ataque:** Las aplicaciones se hacen invisibles a Internet, lo que impide que usuarios y dispositivos no autorizados las descubran. Las conexiones internas 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 darles acceso.
- **Eliminar el movimiento lateral:** Las aplicaciones están segmentadas para que los usuarios solo 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:** Al conectar a los usuarios directamente a las aplicaciones privadas se elimina el lento y costoso retorno a través de las VPN heredadas, al tiempo que se supervisan continuamente y se resuelven de manera proactiva los problemas de experiencia del usuario.

El 92 % de los encuestados comparte la preocupación de que las deficiencias de una VPN sin parchear conducen directamente a incidentes de ransomware, lo que destaca lo difícil que es aplicar parches a las VPN de manera continua y a tiempo

Informe de riesgos de las VPN de ThreatLabz 2025 de Zscaler

*Gartner®, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales. 8 de abril de 2022

© 2025 Zscaler, Inc. Todos los derechos reservados.

Casos importantes de uso

Acceso remoto seguro (sustitución de VPN).
Las VPN en la nube o basadas en dispositivos lo exponen a ciberataques. Están plagadas de vulnerabilidades y, con frecuencia, son explotadas por atacantes. Su diseño centrado en la red redirecciona el tráfico, amplía la superficie de ataque y permite el movimiento lateral al conectar a los usuarios directamente a la red, lo que puede provocar ataques de ransomware. Las VPN son inseguras, lentas y complejas de administrar.

El 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 la IA y protegiendo contra ataques sofisticados con inspección de tráfico integrada y protección de aplicaciones y datos. ZPA proporciona acceso rápido y directo a

a las aplicaciones a través de más de 160 puntos de presencia distribuidos por todo el mundo, sin los riesgos de seguridad inherentes a las VPN. El diseño nativo en la nube de ZPA significa que los equipos de TI pueden eliminar los dispositivos de puerta de enlace de entrada como equilibradores de carga, concentradores VPN y otros dispositivos de seguridad, reduciendo los costos, la complejidad y la sobrecarga de gestión. ZPA ofrece acceso Zero Trust a todas las aplicaciones, incluidas aquellas conectadas a la red, como las de voz sobre IP (VoIP) y las aplicaciones de servidor a cliente, e incluso las alojadas por socios comerciales (extranet) sin la necesidad de implementar infraestructura adicional, como conectores de aplicaciones.

Acceso seguro a aplicaciones para usuarios presenciales y remotos.
En la fuerza de trabajo moderna, los usuarios trabajan desde sus hogares y otras ubicaciones remotas, sucursales y sedes centrales, lo que desafía los paradigmas de seguridad tradicionales. Las organizaciones necesitan acceso ininterrumpido a las aplicaciones, sin comprometer la seguridad Zero Trust durante desastres o periodos de acceso deficiente a la infraestructura. Es fundamental cumplir con los estándares regulatorios y de cumplimiento para garantizar la continuidad empresarial.

ZPA Private Service Edge le permite implementar la potencia 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 Edge con controladores de nube privada, ZPA admite la conmutación totalmente automatizada al modo de continuidad comercial en caso de que se detecte una interrupción. Las políticas y la autenticación se aplican incluso si no se puede acceder a ZPA Cloud.

BYOD y acceso de usuarios externos
El acceso tradicional de terceros dependía de soluciones costosas, complejas y riesgosas 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 agentes externos, reducen costos y minimizan riesgos. Agentes 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 externos y a los dispositivos no administrados aislados de su red y aplicaciones, lo que garantiza que los datos confidenciales estén protegidos contra copias/pegados, impresiones y cargas/descargas no autorizadas. La integración de ZPA y Google Chrome Enterprise Browser mejorará la seguridad de los dispositivos no gestionados/BYOD mediante la verificación de Chrome Enterprise Browser y la incorporación de información adicional sobre la postura 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 las desinversiones plantean desafíos de integración de redes, pero el ZPA acelera este proceso de meses a semanas. La ZPA ofrece un acceso fluido a las aplicaciones privadas, eliminando la necesidad de convergencia de redes o de equipos adicionales.

Acceso remoto privilegiado para OT/TI
Los empleados y proveedores externos necesitan acceder activos de OT/TI regularmente para maximizar el tiempo

© 2025 Zscaler, Inc. Todos los derechos reservados.

de producción y evitar interrupciones por fallas en los equipos y procesos. ZPA permite un acceso rápido, seguro y confiable a los entornos de OT/TI desde ubicaciones de campo, la planta de producción o cualquier otro lugar. ZPA para OT/TI proporciona acceso de escritorio remoto totalmente aislado y sin cliente a sistemas de destino internos RDP, SSH y VNC, sin necesidad de que los usuarios instalen un cliente en su dispositivo mediante hosts de salto y VPN heredadas.

Alternativa a VDI

Los equipos de TI y seguridad carecen de control sobre los dispositivos no administrados, lo que genera riesgos empresariales. Para facilitar el acceso a las aplicaciones en dispositivos no administrados, las organizaciones han utilizado tradicionalmente VDI. Las VDI conectan a los usuarios directamente a la red, exponiendo las aplicaciones internas a puntos finales no administrados. Además, las VDI son costosas, difíciles de administrar y no escalables. Tras la transformación digital, las aplicaciones modernizadas suelen estar basadas en la web o el navegador, y la transmisión de un escritorio completo mediante VDI no ofrece una experiencia óptima para el usuario final.

ZPA es una alternativa eficaz a las 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 servicio perimetral más cercano. La arquitectura ZPA proporciona acceso directo a las aplicaciones, sin conectar al usuario a la red, lo que hace que el acceso a las aplicaciones privadas sea seguro. ZPA Browser Access permite a los usuarios utilizar 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 cuenta con un aislamiento del navegador integrado, gracias al cual solo se transmiten 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.

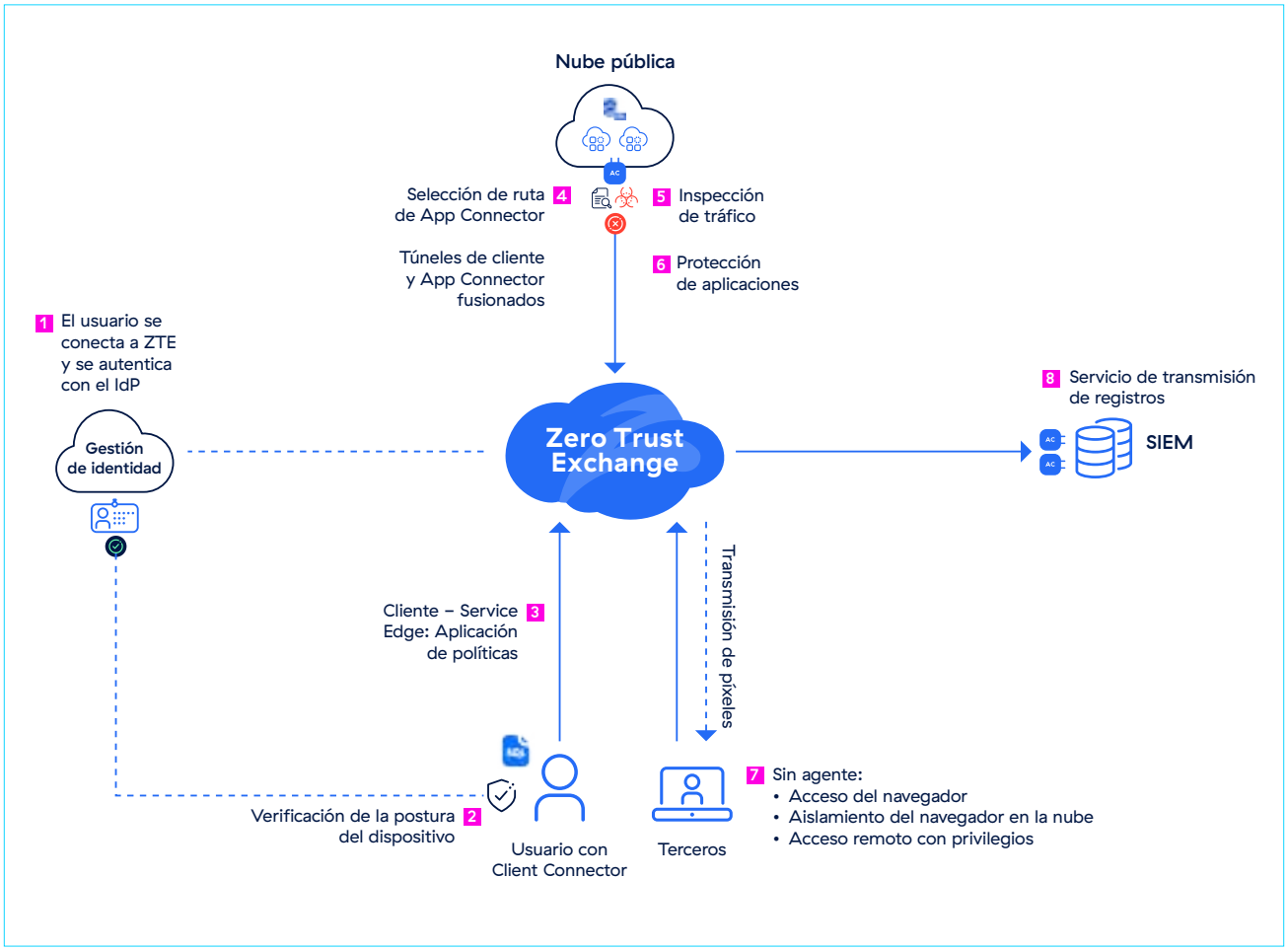
Microsegmentación (Segmentación de usuario a aplicación)

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 violación en un segmento podría comprometer toda la red de la organización. Sin embargo, implementar la segmentación requiere reglas de firewall complejas que son difíciles de mantener, a menudo interrumpen las aplicaciones y pueden dificultar el acceso de los usuarios de VPN. En organizaciones grandes, esto suele requerir alta disponibilidad, enrutamiento complejo y enlaces privados costosos.

La segmentación autónoma de usuario a aplicación 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. Automatiza todo el ciclo de vida de la segmentación al ver cada aplicación a través de la detección, segmentando más rápido con recomendaciones impulsadas por la IA y fortaleciendo su postura con información en vivo.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Cómo funciona ZPA



Cómo funciona

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

1 El usuario se conecta a Zero Trust Exchange con 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, el conector del cliente descarga su configuración, incluida la verificación de la postura del dispositivo.

3 La aplicación Zscaler reenvía el tráfico del usuario al ZPA Service Edge más cercano, que actúa como agente intermediario, donde se comprueban las políticas de seguridad y acceso del usuario.

4 El Service Edge de ZPA une dos túneles de salida, uno desde el conector de clientes, Client Connector, en el dispositivo y el otro desde el Service Edge

© 2025 Zscaler, Inc. Todos los derechos reservados.

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 provenientes de usuarios o dispositivos que puedan estar en peligro

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 externos pueden conectarse a aplicaciones privadas con acceso integrado basado en navegador o Zscaler Browser Isolation para un acceso sin cliente en dispositivos no gestionados

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

El Service Edge de ZPA puede ser alojado por Zscaler en la nube (ZPA Public Service Edge) o ejecutarse en sus instalaciones dentro de su infraestructura (ZPA Private Service Edge), ofreciendo una ruta más corta a las aplicaciones locales y apoyando la Planificación de Continuidad Empresarial.

Capacidades centrales

Detección de aplicaciones	Detecte y catalogue aplicaciones automáticamente mediante nombres de dominio y subredes IP específicos para obtener información granular sobre el estado de su aplicación privada y su posible superficie de ataque.
Segmentación de usuario a aplicación	Asegúrese de que todos los accesos a las aplicaciones se concedan cuando sea estrictamente necesario y con privilegios mínimos de segmentación de usuario a aplicación. Proporcione acceso seguro a aplicaciones específicas a los usuarios autorizados, sin colocar nunca a los usuarios en la red. Evite la necesidad de una segmentación de red complicada con firewalls internos.
Segmentación autónoma de usuario a aplicación	Automatice todo el ciclo de vida de la segmentación al ver cada aplicación a través de la detección, segmentando más rápido con recomendaciones impulsadas por la IA y fortaleciendo su postura con información en vivo. Impulsada por modelos de ML entrenados continuamente con millones de señales de clientes y sus patrones únicos de acceso a aplicaciones, la segmentación autónoma de usuario a aplicación puede ayudarle a eliminar el movimiento lateral de amenazas, acelerar su recorrido hacia ZTNA y simplificar y escalar las operaciones Zero Trust.
Motor de políticas basado en riesgos	Valide continuamente las políticas de acceso basadas en el usuario, el dispositivo, el contenido y la postura de riesgo de la aplicación con un potente motor de políticas nativo para garantizar que solo los usuarios válidos y autenticados puedan tener acceso a las aplicaciones privadas.
Protección de datos y amenazas	Reduzca el riesgo de amenazas con una inspección completa del contenido. Busque y controle los datos confidenciales en la conexión usuario a aplicación
Protección de aplicaciones	Proteja las aplicaciones privadas y la infraestructura contra los ataques más frecuentes con una inspección de seguridad en línea de alto rendimiento de toda la carga útil de aplicaciones que exponga las amenazas. Identifique y bloquee los riesgos de seguridad web conocidos, como el Top 10 de OWASP, y las vulnerabilidades emergentes de día cero que pueden eludir los controles de seguridad de red tradicionales.
Acceso remoto con privilegios	Permita que los administradores y operadores con privilegios se conecten a sitios web de intranet, sistemas internos y equipos de manera segura y sin la necesidad de usar VPN, VDI o clientes de escritorio remoto como RDP, SSH y VNC.
Acceso seguro a aplicaciones S2C heredadas	Habilite el acceso seguro a aplicaciones conectadas a redes heredadas, como VoIP, impresora Follow Me y otras aplicaciones de servidor a cliente.
Acceso a aplicaciones B2B	Habilite el acceso bidireccional seguro a las aplicaciones y cargas de trabajo alojadas en la red de su socio comercial (Extranet)

© 2025 Zscaler, Inc. Todos los derechos reservados.

Acceso basado en cliente y sin cliente	Elija el método óptimo de protección para su entorno híbrido. El acceso basado en agentes asegura que los usuarios administrados estén protegidos incluso cuando están fuera de la red corporativa mediante el agente ligero Zscaler Client Connector. El acceso sin cliente proporciona acceso sin inconvenientes a los contratistas externos y a los usuarios BYOD a las aplicaciones desde cualquier dispositivo y navegador web.
ZTNA en la oficina	Implemente ZTNA para usuarios en la oficina que utilizan perímetros de servicio privados de ZPA, lo que garantiza un acceso rápido y sin inconvenientes a las aplicaciones. Nuestro ZTNA universal garantiza un acceso y políticas uniformes para los usuarios independientemente de la ubicación de estos y las aplicaciones.
Continuidad empresarial y recuperación ante desastres	Garantice el acceso ininterrumpido a aplicaciones de misión crítica incluso durante un evento de cisne negro con una solución de continuidad empresarial totalmente gestionada o alojada por el cliente.

Ventajas

Minimice la superficie de ataque
Eliminar las VPN vulnerables y hacer que las aplicaciones sean invisibles en Internet impide que usuarios no autorizados las encuentren y las ataquen. ZPA crea un segmento de uno entre un usuario autorizado y una aplicación privada específica, eliminando toda la conectividad entrante y permitiendo únicamente 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 manera individual, desde un usuario autorizado hasta las aplicaciones designadas, en lugar de permitir el 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 gestionar segmentaciones de red complejas, listas de control de acceso (ACL), políticas de firewall o traducciones de direcciones de red.

Evite usuarios comprometidos, amenazas internas y atacantes avanzados
Las funciones 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 comunes, incluyendo el Top 10 de OWASP, y compatibilidad total con firmas personalizadas para la aplicación inmediata de parches virtuales contra vulnerabilidades de día cero. ZPA minimiza los riesgos de usuarios exterrnos y BYOD con acceso completamente aislado a las aplicaciones, manteniendo los datos confidenciales fuera de los dispositivos no administrados mediante el aislamiento integrado del navegador en la nube.

Ofrezca una experiencia de usuario excepcional
La conectividad rápida y constante, que no requiere iniciar y cerrar sesión en clientes VPN, ofrece a los usuarios remotos una experiencia de acceso más segura y eficiente. Los contratistas, proveedores y socios externos se benefician de un acceso sin inconvenientes desde cualquier dispositivo y navegador web sin necesidad de instalar un cliente. Los usuarios se registran con sus credenciales de inicio de sesión único (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 la ruta de red o congestión de la red.

Una plataforma unificada para el acceso seguro entre aplicaciones, cargas de trabajo y dispositivos
Amplíe Zero Trust a LAS aplicaciones privadas y los dispositivos de OT/TI para simplificar e integrar múltiples herramientas de acceso remoto inconexas, unificando las políticas de seguridad y acceso para detener las violaciones y reducir la complejidad operativa.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Zscaler Private Access (ZPA): Múltiples opciones para dar los primeros pasos

	Plataforma Zscaler Essentials (ZS-ESS-PLATFORM)	Plataforma ZPA sin cliente (ZPA-CLIENTLESS-PLATFORM)	Plataforma Zscaler Private Access (ZS-ZPA-PLATFORM)	Plataforma Zscaler (ZS-PLATFORM)
Servicios de la plataforma Private Access				
Control de acceso granular por usuario, grupo y puertos	✓ 1 usuario por cada 20 usuarios suscritos (Mínimo: 500 usuarios suscritos)	✓	✓	✓
Servicio de transmisión de registros				
Supervisión continua de la salud de todas las aplicaciones				
Anclaje de IP de origen: Reenvíe selectivamente el tráfico de la aplicación a los servidores de destino adecuados				
App Connector: Máquina virtual ligera que permite conexiones internas a Zscaler ZTE	Tantos como sea necesario, hasta el máximo del sistema	Tantos como sea necesario, hasta el máximo del sistema	Tantos como sea necesario, hasta el máximo del sistema	Tantos como sea necesario, hasta el máximo del sistema
ZPA Private Service Edge: ZTNA para usuarios remotos y en la oficina	–	–		
ZPA para aplicaciones heredadas (VOIP, S2C, etc.)	–	–	Complemento de perímetro de servicio VPN (mínimo: 50 usuarios)	Complemento de perímetro de servicio VPN (mínimo: 50 usuarios)
Nube de continuidad empresarial de ZPA	–	–	Complemento (Mín: 500 usuarios)	Complemento (Mín: 500 usuarios)
Segmentación de usuario a aplicación	10 segmentos de aplicación	20 segmentos de aplicación	20 segmentos de aplicación	20 segmentos de aplicación
Segmentación autónoma de usuario a aplicación y conocimientos	–	–	**Complemento**	**Complemento**
Acceso para terceros			Complemento (Mín: 500 usuarios)	Complemento (Mín: 500 usuarios)
Acceso basado en el navegador para dispositivos no administrados	–	✓	✓ Se pueden comprar licencias adicionales para usuarios invitados con ZPA-CLIENTLESS-PLATFORM	✓ Se pueden comprar licencias adicionales para usuarios invitados con ZPA-CLIENTLESS-PLATFORM
Portal de usuario: Portal web único para que los usuarios accedan a las aplicaciones autorizadas y consolas privilegiadas				
Estándar de acceso remoto privilegiado: PRA sin cliente para sistemas OT (hasta 10) (RDP/SSH/VNC)				
Browser Isolation™ para aplicaciones privadas y SaaS		**Complemento**	**Complemento**	**Complemento**
Supervisión de la experiencia digital	–	–	✓	✓
ZDX Standard: visibilidad del usuario, conectividad y telemetría de aplicaciones				
Proteja aplicaciones y datos privados	**Complemento**			
Protección de datos para aplicaciones privadas, respuesta a incidentes y clasificación de datos		–	**Complemento**	✓
Zscaler Deception: Señuelos integrados para detectar usuarios comprometidos		–	✓ (Mín. 500 usuarios)	✓ (Mín. 500 usuarios)
AppProtection para proteger aplicaciones privadas de los Top 10 de OWASP e inspección del tráfico web		**Complemento**	**Complemento**	**Complemento**

© 2025 Zscaler, Inc. Todos los derechos reservados.

Diferenciadores clave

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

- **Desarrollada desde su creación para un acceso con privilegios mínimos:** Permita que los usuarios autorizados se conecten únicamente a los recursos autorizados, no a su red, lo que es 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 desplazamiento lateral haciendo que las aplicaciones, cargas de trabajo y dispositivos privados sean invisibles para la Internet pública.
- **Inspección completa en línea:** Proteja sus aplicaciones identificando y deteniendo la explotación de aplicaciones privadas, impidiendo automáticamente los ataques web más frecuentes a la vez que protege sus datos con DLP líder del sector.
- **Facilite la continuidad empresarial global sin comprometer la seguridad:** minimice el impacto de las interrupciones y aplique el acceso Zero Trust para cumplir con los estrictos requisitos de cumplimiento incluso cuando la nube de Zscaler no sea accesible.
- **Acceso seguro al navegador:** aproveche el acceso basado en navegador para usuarios externos con DLP integrado
- **Elimine el movimiento lateral con la segmentación autónoma de usuario a aplicación:** 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 evitar las amenazas laterales.
- **Presencia de perímetro global:** Obtenga una seguridad y una experiencia de usuario inigualables con más de 160 ubicaciones de perímetro de nube en todo el mundo, así como un perímetro de servicio local opcional para ampliar la Zero Trust a su sede central.
- **Base nativa en la nube:** Aproveche la escalabilidad de una plataforma en la nube sin costosos dispositivos locales ni infraestructuras complejas a medida que su empresa crece.
- **Plataforma ZTNA unificada para usuarios, cargas de trabajo y dispositivos:** Conéctese de manera segura a aplicaciones, servicios y dispositivos OT privados con la plataforma ZTNA más completa del sector.
- **Parte de una plataforma Zero Trust ampliable:** Proteja y potencie su empresa con Zero Trust Exchange, diseñado a partir de un marco completo de SSE.

Gartner

Zscaler ha sido nombrado Líder en el Gartner® Magic Quadrant™ de 2025 para Security Service Edge**

Más información

**Gartner®, Magic Quadrant for Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15 de abril de 2024

Gartner® no respalda a ningún proveedor, producto o servicio representado 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 su organización de investigación y no deben interpretarse como declaraciones de hecho. Gartner® renuncia a toda garantía, expresa o implícita, con respecto a esta investigación, incluida cualquier garantía de comerciabilidad o adecuación a un fin determinado.

GARTNER es una marca registrada y una marca de servicio de Gartner, Inc. y/o sus afiliados en los Estados Unidos y en otros países, y MAGIC QUADRANT es una marca registrada de Gartner, Inc. y/o sus afiliados y se utiliza en este documento con permiso. Todos los derechos reservados.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Componentes básicos

Zscaler Client Connector
Client Connector es una aplicación ligera que se ejecuta en laptops y dispositivos móviles de los usuarios. Al redireccionar automáticamente el tráfico de los usuarios al Zscaler Service Edge más cercano, garantiza que las políticas de seguridad y acceso se apliquen en todos los dispositivos, ubicaciones y aplicaciones.

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

ZPA App Connector
Los conectores de aplicaciones son máquinas virtuales ligeras que se ubican frente a aplicaciones privadas implementadas en el centro de datos o la nube pública, negociando la conectividad de seguridad entre un usuario autorizado y una aplicación designada con una conexión de adentro hacia afuera que no expone las aplicaciones a Internet.

ZPA Network Connector
Los conectores de red son máquinas virtuales ligeras que se implementan frente a los servidores de aplicaciones en el centro de datos y se conectan a los perímetros de servicio VPN en la nube de Zscaler con un túnel de adentro hacia afuera.

ZPA Service Edges
Los perímetros de servicio aplican políticas de seguridad y acceso, integrando la conexión interna y externa entre un usuario autorizado (mediante Client Connector y el acceso al navegador) y una aplicación privada específica (mediante App Connector). La mayoría de los clientes utilizan nuestros perímetros de servicio públicos, alojados en más de 160 puntos de presencia (PoP) en todo el mundo y que gestionan millones de usuarios simultáneos para las organizaciones más grandes del mundo. Los perímetros de servicio privados, gestionados por Zscaler, también están disponibles para su alojamiento in situ, ofreciendo a los usuarios locales la ruta más corta a las aplicaciones locales sin salir de la red local. Además, garantizan la continuidad empresarial con acceso ininterrumpido a aplicaciones críticas, incluso durante un evento de cisne negro.

ZPA Private Cloud Controller
Los controladores de nube privada son un controlador por inquilino que los usuarios, los perímetros de servicio privado de ZPA y los conectores de aplicaciones pueden aprovechar cuando la nube de Zscaler no está disponible o no se puede acceder a ella.

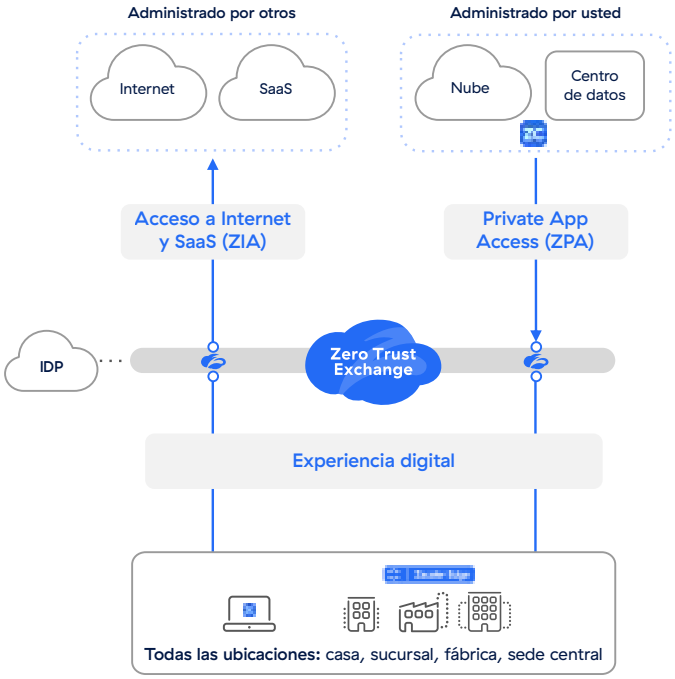
ZPA forma parte del intercambio holístico Zero Trust Exchange

Zscaler Zero Trust Exchange es una plataforma nativa de la nube que impulsa un Security Service Edge (SSE) completo para conectar usuarios, cargas de trabajo y dispositivos sin ponerlos 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 pueden evitar la pérdida de datos.

© 2025 Zscaler, Inc. Todos los derechos reservados.

Zscaler protege a la fuerza de trabajo: Acceso seguro, rápido y confiable a aplicaciones.

Implementable en días para mejorar la ciberprotección y la experiencia del usuario.



Protección superior frente a amenazas y datos,
gran experiencia de usuario, reducción de costos y complejidad

Especificaciones técnicas

Componente de Zscaler	Plataformas y sistemas compatibles	
Client Connector	iOS 17 o posterior Android 9 o posterior Windows 8 o posterior	ChromeOS versión 137 o posterior Linux MacOS 14 o posterior
Acceso sin cliente	Navegadores web modernos: (compatibles con HTML 5), Chrome, Edge, FireFox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Servicio de Perímetro Privado	AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat	
Controlador de nube privada	AWS, Microsoft Azure, VMware, Red Hat	

zscaler™ | Experience your world, secured.™

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

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas registradas o marcas de servicio o (ii) marcas registradas o marcas de servicio de Zscaler, Inc. en los Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

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