Ficha de datos

Zscaler Private Access™

Proporcione a sus empleados un acceso rápido, seguro y fiable a aplicaciones privadas con la primera y única ZTNA de nueva generación del sector.

Zscaler redefine el acceso a las aplicaciones privadas con conectividad avanzada, segmentación y capacidades de seguridad para proteger su empresa de las amenazas a la vez que brinda una excelente experiencia de usuario.

Las redes y los modelos de seguridad heredados no satisfacen las necesidades de la fuerza de trabajo híbrida actual.

Conectar a los usuarios con aplicaciones privadas no debería ser lento, complicado ni arriesgado. El trabajo híbrido y la transformación en la nube han trastocado los modelos de seguridad de red basados en el perímetro, con aplicaciones privadas que se trasladan a la nube y usuarios que acceden a las aplicaciones a través de la Internet pública, en cualquier dispositivo y desde cualquier lugar. Los modelos tradicionales que se basan en VPN y firewalls heredados para controlar el acceso a las aplicaciones se han vuelto ineficaces en un mundo en el que predomina la nube y la movilidad.

Para 2025, al menos el 70 % de las nuevas implementaciones de acceso remoto se realizarán principalmente mediante el acceso a redes de confianza cero (ZTNA), en lugar de los arcaicos servicios VPN, lo que supone un aumento del 10 % con respecto a los datos de finales de 2021, según Gartner.

Beneficios:

- **Aumente la productividad de la fuerza de trabajo híbrida**
  Obtenga un acceso rápido y sin interrupciones a las aplicaciones privadas tanto si está en casa como en la oficina o en cualquier otro lugar
- **Mitigue el riesgo de una violación de datos**
  Minimice la superficie de ataque y el movimiento lateral haciendo que las aplicaciones sean invisibles a Internet al tiempo que aplica el acceso con la menor cantidad de privilegios
- **Detenga a los adversarios más avanzados**
  La protección de aplicaciones privadas de primera clase y la inspección completa del tráfico en línea minimizan el riesgo de usuarios afectados y atacantes activos
- **Extienda la confianza cero a aplicaciones, cargas de trabajo y dispositivos**
  La plataforma ZTNA más completa del mundo proporciona acceso con la la menor cantidad de privilegios a aplicaciones privadas, cargas de trabajo y dispositivos OT/IIoT
- **Reduzca la complejidad operativa**
  Nuestra plataforma nativa en la nube elimina las soluciones de acceso remoto heredadas, como las VPN que son difíciles de escalar, gestionar y configurar

Los atacantes pueden burlar fácilmente los modelos de seguridad de red heredados aprovechando la confianza inherente y el acceso excesivamente permisivo de las arquitecturas tradicionales de castillo y foso, 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 sensibles.
- **Los usuarios en peligro y las amenazas internas pueden eludir los controles tradicionales:** los atacantes avanzados pueden robar credenciales y alterar la identidad para tener acceso a aplicaciones privadas con herramientas de acceso a distancia heredadas y ofertas ZTNA de primera generación.

Es hora de replantearnos cómo conectamos de forma segura y constante a los usuarios con las aplicaciones que necesitan y redefinir la seguridad de las aplicaciones privadas con una nueva generación de ZTNA.

Zscaler Private Access™ (ZPA)

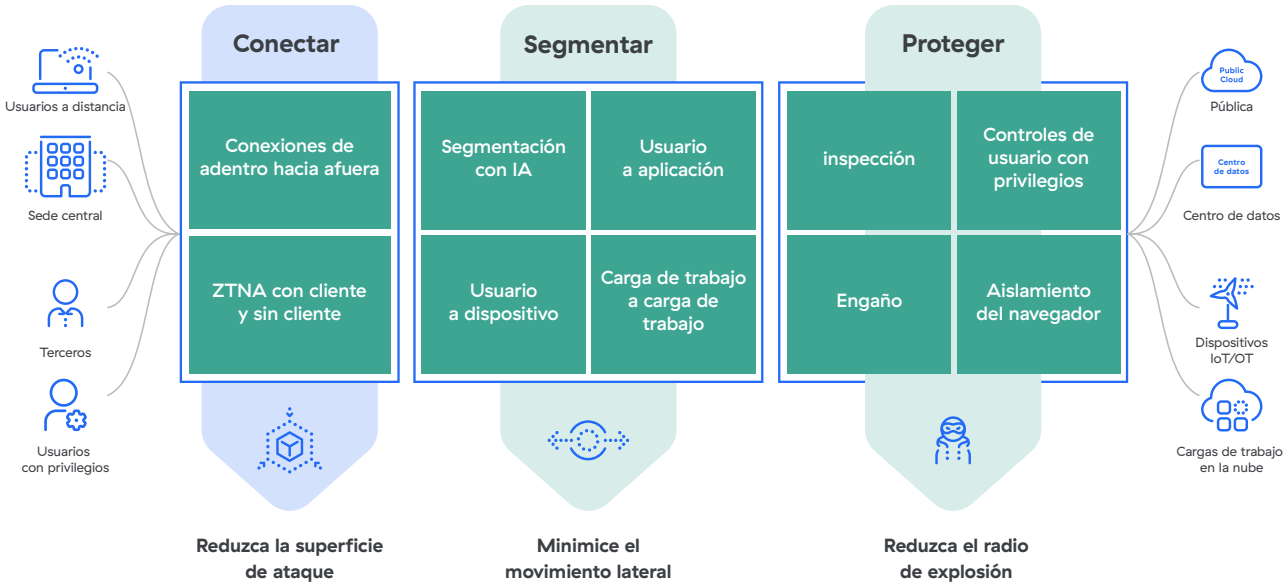
ZPA es la plataforma de ZTNA más implementada del mundo, que aplica el principio de privilegio mínimo para brindar a los usuarios una conectividad segura y directa a las aplicaciones privadas que se ejecutan en las instalaciones o en la nube pública, al tiempo que elimina el acceso no autorizado y el movimiento lateral. ZPA es un servicio 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:

- **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 forma proactiva los problemas de experiencia del usuario.
- **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.
- **Imponer un acceso con privilegios mínimos:** El acceso a las aplicaciones se determina por identidad y contexto, no por una dirección IP, y nunca se pone a los usuarios en 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.
- **Detectar usuarios y dispositivos afectados:** Los señuelos integrados funcionan para identificar y eliminar rápidamente usuarios y dispositivos maliciosos.

En 2025, al menos el 70 % de las nuevas implementaciones de acceso a distancia serán principalmente de acceso a la red de zero trust (ZTNA).

— Gartner

Cómo resuelve la ZPA los nuevos casos de uso de la ZTNA



Casos importantes de uso

Alternativa a las VPN

Las VPN no se diseñaron pensando en la seguridad, la escalabilidad o la experiencia del usuario. Tradicionalmente, las VPN transportan todo el tráfico de retorno de usuarios remotos a centros de datos que pueden estar a miles de kilómetros de distancia, lo que provoca latencia y frustración en los usuarios. Una vez conectadas, los usuarios de las VPN pasan por el firewall y se sitúan en la misma red que sus aplicaciones, lo que permite un movimiento lateral libre.

La ZPA supera estos problemas proporcionando un acceso rápido y directo a las aplicaciones a través de más de 150 puntos de presencia (PoP) distribuidos por todo el mundo, sin los riesgos de seguridad inherentes a las VPN. Su conectividad de dentro hacia fuera garantiza que el acceso a las aplicaciones esté desacoplado del acceso a la red, a la vez que elimina la huella que deja en Internet. ZPA conecta a los usuarios con las aplicaciones, no con las redes, y los usuarios solo pueden acceder a las aplicaciones especificadas, sin posibilidad de moverse lateralmente. 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.

Fuerza de trabajo híbrida segura

El personal moderno trabaja desde sus hogares y otras ubicaciones remotas, sucursales y oficinas centrales, lo que supone un problema para los paradigmas de seguridad heredados. ZPA permite un acceso fluido y seguro a las aplicaciones privadas desde donde necesiten trabajar, en cualquier dispositivo. Los usuarios del campus se benefician de una experiencia idéntica a través de ZPA Private Service Edge.

ZPA Private Service Edge le permite desplegar la potencia de la nube en sus instalaciones, aplicando los mismos controles de seguridad que sus usuarios remotos con el mismo alto rendimiento. ZPA puede ofrecer ahora capacidades ZTNA universales para una experiencia de usuario rápida y uniforme. Además, con el monitoreo de la experiencia digital, obtiene visibilidad en tiempo real

de la degradación del rendimiento y las interrupciones, lo que permite un trabajo híbrido productivo. Al formar parte de Zscaler Zero Trust Exchange™, los usuarios se benefician de una plataforma SSE integrada para un acceso seguro, rápido y directo a Internet, SaaS, cargas de trabajo, dispositivos y aplicaciones privadas.

Acceso de terceros/Alternativa VDI
En el pasado, el acceso de terceros dependía de una infraestructura de escritorio virtual (VDI) complicada y costosa u otros clientes de escritorio remoto, como RDP, SSH o VNC, que ponían a los usuarios directamente en su red y exponían los sistemas internos a dispositivos no fiables. Las capacidades de acceso sin clientes de ZPA hacen que el acceso de terceros sea tan sencillo como acceder a la web, al tiempo que reducen los costos y minimizan los riesgos. Sus proveedores, contratistas y socios pueden utilizar libremente cualquier navegador web desde sus propios dispositivos para conectarse a los sitios web de la intranet, los sistemas internos y los equipos, sin necesidad de clientes. ZPA mantiene a los usuarios externos y a los dispositivos no administrados aislados de su red y sus aplicaciones, garantizando que los datos confidenciales nunca estén fuera de su control y que estén protegidos de las operaciones de copia/pegar, impresión y carga/descarga no autorizadas. Con el acceso sin cliente, el departamento de TI puede ofrecer una experiencia mejor y más segura a los usuarios sin incurrir en los costos de gestión de la VDI heredada.

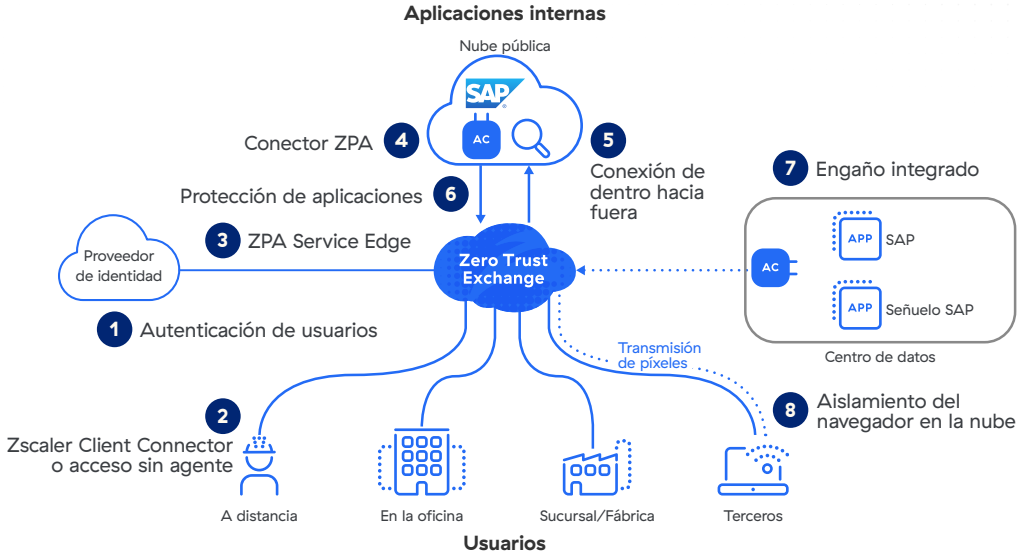
Fusiones y adquisiciones y desinversiones
Las fusiones y adquisiciones y las desinversiones a menudo requieren combinar redes, lo que puede suponer una dificultad debido al solapamiento del espacio de propiedad intelectual y a la creación de firewalls entre las dos entidades. ZPA acelera drásticamente la integración y el tiempo de creación de valor tras las fusiones y adquisiciones, acelerando el proceso a cuestión de semanas en lugar de meses. Proporciona un acceso sin interrupciones a las aplicaciones privadas (sin necesidad de VPN) y elimina la necesidad de fusionar varias redes o de adquirir equipos de red adicionales, lo que libera recursos para centrarse en el trabajo de alto impacto.

Acceso seguro del operador para OT e IIoT
Los empleados y proveedores externos necesitan acceder a los activos de OT e IIoT con regularidad para maximizar el tiempo de actividad de la producción, así como para evitar interrupciones por fallos en los equipos y procesos. ZPA permite un acceso rápido, seguro y fiable a los entornos OT e IIoT desde ubicaciones sobre el terreno, la planta de producción o cualquier otro lugar. ZPA para IoT y OT 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.

Conectividad segura de carga de trabajo a carga de trabajo
Las organizaciones modernas requieren una conectividad rápida y segura de carga de trabajo a carga de trabajo a través de entornos privados, híbridos y de múltiples nubes. ZPA para Cargas de Trabajo reduce la complejidad operativa y los costos al tiempo que establece una conectividad basada en la confianza cero para las cargas de trabajo en todos estos entornos. Como las cargas de trabajo se ocultan tras ZPA, son invisibles a Internet e imposibles de atacar.

Conectividad de sucursales de confianza cero
La conectividad de sucursales de confianza cero conecta de forma segura sucursales, fábricas y centros de datos sin la complejidad de las VPN, garantizando un acceso de confianza cero entre usuarios, dispositivos IoT/OT y aplicaciones basado en políticas empresariales. Además, elimina la superficie de ataque y evita el movimiento lateral de amenazas conectando a los usuarios y los dispositivos IoT/OT con las aplicaciones a través del Zero Trust Exchange. La Conectividad de Sucursales de Confianza Cero simplifica drásticamente las comunicaciones de las sucursales al eliminar el enrutamiento complejo, las VPN y los firewalls, al tiempo que permite un reenvío flexible y una gestión sencilla de las políticas con el marco de políticas ZIA y ZPA de eficacia probada.

ZPA amplía el acceso con privilegios mínimos en toda la empresa



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. Autenticación del usuario con IDP utilizando sus credenciales SAML SSO existentes.
2. La postura del dispositivo del usuario se verifica con Zscaler Client Connector, un agente de reenvío ligero instalado en la computadora portátil o el dispositivo móvil del usuario. ZPA también puede incorporar la postura de los dispositivos a través de la integración de terceros con los principales proveedores de EPP/EDR/XDR (ej. CrowdStrike, Microsoft Defender, SentinelOne).
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. A continuación, ZPA Service Edge determina la aplicación más cercana al usuario y establece una conexión segura con un conector de aplicaciones, ZPA App Connector, una máquina virtual ligera instalada en el entorno que aloja los servidores y las aplicaciones.
5. ZPA Service Edge une dos túneles de salida, uno desde el conector de clientes, Client Connector, en el dispositivo y el otro desde el App Connector.
6. 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.
7. Integrated Zscaler Deception detecta a los usuarios en peligro que tienen acceso a aplicaciones señuelo y puede bloquear el acceso a los recursos internos con Zscaler Zero Trust Exchange.
8. Además, los usuarios externos pueden conectarse a aplicaciones privadas con acceso integrado basado en navegador o Zscaler Browser Isolation para acceso sin cliente en dispositivos no administrados.

Un ZPA Service Edge puede ser alojado por Zscaler en la nube (ZPA Public Service Edge) o ejecutarse in situ dentro de su infraestructura (ZPA Private Service Edge). En cualquier caso, Service Edge es administrado por Zscaler sin necesidad de ningún dispositivo

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 y las aplicaciones.
Recuperación ante desastres	Garantice un acceso ininterrumpido a las aplicaciones más importantes incluso durante un evento inesperado con una solución de continuidad empresarial controlada por el cliente que crea la ruta de acceso a aplicaciones privadas más importantes a través de ZPA Private Service Edge.
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.
Segmentación de usuario a dispositivo.	Asegúrese de que todo el acceso a los equipos y sistemas OT/IIoT se otorgue según los privilegios mínimos de segmentación de usuario a dispositivo. Permita que los proveedores externos y los usuarios remotos se conecten a los equipos desde cualquier sitio con ZPA para IoT y OT.
Segmentación de carga a carga de trabajo	Conectividad y comunicación segura de carga a carga de trabajo en entornos híbridos y multinube con ZPA for Workloads.
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.
Engaño integrado	Detecte y detenga a los atacantes más sofisticados y las amenazas internas con engaño nativo de aplicaciones que incluye la contención automatizada de usuarios en peligro en Zero Trust Exchange.
Aislamiento del navegador en la nube integrado	Proporcione acceso sin cliente y aislado físicamente a aplicaciones web más importantes a los contratistas y empleados que utilizan equipos propios. Asegúrese de que los puntos finales no administrados con vulnerabilidades o infecciones de malware no comprometan su red o aplicaciones. Aplique controles de exfiltración de datos (copiar/pegar, imprimir, cargar/descargar) para evitar la pérdida de datos confidenciales.
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.
Zero Trust SD-WAN	Conecte de forma segura sucursales, fábricas y centros de datos sin la complejidad de las VPN, garantizando un acceso de confianza cero entre usuarios, dispositivos IoT/OT y aplicaciones basadas en políticas empresariales.

Beneficios

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.

Minimice el movimiento lateral

La conectividad basada en el acceso con mínimo privilegio garantiza que el acceso a las aplicaciones se conceda de forma individual de un usuario autorizado a las aplicaciones especificadas, 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 ZPA no se basa en direcciones IP, se elimina la necesidad de configurar y gestionar una segmentación de red compleja, listas de control de acceso (ACL), políticas de firewalls o conversiones de direcciones de red. Las capacidades de engaño integradas de ZPA permiten a los equipos de seguridad detectar y aislar inmediatamente a un usuario malicioso o a un dispositivo afectado que intente desplazarse lateralmente por la organización.

Evite los usuarios comprometidos, las amenazas internas y los atacantes avanzados

La protección de aplicaciones privadas, primera en su clase, con funciones integradas de inspección en línea, engaño y prevención de pérdida de datos, minimiza el riesgo de usuarios afectados y atacantes activos. ZPA detiene automáticamente los ataques web con una cobertura completa para las técnicas más prevalentes, incluidas las 10 principales de OWASP, y compatibilidad total con firmas personalizadas para la aplicación inmediata de parches virtuales contra las vulnerabilidades de día cero. ZPA minimiza los riesgos de terceros y dispositivos BYOD con un acceso totalmente aislado a las aplicaciones que mantiene los datos confidenciales fuera de los dispositivos no administrados mediante el aislamiento integrado del navegador en la nube. La tecnología del engaño integrada que utiliza aplicaciones señuelo permite a los equipos de seguridad contener las amenazas activas en la red impidiendo que los usuarios afectados tengan acceso a los recursos.

Ofrezca una experiencia de usuario excepcional

Una conectividad rápida y constante 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 forma 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 entre aplicaciones, cargas de trabajo y dispositivos

Extienda zero trust a aplicaciones privadas, cargas de trabajo y dispositivos OT/IIoT para simplificar e integrar múltiples herramientas dispares de acceso a distancia, unificando las políticas de seguridad y acceso para detener los ataques exitosos y reducir la complejidad operativa.

Ediciones de Zscaler Private Access

	Edición ZPA Essentials	Edición ZPA Business	Edición ZPA Transformation	Edición ZPA Unlimited
Servicios de plataforma	Anclaje de la IP de origen, IdP múltiple, LSS	(+) Acceso DC ampliado	(+) Entorno de prueba, PKI del cliente	(+) Entorno de prueba, PKI del cliente
Segmentación de usuario a aplicación	10 segmentos de aplicación	500 segmentos de aplicaciones	Segmentos de aplicaciones ilimitados	Segmentos de aplicaciones ilimitados
App Connector	20 pares	50 pares	Pares ilimitados	Pares ilimitados
ZTNA en el campus[1]	1 par (virtual)	1 par de Private Service Edge por cada 5,000 usuarios	1 par de Private Service Edge por cada 2,000 usuarios	1er par de perímetros de servicio privado incluido, 1 par adicional por cada 1,000 usuarios
Acceso sin cliente[2]	—	✓	✓	✓
Supervisión integrada de la experiencia digital	—	Estándar	Estándar	Estándar
Engaño integrado	—	Estándar	Avanzado	Advanced Plus
Protección de aplicaciones	—	—	✓	✓
Aislamiento integrado	—	—	Estándar	Advanced Plus
Protección de datos (aplicaciones privadas)	—	—	—	✓
Soporte premium	—	—	—	✓

Diferenciadores clave

Zscaler Private Access es la única plataforma ZTNA de vanguardia del sector y ofrece una 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.
- **Engaño integrado:** Detenga los intentos de desplazamiento lateral y la propagación del ransomware con la única solución ZTNA con engaño nativo de aplicaciones.
- **Acceso sin clientes:** Aproveche el acceso basado en navegador para terceros con DLP integrado
- **Productividad mejorada:** Mantenga una visibilidad completa del acceso a las aplicaciones privadas para detectar los problemas de los usuarios que repercuten en su experiencia.
- **Presencia de perímetro global:** Obtenga una seguridad y una experiencia de usuario inigualables con más de 150 ubicaciones de perímetro de nube en todo el mundo, así como un perímetro de servicio local opcional para ampliar la confianza cero 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.

[1]La Edición Empresarial de ZPA admite hasta 5 pares de Private Service Edge; se requiere comprar pares adicionales después de 50,000 usuarios. La edición ZPA Transformation admite hasta 10 pares de Private Service Edge; es necesario adquirir pares adicionales después de 50,000 usuarios. La edición ZPA Unlimited admite hasta 50 pares de Private Service Edge; se requiere la compra de pares adicionales después de 50,000 usuarios.

[2]El acceso sin cliente incluye Browser Access y acceso remoto con privilegios (para hasta 10 sistemas).

- **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 extensible de confianza cero:** Proteja y potencie su empresa con Zero Trust Exchange, diseñado a partir de un marco completo de SSE.

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 Branch Connector
Está disponible en factores de forma de dispositivo físico y virtual, mejora el rendimiento de las aplicaciones eliminando el retorno y reenviando todo el tráfico de sucursales y centros de datos directamente a la ubicación de perímetro de Zscaler más cercana, minimizando la latencia. Permite la comunicación bidireccional entre usuarios, servidores y dispositivos IoT/OT (donde no se puede instalar Client Connector) y aplicaciones, a través de cualquier red mediante Zero Trust Exchange.

Zscaler Clientless Access
Los usuarios pueden conectarse de forma segura a aplicaciones, cargas de trabajo y dispositivos OT a través del acceso integrado basado en navegador (web, RDP, SSH, VNC) o Zscaler Browser Isolation para 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.

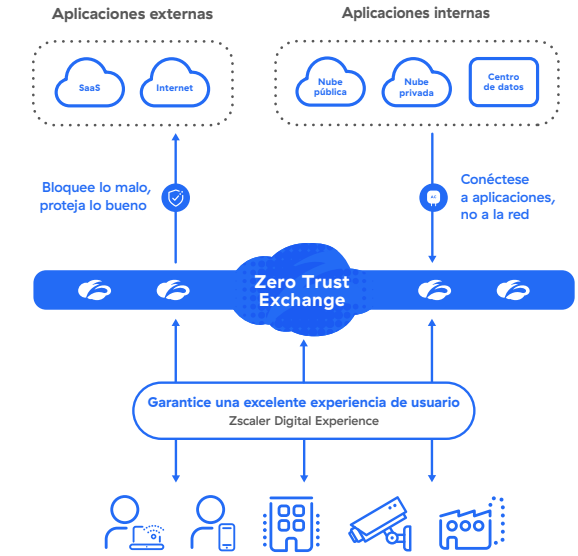
ZPA Service Edges
Los Service Edges (perímetros de servicio) aplican las políticas de seguridad y acceso, cohesionando la conexión de dentro a fuera entre un usuario autorizado (a través de Client Connector y Browser Access) y una aplicación privada específica (a través de App Connector). La mayoría de los clientes utilizan nuestros Public Service Edges, que están alojados en más de 150 centrales de todo el mundo y gestionan millones de usuarios simultáneos para las mayores organizaciones del mundo. Los Private Service Edges, administrados 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.

ZPA forma parte del intercambio integral de 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 ofrece Zscaler confianza cero para los usuarios, la carga de trabajo y la IIoT/OT

Implemente en semanas para mejorar la protección cibernética 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	macOSX 10.10 o posterior
	Android 5 o posterior	CentOS 8
	Windows 7 o posterior	Ubuntu 20.04
Branch Connector	Centos, Redhat	VMware vCenter o vSphere Hypervisor
Acceso sin cliente	Navegadores web modernos:	Chrome
	(Admiten HTML 5)	Edge
		FireFox
App Connector	AWS	Microsoft Hyper-V
	Centos, Oracle y Red hat	VMware vCenter o vSphere Hypervisor
	Microsoft Azure	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 ataques cibernéticos y pérdida de datos al conectar de forma 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. (HQ) • 120 Holger Way • San José, CA 95134 zscaler.com.mx