Ficha de datos

Zscaler Private Access™

Capacite a su personal híbrido con acceso rápido, seguro y confiable a aplicaciones privadas con el único ZTNA de próxima generación del sector.

Zscaler redefine el acceso a aplicaciones privadas con capacidades avanzadas de conectividad, segmentación y seguridad para proteger a su empresa de las amenazas y brindar una excelente experiencia de usuario.

Los enfoques de seguridad y redes heredados no satisfacen las necesidades del personal híbrido actual. Conectar usuarios a aplicaciones privadas no debería ser lento, complicado ni arriesgado. El trabajo híbrido y la transformación de la nube han trastocado los modelos de seguridad de red basados en perímetros, con aplicaciones privadas que migran a la nube y usuarios que acceden a aplicaciones a través de la Internet pública, en cualquier dispositivo y desde cualquier ubicación. Los enfoques tradicionales que se basan en VPN y cortafuegos heredados para controlar el acceso a las aplicaciones se han vuelto ineficaces en el mundo de la nube y de los dispositivos móviles.

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

Ventajas:

- **Aumente la productividad del personal híbrido** Obtenga un acceso rápido y fluido a aplicaciones privadas, tanto si está en casa, como en la oficina o en cualquier otro lugar
- **Mitigue el riesgo de una infracción de datos** Minimice la superficie de ataque y el movimiento lateral al hacer que las aplicaciones sean invisibles para Internet y al mismo tiempo imponer el acceso con menos privilegios
- **Detenga a los adversarios más avanzados** La protección de aplicaciones privadas, primera en su clase, y la inspección completa del tráfico en línea minimizan el riesgo de usuarios comprometidos y atacantes activos
- **Amplíe la seguridad de confianza cero en aplicaciones, cargas de trabajo y dispositivos** La plataforma ZTNA más completa del mundo brinda acceso con menos privilegios a aplicaciones privadas, cargas de trabajo y dispositivos OT/IIoT
- **Reduzca la complejidad operativa** Nuestra plataforma nativa en la nube elimina las soluciones heredadas de acceso remoto, como las VPN, que son difíciles de escalar, administrar y configurar

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 vulnerados y las amenazas internas pueden flanquear los controles tradicionales:** los atacantes avanzados pueden robar credenciales y subvertir la identidad para acceder a aplicaciones privadas con herramientas de acceso remoto heredadas y ofertas ZTNA de primera generación.

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

Zscaler Private Access™ (ZPA)

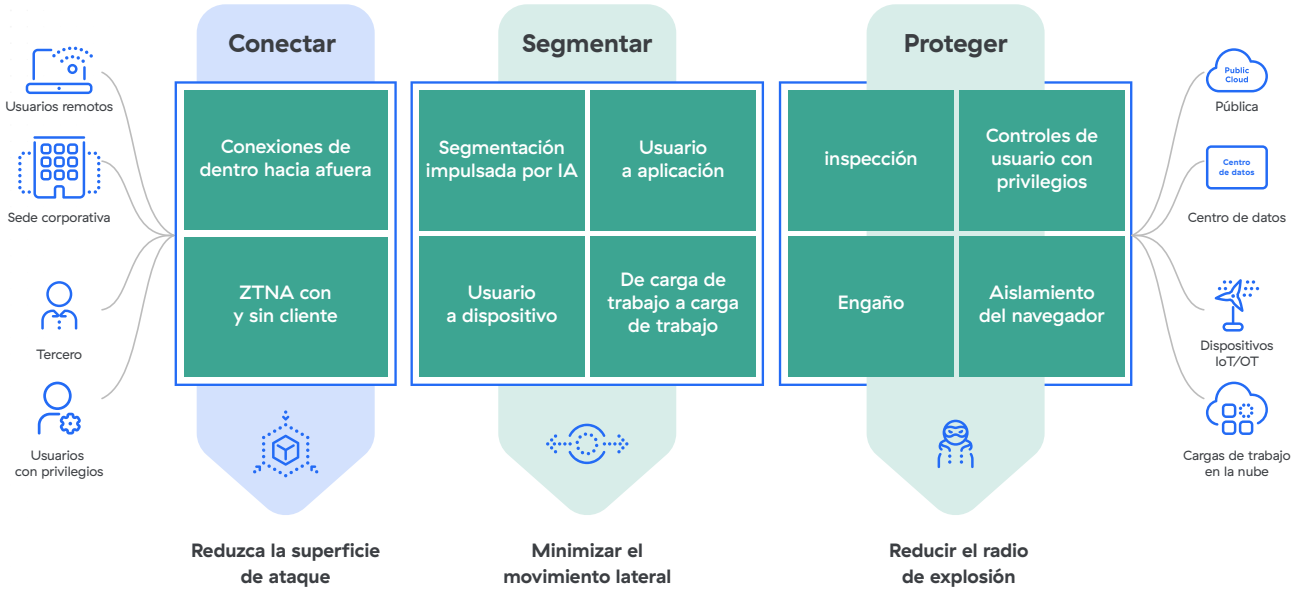
ZPA es la plataforma ZTNA más implementada del mundo, que aplica los principios de privilegios mínimos para brindar a los usuarios una conectividad segura y directa a las aplicaciones privadas que se ejecutan en las instalaciones o en la nube pública, al tiempo que elimina el acceso no autorizado y el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

- **Ofrecer una experiencia de usuario superior:** conectar a los usuarios directamente a aplicaciones privadas elimina el retorno lento y costoso a través de VPN heredadas y, al mismo tiempo, supervisa y resuelve de manera proactiva los problemas de la experiencia del usuario.
- **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 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 dar acceso.
- **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
- **Detectar usuarios y dispositivos comprometidos:** 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 remoto se realizarán predominantemente mediante el acceso a la red de confianza cero (ZTNA).

– Gartner

Cómo aborda ZPA los casos de uso emergentes de ZTNA



Casos de uso clave

VPN alternativas

Las VPN no se diseñaron teniendo en cuenta la seguridad, la escalabilidad o la experiencia del usuario. Tradicionalmente, las VPN retornan todo el tráfico de usuarios remotos a centros de datos que podrían estar a miles de kilómetros de distancia, lo que genera latencia y frustración en los usuarios. Una vez conectadas, las VPN canalizan a los usuarios más allá del cortafuegos y los colocan en la misma red que sus aplicaciones, lo que permite el libre movimiento lateral.

ZPA supera estos desafíos proporcionando acceso rápido y directo a aplicaciones a través de más de 150 puntos de presencia (PoP) distribuidos globalmente sin los riesgos de seguridad inherentes a la VPN. Su conectividad de dentro hacia afuera garantiza que el acceso a las aplicaciones sea independiente del acceso a la red y, al mismo tiempo, elimina la huella de Internet. ZPA conecta a los usuarios con aplicaciones, no con redes, y los usuarios sólo pueden acceder a aplicaciones con nombre, sin posibilidad de moverse lateralmente. 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.

Personal híbrido seguro

En el mundo laboral moderno, los usuarios trabajan desde sus hogares y otras ubicaciones remotas, sucursales y oficinas centrales, desafiando los paradigmas de seguridad heredados. ZPA permite un acceso fluido y seguro a aplicaciones privadas desde donde necesiten trabajar, en cualquier dispositivo. Los usuarios del campus se benefician de una experiencia idéntica gracias a ZPA Private Service Edge.

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. ZPA ahora puede proporcionar capacidades ZTNA Universal para una experiencia de usuario rápida y consistente. Además, con la supervisión de la experiencia digital, obtiene visibilidad en tiempo real

de la degradación del rendimiento y las interrupciones, lo que permite un trabajo híbrido productivo. Como 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) costosa e imperfecta, o de otros clientes de escritorio remoto, como RDP, SSH o VNC, que colocaban a los usuarios directamente en su red y exponían los sistemas internos a dispositivos que no eran de confianza. Las capacidades de acceso sin cliente de ZPA hacen que el acceso de terceros sea tan sencillo como acceder a la web, al mismo tiempo que reduce los costes y minimiza los riesgos. Sus proveedores, contratistas y socios pueden utilizar libremente cualquier navegador web desde sus propios dispositivos para conectarse a sitios web de intranet, sistemas internos y equipos, sin necesidad de 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 nunca queden fuera de su control y estén protegidos frente a acceso no autorizado, funciones de copiar y pegar, impresión, y carga/descarga. Con acceso sin cliente, TI puede ofrecer una experiencia mejor y más segura a los usuarios sin incurrir en los costes de administrar VDI heredado.

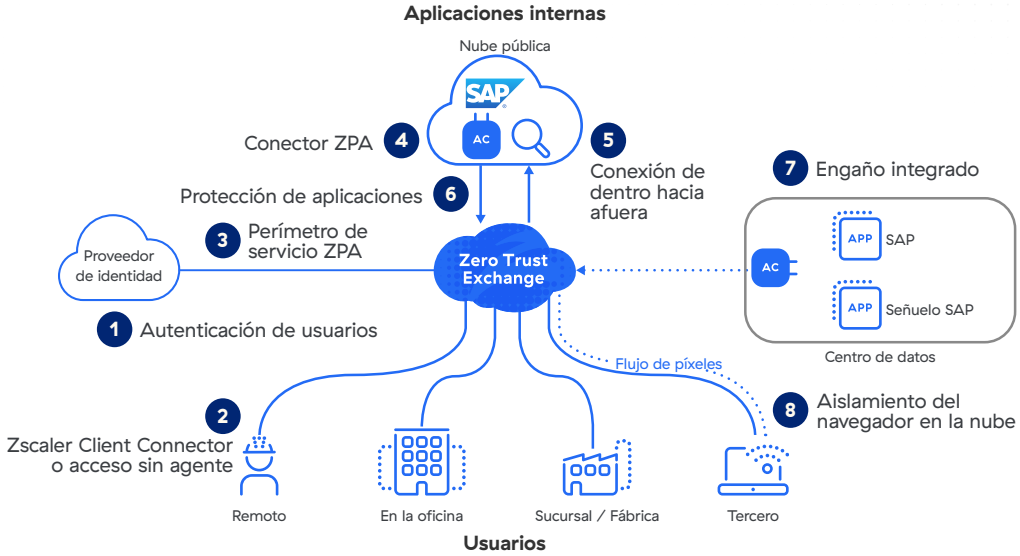
Fusiones y adquisiciones, y desinversiones
Las fusiones, adquisiciones y desinversiones a menudo requieren combinar redes, lo que puede ser un desafío debido a la superposición del espacio de IP y la creación de cortafuegos entre las dos entidades. ZPA acelera drásticamente la integración y el tiempo de valorización tras la fusión y adquisición, acelerando el proceso a cuestión de semanas en lugar de meses. Proporciona acceso fluido a aplicaciones privadas, sin necesidad de VPN, y elimina la necesidad de combinar varias redes o comprar equipos de red adicionales, lo que libera recursos para centrarse en trabajos de alto impacto.

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

Conectividad segura entre cargas de trabajo
Las organizaciones modernas requieren una conectividad rápida y segura entre cargas de trabajo en entornos privados, híbridos y multinube. ZPA para cargas de trabajo reduce la complejidad operativa y el coste, al tiempo que implementa una conectividad basada en confianza cero para cargas de trabajo en todos estos entornos. Debido a que las cargas de trabajo están ocultas detrás de ZPA, son invisibles para 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, lo que garantiza un acceso de confianza cero entre usuarios, dispositivos IoT/OT y aplicaciones basados en políticas empresariales. Elimina la superficie de ataque y previene el movimiento lateral de amenazas al conectar a usuarios y dispositivos IoT/OT a aplicaciones a través de Zero Trust Exchange. La conectividad de sucursales de confianza cero simplifica drásticamente las comunicaciones de las sucursales al eliminar enrutamiento complejo, VPN y cortafuegos, al tiempo que permite un reenvío flexible y una gestión de políticas simple con el marco de políticas probado ZIA y ZPA.

ZPA amplía el acceso con privilegios mínimos a toda la empresa



Cómo funciona

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

1. Autenticación del usuario con IDP utilizando sus credenciales de SSO SAML existentes.
2. Verificación de la postura del dispositivo de un usuario con Zscaler Client Connector, un agente de reenvío ligero instalado en el ordenador portátil o dispositivo móvil del usuario. ZPA también puede determinar la postura del dispositivo a través de la integración de terceros con todos los principales proveedores de EPP/EDR/XDR (por ejemplo, Crowdstrike, Microsoft Defender y SentinelOne).
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. A continuación, ZPA Service Edge determina la aplicación más cercana al usuario y establece una conexión segura a ZPA App Connector, una máquina virtual ligera instalada en el entorno que aloja servidores y aplicaciones.
5. Dos túneles salientes, uno de Client Connector en el dispositivo y el otro de App Connector, se unen mediante el perímetro de servicio de ZPA.
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 procedentes de usuarios o dispositivos que puedan haber sido vulnerados.
7. El sistema de engaño integrado detecta a los usuarios vulnerados que acceden a las aplicaciones señuelo y puede desactivar el acceso a los recursos internos en Zscaler Zero Trust Exchange.
8. Además, 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.

Zscaler puede alojar un ZPA Service Edge en la nube (ZPA Public Service Edge) o se puede ejecutar en las instalaciones de la infraestructura del cliente (ZPA Private Service Edge). En cualquier caso, son administrados por Zscaler sin necesidad de ningún dispositivo.

Capacidades principales

Motor de políticas basadas en el riesgo	Valide continuamente las políticas de acceso en función de la postura de riesgo del usuario, el dispositivo, el contenido y la aplicación con un potente motor de políticas nativo para garantizar que solo los usuarios válidos y autenticados puedan acceder a las aplicaciones privadas.
Cliente unificado y acceso sin cliente	Elija el método óptimo de protección para su entorno híbrido. El acceso basado en agente garantiza que los usuarios administrados estén protegidos incluso cuando están fuera de la red corporativa a través de un agente ligero, Zscaler Client Connector. El acceso sin agente da a los usuarios no gestionados acceso a aplicaciones sin fricciones desde cualquier dispositivo y navegador web, sin necesidad de cliente.
Browser Access	Permita que los usuarios que usan dispositivos propios y los usuarios de terceros utilicen libremente sus propios dispositivos para acceder de forma segura y sin problemas a las aplicaciones internas aprovechando cualquier navegador web, sin necesidad de cliente.
ZTNA en el campus	Experimente ZTNA para usuarios en el campus y conecte de forma segura a los usuarios a las aplicaciones en sus oficinas. Universal ZTNA garantiza un acceso y políticas uniformes para los usuarios, independientemente de la ubicación de estos y las aplicaciones correspondientes.
Recuperación de desastres	Acceso ininterrumpido a aplicaciones esenciales incluso durante un evento de cisne negro con una solución de continuidad comercial controlada por el cliente que crea la ruta de acceso a aplicaciones privadas esenciales a través de ZPA Private Service Edge.
Detección de aplicaciones	Descubra y catalogue automáticamente las aplicaciones mediante nombres de dominio y subredes IP específicos para obtener información detallada de su estado de aplicaciones privadas, así como de su posible superficie de ataque.
Segmentación de aplicaciones mediante IA	Aplique las recomendaciones de segmentación basadas en ML que se le proporcionan automáticamente vía ZPA. De esta manera podrá identificar los segmentos de aplicaciones adecuados y crear las políticas de acceso correctas de forma fácil y rápida. Con la tecnología de modelos de aprendizaje automático, probada continuamente en millones de señales de clientes, y sus patrones únicos de acceso a aplicaciones, la segmentación basada en ML puede ayudarle a minimizar su superficie de ataque interna.
Segmentación de usuario a aplicación	Asegúrese de que cualquier acceso a la aplicación se otorgue según la "necesidad de saber", en base a los privilegios mínimos, con la segmentación de usuario a aplicación. Proporcione a los usuarios autorizados acceso seguro a aplicaciones específicas, sin colocar nunca a los usuarios en la red. Evite la necesidad de una segmentación de red complicada con cortafuegos internos.
Segmentación de usuario a dispositivo	Asegúrese de que cualquier acceso a los equipos y sistemas TO/IIoT se otorgue en base a los privilegios mínimos con la segmentación de usuario a dispositivo. Permita que proveedores terceros y usuarios remotos se conecten a los equipos desde cualquier ubicación con ZPA para IoT y TO.
Segmentación de carga de trabajo a carga de trabajo	Proteja la conectividad y la comunicación entre cargas de trabajo en entornos híbridos y multinube con ZPA for Workloads.
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.
Engaño integrado	Detecte y detenga a los atacantes más sofisticados y las amenazas internas con el engaño de aplicaciones nativo, incluida la contención automatizada de usuarios vulnerados en Zero Trust Exchange.
Cloud Browser Isolation integrado	Proporcione acceso aislado y sin cliente a aplicaciones web esenciales para contratistas y empleados que utilizan sus propios dispositivos. 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 (portapapeles, impresión, carga/descarga) para evitar la pérdida de datos confidenciales.
Acceso remoto privilegiado	Permita que los administradores y operadores con privilegios se conecten de forma segura a sitios web de intranet, sistemas internos y equipos sin necesidad de VPN, VDI o clientes de escritorio remoto como RDP, SSH y VNC.
Protección de datos y frente a amenazas	Reduzca el riesgo de amenazas con una inspección completa del contenido. Encuentre y controle los datos confidenciales en la conexión entre el usuario y la aplicación.
SD-WAN de confianza cero	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 basados en políticas empresariales.

Ventajas

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

Minimice el movimiento lateral
La conectividad basada en el acceso con privilegios mínimos garantiza que el acceso a las aplicaciones se otorgue de forma individualizada desde un usuario autorizado a las aplicaciones designadas, en lugar de un acceso completo 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 administrar segmentaciones de red complejas, listas de control de acceso (ACL), políticas de cortafuegos o traducciones de direcciones de red. Las capacidades de engaño integradas de ZPA permiten a los equipos de seguridad detectar y aislar inmediatamente a un usuario malintencionado o un dispositivo comprometido que intenta moverse lateralmente por la organización.

Evite usuarios comprometidos, amenazas internas y atacantes avanzados
La protección de aplicaciones privadas, primera en su clase, con capacidades integradas de inspección en línea, engaño y prevención de pérdida de datos, minimiza el riesgo de usuarios comprometidos y atacantes activos. ZPA detiene automáticamente los ataques web con una cobertura completa para las técnicas más frecuentes, incluido OWASP Top 10, y soporte completo de firmas personalizadas para revisiones virtuales inmediatas contra vulnerabilidades de día cero. ZPA minimiza los riesgos de terceros y el uso de dispositivos propios con acceso completamente aislado a aplicaciones que mantiene los datos confidenciales fuera de los dispositivos no administrados mediante el aislamiento integrado del navegador en la nube. La tecnología de engaño integrada que utiliza aplicaciones señuelo permite a los equipos de seguridad contener amenazas activas en la red al impedir que los usuarios comprometidos accedan a los recursos.

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

Una plataforma unificada para el acceso seguro a través de aplicaciones, cargas de trabajo y dispositivos OT
Extienda la confianza cero a las aplicaciones privadas, las cargas de trabajo y los dispositivos OT/IIoT para simplificar e integrar múltiples herramientas independientes de acceso remoto. De esta forma, se unifican las políticas de seguridad y acceso para detener las infracciones y reducir la complejidad operativa.

Ediciones de Zscaler Private Access

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Servicios de la plataforma	Anclaje 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 aplica–ciones	Segmentos de aplicación ilimitados	Segmentos de aplicación ilimitados
App Connector	20 pares	50 pares	Pares ilimitados	Pares ilimitados
ZTNA en el campus[1]	1 par (virtual)	1 par de perímetro de servicio seguro por 5000 usuarios	1 par de perímetro de servicio seguro por 2000 usuarios	1er par de perímetro de servicio privado incluido, par adicional por cada 1000 usuarios
Clientless Access[2]	—	✓	✓	✓
Supervisión de la experiencia digital integrada	—	Estándar	Estándar	Estándar
Engaño integrado	—	Estándar	Avanzado	Avanzado Plus
Protección de aplicaciones	—	—	✓	✓
Aislamiento integrado	—	—	Estándar	Avanzado Plus
Protección de datos (aplicaciones privadas)	—	—	—	✓
Asistencia prémium	—	—	—	✓

Diferenciadores clave

Como única plataforma ZTNA de próxima generación del sector, Zscaler Private Access 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
- **Engaño integrado:** detenga los intentos de movimiento lateral y la propagación de ransomware con la única solución ZTNA con engaño de aplicación nativa
- **Acceso sin cliente:** aproveche el acceso basado en navegador para terceros con DLP integrado
- **Productividad mejorada:** mantenga una visibilidad completa del acceso a aplicaciones privadas para detectar problemas de usuario que afectan la experiencia del usuario
- **Presencia de perímetro global:** obtenga una seguridad y una experiencia de usuario sin parangón con más de 150 ubicaciones en el perímetro de la nube en todo el mundo. Un perímetro de servicio local opcional extiende la confianza cero 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

[1]ZPA Business Edition admite hasta 5 Private Service Edge; se requiere comprar pares adicionales al superar los 50 000 usuarios. ZPA Transformation Edition admite hasta 10 pares Private Service Edge; se requiere comprar pares adicionales al superar los 50 000 usuarios. ZPA Unlimited Edition admite hasta 50 Private Service Edge; se requiere comprar pares adicionales al superar los 50 000 usuarios.

[2]Clientless Access incluye Browser Access y acceso remoto privilegiado (para hasta 10 sistemas).

- **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

Componentes fundamentales

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

Zscaler Branch Connector
Branch Connector, disponible en factores de forma de dispositivo físico y virtual, mejora el rendimiento de las aplicaciones al eliminar el retorno y reenviar 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 a través de Zero Trust Exchange.

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

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

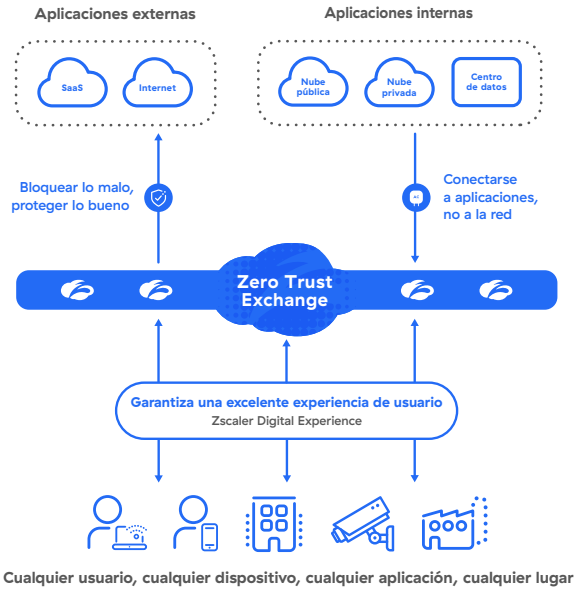
ZPA Service Edges
Los perímetros de servicio aseguran el cumplimiento de políticas de seguridad y acceso, uniendo la conexión interna entre un usuario autorizado (a través de Client Connector y Browser Access) y una aplicación privada específica (a través de App Connector). La mayoría de los clientes utilizan nuestros perímetros de servicio públicos, que están alojados en más de 150 intercambios en todo el mundo y manejan millones de usuarios simultáneos para las mayores organizaciones del mundo. Los perímetros de servicio privados, administrados por Zscaler, también están disponibles para alojarse en el sitio para brindar a los usuarios locales la ruta más corta a las aplicaciones locales sin salir de la red local.

ZPA forma parte de la plataforma global Zero Trust Exchange

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

Cómo Zscaler ofrece confianza cero para usuarios, cargas de trabajo y IIoT/OT

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



Especificaciones técnicas

Componente 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
Clientless Access	Navegadores web modernos:	Chrome
	(compatible con HTML 5)	Edge
		Firefox
App Connector	AWS	Microsoft Hyper-V
	Centos, Oracle y Red hat	VMware vCenter o vSphere Hypervisor
	Microsoft Azure	Anfitrión acoplable

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

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

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