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.

Las estrategias de seguridad de red tradicionales no satisfacen las necesidades de su fuerza laboral 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 laboral híbrida y de terceros aumenta el riesgo cibernético, 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 ThreatLabz 2025, el 92 % de los encuestados comparte la preocupación de que los fallos de VPN sin revisar conducen directamente a incidentes de ransomware, lo que destaca lo difícil que es aplicar revisiones a las VPN de manera continua y a tiempo.

Ventajas:

- **Reemplace las soluciones de VPN vulnerables.** Reduzca la superficie de ataque y elimine el movimiento lateral conectando a los usuarios directamente con las aplicaciones (no con la red), fortaleciendo así su postura de seguridad.
- **Prevenir 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 fuerza laboral híbrida** Amplíe sin inconvenientes el acceso ultrarrápido a aplicaciones privadas entre usuarios, sede central, sucursales y terceros.
- **Reduzca la complejidad operativa.** Ofrezca un acceso seguro y optimizado, sin productos puntuales costosos y complejos, mediante una plataforma ZTNA unificada y nativa en la nube para usuarios, cargas de trabajo y entornos OT/IT

©2025 Zscaler, Inc. Todos los derechos reservados.

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 cómo redefinimos la seguridad de las aplicaciones privadas con una nueva solución Zero Trust Network Access (ZTNA).

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
- **Ofrezca una experiencia de usuario superior:** conectar a los usuarios directamente a aplicaciones privadas elimina el retorno lento y costoso a través de VPN tradicionales mientras supervisa continuamente y resuelve de manera proactiva los problemas de experiencia del usuario.

El 92% de los encuestados comparte la preocupación de que los fallos de VPN sin revisar conducen directamente a incidentes de ransomeware, lo que destaca lo difícil que es aplicar revisiones a las VPN de manera continua y a tiempo.

Informe de riesgos de VPN de Zscaler ThreatLabz 2025

*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

©2025 Zscaler, Inc. Todos los derechos reservados.

Casos de uso clave

Acceso remoto seguro (sustitución de VPN).
Las VPN en la nube o basadas en dispositivos lo exponen a ciberataques. Están plagadas de vulnerabilidades y son explotadas con frecuencia 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.

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 proporciona acceso rápido y directo a

a aplicaciones a través de más de 160 puntos de presencia (PoP) distribuidos globalmente sin los riesgos de seguridad inherentes a las 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 aplicaciones conectadas a la red, como Voz sobre IP (VoIP) y aplicaciones de servidor a cliente, e incluso aplicaciones 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 laboral 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 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.

BYOD 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, actividades 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 costes 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.

El acceso remoto con privilegios para
empleados de OT/IT y proveedores externos es esencial, ya que necesitan acceder regularmente a los activos

©2025 Zscaler, Inc. Todos los derechos reservados.

de OT/IT para maximizar el tiempo de actividad de la producción y evitar interrupciones derivadas de fallos en equipos y procesos. ZPA permite un acceso rápido, seguro y fiable a entornos de OT/IT desde ubicaciones de campo, la planta de producción o cualquier otro lugar. ZPA para OT/IT ofrece acceso remoto a sistemas internos RDP, SSH y VNC totalmente aislado y sin cliente, sin que los usuarios tengan que instalar ningún software en sus dispositivos ni depender de jump hosts o VPN heredadas.

Alternativa 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 endpoints 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.

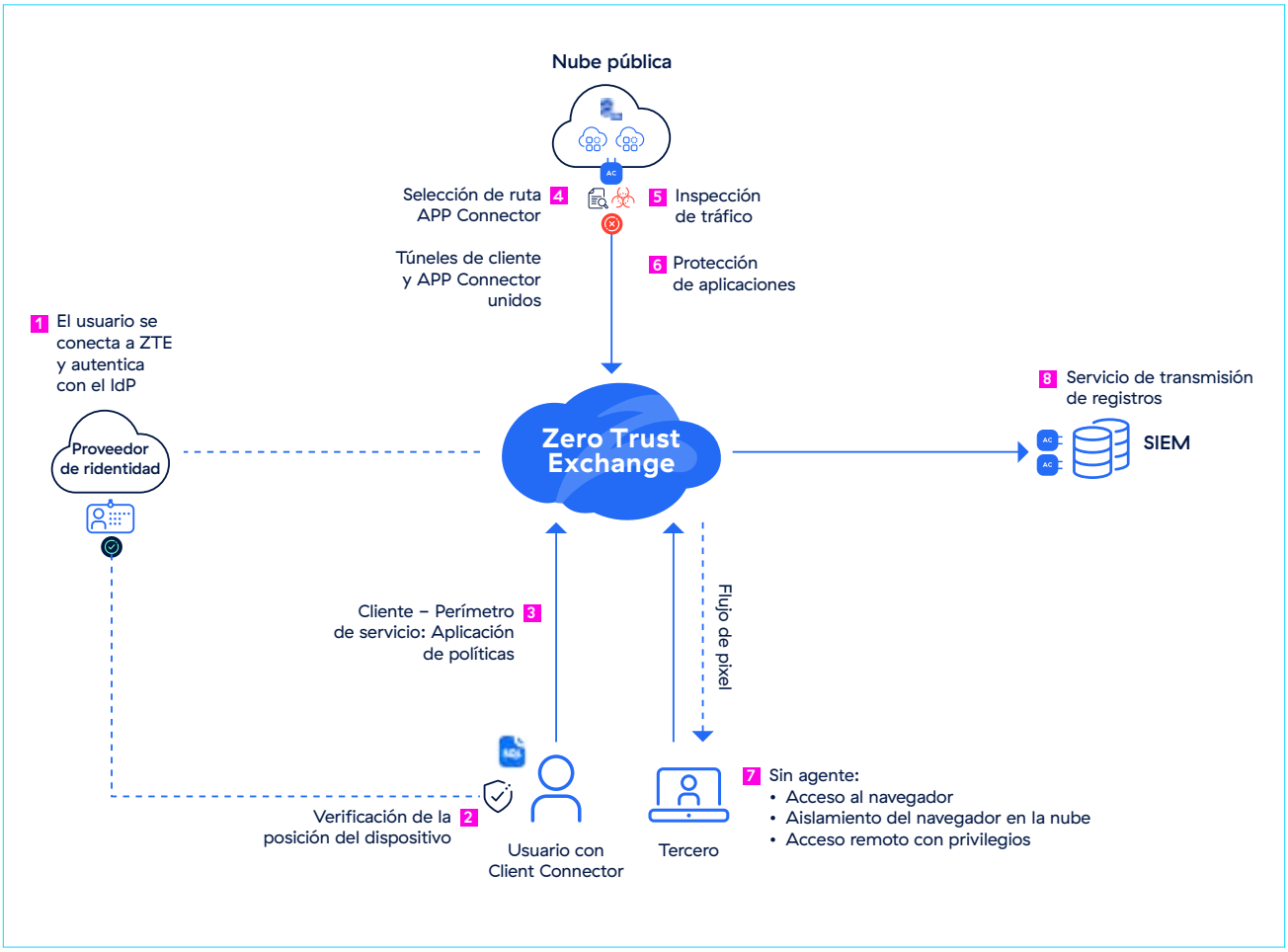
ZPA es una alternativa eficaz a VDI que ofrece acceso seguro, sin agentes y basado en navegador en dispositivos no administrados. Los usuarios obtienen acceso rápido y sin inconvenientes a aplicaciones privadas gestionadas por el perímetro de servicio más cercano. La arquitectura ZPA proporciona acceso 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 (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 brecha 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 entre usuarios y aplicaciones, junto con una solución sólida para implementar políticas coherentes a escala y eliminar el movimiento lateral de amenazas. Automatiza todo el ciclo de vida de la segmentación al ver cada aplicación a través del descubrimiento, segmentando más rápido con recomendaciones impulsadas por 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, 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

©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 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

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 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.
Segmentación autónoma de usuarios a aplicaciones	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 IA y fortaleciendo su postura con información en vivo. Impulsada por modelos ML entrenados continuamente en millones de señales de clientes y sus patrones únicos de acceso a aplicaciones, la segmentación autónoma de usuario a aplicación puede ayudarlo a eliminar el movimiento de amenazas laterales, acelerar su recorrido ZTNA y simplificar y escalar las operaciones Zero Trust.
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.
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.
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.
Acceso seguro a aplicaciones S2C heredadas	Habilite el acceso seguro a aplicaciones conectadas a redes heredadas, como VoIP, Follow me printer y aplicaciones de servidor a cliente.
Acceso a aplicaciones B2B	Habilite el acceso seguro bidireccional 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 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 cliente proporciona a los contratistas externos y a los usuarios BYOD acceso sin inconvenientes a las aplicaciones desde cualquier dispositivo y navegador web.
ZTNA en la oficina	Implemente ZTNA para usuarios en la oficina que utilizan bordes de servicio privados ZPA, lo que garantiza un acceso rápido y sin inconvenientes a las aplicaciones. Nustro 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 comercial totalmente administrada o alojada por el cliente.

Ventajas

Minimiza 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 el descubrimiento de aplicaciones, lo que reduce aún más la superficie de ataque.

Eliminación del movimiento lateral.
La conectividad basada en el acceso con privilegios mínimos garantiza que el acceso a las aplicaciones se otorgue individualmente, 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.

Prevenga 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 revisiones virtuales contra vulnerabilidades de día cero. ZPA minimiza los riesgos de terceros 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 en 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.

©2025 Zscaler, Inc. Todos los derechos reservados.

Acceso privado a Zscaler (ZPA): Múltiples opciones para comenzar

	Plataforma Zscaler Essentials (ZS-ESS-PLATFORM)	Plataforma sin cliente de ZPA (ZPA-CLIENTLESS-PLATFORM)	Plataforma de acceso privado de Zscaler (ZS-ZPA-PLATFORM)	Plataforma Zscaler (ZS-PLATFORM)
Servicios de la plataforma de acceso privado				
Control de acceso granular por usuario, grupo y puertos	✓ 1 usuario por cada 20 suscritos (500 usuarios suscritos como mínimo)	✓	✓	✓
Servicio de transmisión de registros				
Supervisión continua del estado de todas las aplicaciones				
Anclaje de IP de origen: reenvíe selectivamente el tráfico de la aplicación a los servidores de destino adecuados				
Conector de aplicaciones: máquina virtual ligera que permite conexiones internas a Zscaler ZTE	Tantos como sean necesarios, hasta el máximo del sistema	Tantos como sean necesarios, hasta el máximo del sistema	Tantos como sean necesarios, hasta el máximo del sistema	Tantos como sean necesarios, 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 VPN Service Edges (mínimo 50 usuarios)	Complemento VPN Service Edges (mínimo 50 usuarios)
Nube de continuidad empresarial 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 y análisis autónomos de usuario a aplicación	–	–	**Complemento**	**Complemento**
Acceso de terceros			Complemento (Mín: 500 usuarios)	Complemento (Mín: 500 usuarios)
Acceso basado en navegador para dispositivos no administrados	–	✓	✓ Se pueden comprar licencias de usuarios invitados adicionales con ZPA-CLIENTLESS-PLATFORM	✓ Se pueden comprar licencias de usuarios invitados adicionales con ZPA-CLIENTLESS-PLATFORM
Portal de usuario: portal web único para que los usuarios accedan a aplicaciones autorizadas y consolas privilegiadas				
Estándar de acceso remoto privilegiado: PRA sin cliente para sistemas OT (hasta 10) (RDP/SSH/VNC)				
Aislamiento de navegador para aplicaciones SaaS/privadas		**Complemento**	**Complemento**	**Complemento**
Supervisión de la experiencia digital	–	–	✓	✓
Estándar ZDX: visibilidad del usuario, la conectividad y la telemetría de la aplicación				
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		–	✓ (Mínimo 500 usuarios)	✓ (Mínimo 500 usuarios)
AppProtection para proteger aplicaciones privadas de OWASP Top 10 y la inspección del tráfico web		**Complemento**	**Complemento**	**Complemento**

©2025 Zscaler, Inc. Todos los derechos reservados.

Diferenciadores clave

Como la primera solución ZTNA del sector impulsada por IA, ZPA ofrece una 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, 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, 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 seguro al navegador:** Aproveche el acceso basado en navegador para terceros 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 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

Zscaler nombrado líder en el Gartner® Magic Quadrant™ 2025 para Security Service Edge

Más información

**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.

©2025 Zscaler, Inc. Todos los derechos reservados.

Componentes fundamentales

Conector de Cliente de Zscaler:
El conector de cliente es una aplicación ligera que se ejecuta en los portátiles 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 forma segura a aplicaciones, cargas de trabajo y dispositivos OT a través del acceso integrado basado en navegador (Web, RDP, SSH, VNC) o el aislamiento del navegador Zscaler para acceso sin cliente en dispositivos no administrados.

Conector de aplicaciones ZPA
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.

Conector de red ZPA
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 bordes de servicio VPN en Zscaler Cloud con un túnel de adentro hacia afuera.

Bordes de servicio ZPA
Los bordes de servicio aplican políticas de seguridad y acceso, integrando la conexión interna y externa entre un usuario autorizado (mediante el conector de cliente y el acceso al navegador) y una aplicación privada específica (mediante el conector de aplicaciones). La mayoría de los clientes utilizan nuestros bordes 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 bordes 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 en las instalaciones sin salir de la red local. Además, garantizan la continuidad del negocio con acceso ininterrumpido a aplicaciones críticas, incluso durante un evento de cisne negro.

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

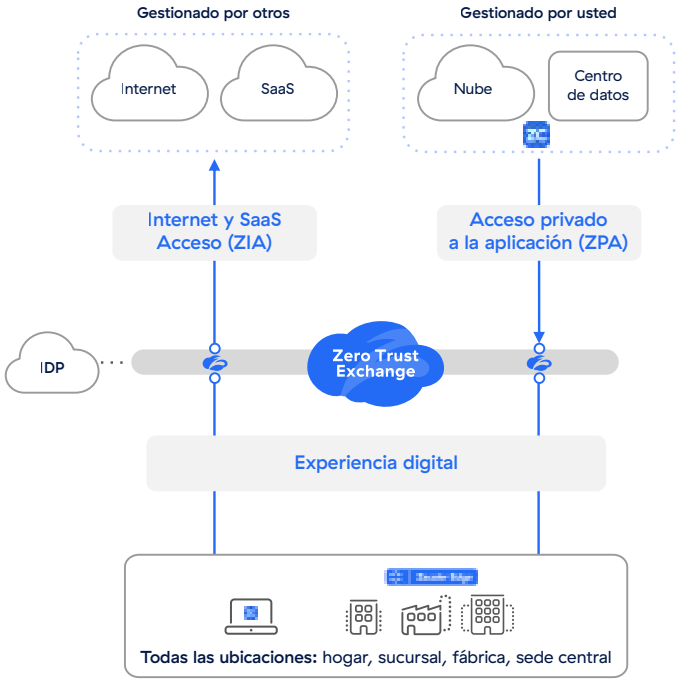
ZPA forma parte de la plataforma holística Zero Trust Exchange

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.

©2025 Zscaler, Inc. Todos los derechos reservados.

Zscaler protege a la fuerza laboral: acceso seguro, rápido y confiable a aplicaciones.

Implementable en días para mejorar la protección cibernética y la experiencia del usuario.



Protección superior de datos y amenazas,
excelente experiencia de usuario, coste y complejidad reducidos

Especificaciones técnicas

Componente 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
Clientless Access	Navegadores web modernos: (compatibles con HTML 5), Chrome, Edge, FireFox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Private Service Edge	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, 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. Distribuida 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**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas comerciales mencionadas en **zscaler.es/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas 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.

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