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.

Los enfoques de seguridad de red tradicionales no satisfacen las necesidades de su fuerza de trabajo híbrida y de su empresa.
Los firewalls 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 su fuerza de trabajo híbrida y el acceso de terceros aumenta el ciberriesgo, 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.

Para 2025, al menos el 70 % de las nuevas implementaciones de acceso a distancia serán principalmente de acceso a la red Zero Trust (ZTNA) a diferencia de los servicios de VPN, que aumentaron 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.
- **Evite los ciberataques**
  Minimice el riesgo de una violación con la protección de aplicaciones privadas frente a las amenazas web y de identidad, la protección avanzada frente a amenazas con inspección completa en línea y la prevención de la pérdida de datos.
- **Potencie su fuerza de trabajo híbrida**
  Amplíe fácilmente el acceso ultrarrápido a las aplicaciones privadas entre los 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 y OT/TI.

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 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.

Para 2025, al menos el 70 % de las nuevas implementaciones de acceso a distancia serán principalmente de acceso a la red Zero Trust (ZTNA) a diferencia de los servicios de VPN, que aumentaron menos del 10 % a finales de 2021.*

— Gartner®

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

Casos importantes de uso

Acceso remoto seguro (reemplazo de VPN)
Las VPN basadas en dispositivos o en la nube lo dejan expuesto a ciberataques. 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.

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 un acceso rápido y directo 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 las 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) 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
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 heredados. Las organizaciones necesitan acceso ininterrumpido a las aplicaciones, sin comprometer la seguridad Zero Trust durante desastres o períodos de acceso degradado a la infraestructura. Se deben cumplir los estándares regulatorios y de cumplimiento para 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 externo dependía de soluciones costosas, complejas y riesgosas como VDI, RDP, SSH o VNC, que conectaban a los usuarios directamente a 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 a los activos OT/TI con regularidad para maximizar el tiempo de actividad de la producción, así como para evitar interrupciones por fallas en los equipos y procesos. ZPA permite un acceso rápido, seguro y confiable a los entornos OT/TI en el campo, la planta de producción o cualquier otro lugar. ZPA para OT/TI proporciona un acceso de escritorio remoto totalmente aislado y sin clientes a sistemas de destino RDP, SSH y VNC internos, sin necesidad de que los usuarios instalen un cliente en su dispositivo mediante hosts de salto y VPN heredadas.

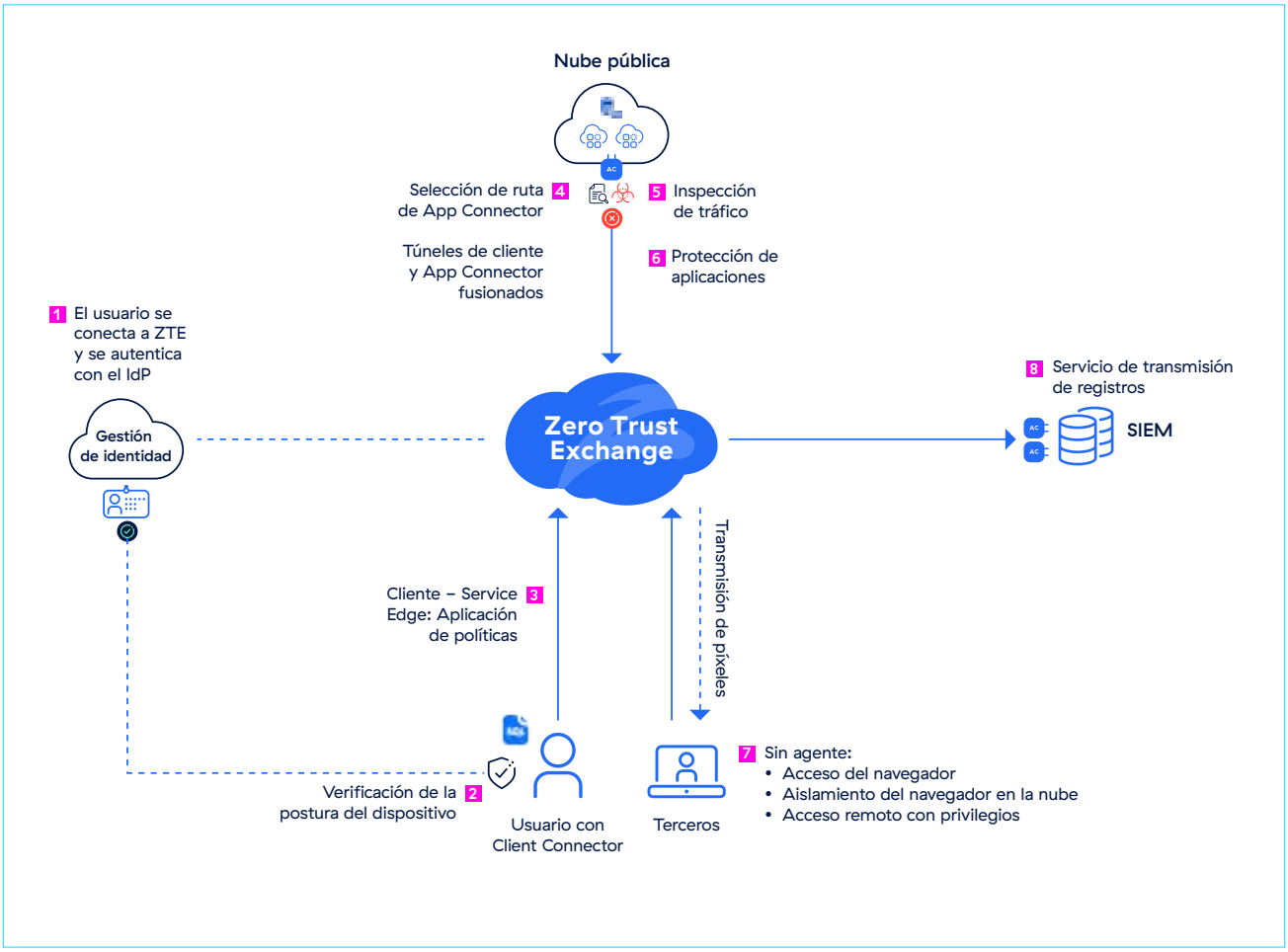
Alternativa a la VDI
Los equipos de TI y de seguridad carecen de control sobre los dispositivos no gestionados, lo que genera riesgos para el negocio. Para permitir el acceso a las aplicaciones en dispositivos no gestionados, tradicionalmente las organizaciones han recurrido a las VDI. Las VDI colocan a los usuarios directamente en la red, exponiendo las aplicaciones internas a puntos finales no gestionados. Además, las VDI son caras, complicadas de gestionar y no son escalables. A raíz de la transformación digital, las aplicaciones modernizadas suelen estar basadas en la web o en navegadores, y la transmisión de un escritorio completo a través de VDI ofrece una experiencia de usuario final deficiente.

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 sólo 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
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. Dicho esto, la implementación de la segmentación requiere reglas de firewall complejas que son difíciles de mantener, a menudo interrumpen las aplicaciones y pueden complicar el acceso para los usuarios de VPN. En las grandes organizaciones, esto a menudo requiere alta disponibilidad, enrutamiento complejo y enlaces privados costosos.

La segmentación de aplicaciones impulsada por la 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, 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.

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

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.
Acceso unificado de 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 rápido Zscaler Client Connector. El acceso sin clientes proporciona a los usuarios no administrados un acceso sin interrupciones a la aplicación desde cualquier dispositivo y navegador web.
Browser Access	Permita que los usuarios con equipos propios y de terceros utilicen libremente sus dispositivos para acceder sin problemas y de manera segura a las aplicaciones internas aprovechando cualquier navegador web, sin necesidad de usar un cliente.
ZTNA en el campus	Experimente ZTNA para usuarios en el campus, conectando a los usuarios de manera segura a las aplicaciones de sus oficinas. Un 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 las aplicaciones de misión crítica incluso durante un evento de cisne negro con una solución de continuidad empresarial controlada por el cliente o totalmente gestionada, creando la ruta de acceso a las aplicaciones privadas críticas a través del Private Service Edge de ZPA.
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 aplicaciones con IA	Aplique las recomendaciones de segmentación basadas en el aprendizaje automático que se le ofrecen automáticamente en ZPA, lo que hace que sea rápido y fácil identificar los segmentos de aplicaciones adecuados y crear las políticas de acceso correctas. Gracias a los modelos de aprendizaje automático (ML) que se entrenan continuamente con millones de señales de clientes y sus patrones únicos de acceso a aplicaciones, la segmentación basada en ML puede minimizar su superficie de ataque interna.
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.
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 los 10 principales de OWASP, y las vulnerabilidades emergentes de día cero que pueden eludir los controles tradicionales de seguridad de la red.

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.
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.
Identidad e inicio de sesión único (SSO)	Intégrelo fácilmente con su infraestructura de identidad y autenticación existente, aprovechando el SSO para reducir aún más la complejidad.
Acceso seguro a aplicaciones de la red	Habilite el acceso seguro a aplicaciones conectadas a redes heredadas, como VoIP y aplicaciones de servidor a cliente.
Conectividad IPsec	Permita el acceso Zero Trust a las aplicaciones de socios comerciales y proveedores (Aplicación Extranet) alojadas en sus redes

Ventajas

Minimice la superficie de ataque
Eliminar las VPN vulnerables y hacer que las aplicaciones sean invisibles a Internet imposibilita que los usuarios no autorizados puedan encontrarlas y atacarlas. ZPA crea un segmento de uno entre un usuario autorizado y una app privada específica, eliminando toda conectividad entrante y permitiendo solo conexiones de dentro hacia fuera a través de microtúneles cifrados a los dispositivos de los usuarios. Los administradores pueden descubrir y segmentar automáticamente las aplicaciones, servicios y cargas de trabajo no autorizadas mediante el descubrimiento 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 conceda de manera individual de 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. Como el ZPA no se basa en direcciones IP, se elimina la necesidad de configurar y gestionar una compleja segmentación de la red, listas de control de acceso (ACL), políticas de firewall o traducciones de direcciones de red.

Evite los usuarios comprometidos, las amenazas internas y los 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 protección integral contra las técnicas más prevalentes, incluido el Top 10 de OWASP, y compatibilidad total con firmas personalizadas para la aplicación inmediata de parches virtuales contra las vulnerabilidades de día cero.

Ofrezca una experiencia de usuario excepcional
Una conectividad rápida y uniforme que no requiera entrar y salir de los clientes VPN ofrece a los usuarios remotos una experiencia de acceso más segura y eficaz. Los contratistas, proveedores y socios externos se benefician de un acceso sin interrupciones 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 de manera proactiva los problemas de rendimiento de los usuarios finales causados por dificultades de acceso a aplicaciones privadas, interrupciones de la ruta de red o congestión de la red.

Una plataforma unificada para el acceso seguro a través de aplicaciones, cargas de trabajo y dispositivos
Extienda Zero Trust a través de aplicaciones privadas y dispositivos 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.

Opciones de paquetes de Zscaler Private Access

	Plataforma Zscaler Essentials (ZS-ESS-PLATFORM)	Platforma Zscaler Private Access (ZS-ZPA-PLATFORM)	Plataforma Zscaler (ZS-PLATFORM)
Servicios de la plataforma Private Access	comprobar 1 usuario por cada 20 usuarios suscritos (Mín: 500 usuarios suscritos)	comprobar	comprobar
Control de acceso granular por usuario, grupo y puertos			
Servicio de transmisión de registros			
Supervisión continua de la salud 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 para terceros	$	comprobar PRA para más de 500 usuarios	comprobar PRA para más de 500 usuarios
Acceso basado en el navegador			
Portal del usuario			
Estándar de acceso remoto privilegiado (PRA, por sus siglas en inglés)			
Supervisión de la experiencia digital	$	comprobar	comprobar
Estándar ZDX			
Seguridad para aplicaciones privadas	$	$	comprobar Capacidades de engaño para más de 500 usuarios
Protección de datos para aplicaciones privadas			
Gestión de riesgos: Engaño			
Segmentación	20 segmentos de aplicación (10 reg/ 90 días, revisión retrospectiva limitada)	20 segmentos de aplicación (10 reg/ 90 días, revisión retrospectiva limitada)	20 segmentos de aplicación (10 reg/ 90 días, revisión retrospectiva limitada)
Segmentos de aplicaciones y vista previa de segmentación			
Complemento de segmentación	comprobar 100 reg/ 14 días Informes semanales a la carta, descargue y analice hasta 30 días de datos Importe aplicaciones del sistema interno o de fuentes externas (Qualys, Tenable, ServiceNow)	comprobar 100 reg/ 14 días Informes semanales a la carta, descargue y analice hasta 30 días de datos Importe aplicaciones del sistema interno o de fuentes externas (Qualys, Tenable, ServiceNow)	comprobar 100 reg/ 14 días Informes semanales a la carta, descargue y analice hasta 30 días de datos Importe aplicaciones del sistema interno o de fuentes externas (Qualys, Tenable, ServiceNow)
Segmentos de aplicación ilimitados			
Segmentación impulsada por la IA			
Información de segmentación			
Importación de segmentos de aplicaciones (desde archivos de datos estructurados)			
Complemento AppProtection	Complemento	Complemento	Complemento
Visibilidad de ataques a aplicaciones			
Top 10 de defensa de OWASP: Inyección SQL, scripting 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 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.
- **Permita la continuidad empresarial global sin comprometer la seguridad:** Minimice el impacto de las interrupciones y aplique el acceso Zero Trust para cumplir los estrictos requisitos de cumplimiento incluso cuando la nube de Zscaler sea inaccesible.
- **Acceso sin cliente:** Aproveche el acceso basado en navegador para terceros con DLP integrado
- **Elimine el movimiento lateral con segmentación potenciada 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.
- **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®, 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.

Componentes básicos

Zscaler Client Connector
Es una aplicación ligera que se ejecuta en las computadoras portátiles y dispositivos móviles de los usuarios. Al reenviar 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.

Zscaler Clientless Access
Los usuarios pueden conectarse de manera 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 el acceso sin cliente en dispositivos no administrados.

ZPA App Connector
Los conectores de aplicaciones son máquinas virtuales rápidas que se encuentran al frente de las aplicaciones privadas implementadas en el centro de datos o en la nube pública, y actúan de intermediarios de 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.

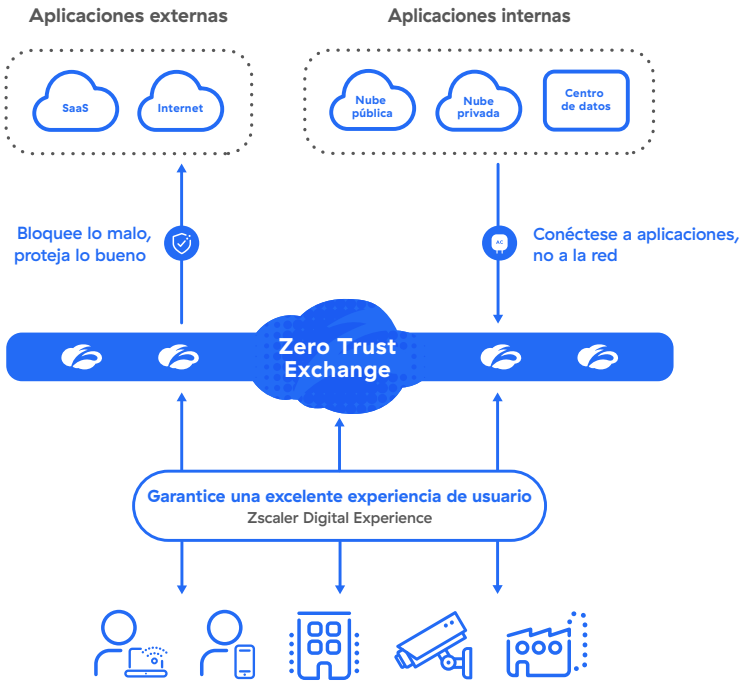
ZPA Service Edges
Los Service Edges aplican las políticas de seguridad y acceso, cohesionando la conexión de dentro a fuera entre un usuario autorizado (a través de Client Connector y Browser Access) y una aplicación privada específica (a través de App Connector). La mayoría de los clientes utilizan nuestros Public Service Edges, que están alojados en más de 160 puntos de presencia en todo el mundo y gestionan millones de usuarios simultáneos para las mayores organizaciones del mundo. Los Private Service Edges, gestionados por Zscaler, también están disponibles para ser alojados in situ con el fin de ofrecer a los usuarios locales el camino más corto a las aplicaciones locales sin salir de la red local. También garantiza la continuidad empresarial con un acceso ininterrumpido a las aplicaciones de misión crítica, incluso durante un evento de cisne negro.

ZPA forma parte del intercambio integral 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.

Cómo Zscaler ofrece Zero Trust para los usuarios, las cargas de trabajo y la OT/IT

Implemente en semanas para mejorar la ciberprotección y la experiencia del usuario



Cualquier usuario, cualquier dispositivo, cualquier aplicación, cualquier ubicación

Especificaciones técnicas

Componente de 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
Acceso sin cliente	Navegadores web modernos: (Admiten HTML 5)	Chrome Edge FireFox
App Connector	AWS Centos, Oracle y Red hat Microsoft Azure	Microsoft Hyper-V VMware vCenter o vSphere Hypervisor Host de docker

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, fuertes 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**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134

zscaler.com/mx