Zscaler Internet Access

Protección basada en IA en todas partes para todos los usuarios, todas las aplicaciones y todas las ubicaciones

FICHA DE DATOS

Zscaler Internet Access™ define el acceso seguro y rápido a Internet y SaaS con la plataforma Zero Trust más completa y confiable del sector.

La seguridad de las redes tradicional se ha vuelto ineficaz en un mundo que da prioridad a la nube y la movilidad

Las arquitecturas hub-and-spoke tradicionales eran eficaces cuando los usuarios se encontraban principalmente en la sede central o en una sucursal, las aplicaciones residían únicamente en el centro de datos corporativo y su superficie de ataque se limitaba a lo que sancionaba su organización. Hoy vivimos en un mundo drásticamente diferente, con un panorama de amenazas en el que el ransomware, las amenazas cifradas, los ataques a la cadena de suministro y otras amenazas avanzadas atraviesan las defensas de red tradicionales. Es hora de encontrar una solución de seguridad nativa de la nube que reduzca de manera integral el riesgo y la complejidad y, al mismo tiempo, permita flexibilidad para ayudar a impulsar las iniciativas comerciales.

Zscaler Internet Access

La seguridad de la empresa actual, que da prioridad a la nube y a los dispositivos móviles, requiere un enfoque fundamentalmente diferente basado en Zero Trust. Zscaler Internet Access, parte de Zscaler Zero Trust Exchange™, es la plataforma Security Service Edge (SSE) más implementada del mundo y está respaldada por una década de liderazgo de puertas de enlace web seguras.

Suministrada como una plataforma de seguridad en la nube SaaS escalable y resistente, ZIA elimina las soluciones de seguridad de red heredadas para detener los ataques avanzados y evitar la pérdida de datos con un enfoque Zero Trust integral, que ofrece:

Seguridad uniforme y la mejor de su clase para la fuerza de trabajo híbrida de la actualidad: al trasladar la seguridad a la nube, todos los usuarios, aplicaciones, dispositivos y ubicaciones obtienen una protección contra amenazas que está siempre activa basada en la identidad y el contexto. Su política de seguridad llega a todos los lugares a los que van sus usuarios.

Acceso ultrarrápido sin infraestructura: la arquitectura directa a la nube garantiza una experiencia de usuario rápida y sin inconvenientes. Esto elimina el retorno del tráfico, mejora el rendimiento y la experiencia del usuario, y simplifica la administración de la red, sin necesidad de infraestructura física.

Protección impulsada por la IA desde la nube de seguridad más grande del mundo: inspección en línea de todo el tráfico de Internet y SaaS, incluido el descifrado SSL, con un conjunto de servicios de seguridad en la nube impulsados por la IA para detener ransomware, phishing, malware de día cero y ataques avanzados basados en inteligencia sobre amenazas a partir de 500 billones de señales diarias.

Gestión simplificada: el uso de una solución de seguridad nativa de la nube dotada de IA, menos hardware que gestionar, automatización para agilizar los flujos de trabajo y creación de políticas centradas en la actividad empresarial ahorra tiempo a su equipo para que se centre en los objetivos estratégicos.

Servicios integrados de seguridad y protección de datos con IA

Zscaler Internet Access incluye un conjunto completo de servicios de seguridad y protección de datos con IA para ayudarle a detener los ciberataques y la pérdida de datos. Como una solución SaaS totalmente distribuida en la nube, puede agregar nuevas funcionalidades sin ningún hardware adicional ni largos ciclos de implementación. Los módulos disponibles como parte de Zscaler Internet Access son:

- **Cloud Secure Web Gateway (SWG):** ofrezca una experiencia web rápida y segura que elimine ransomware, malware y otros ataques avanzados con análisis en tiempo real impulsado por la IA y filtrado de URL.
- **Cloud Access Security Broker (CASB):** proteja los datos, detenga las amenazas y garantice el cumplimiento normativo en todos sus entornos SaaS e IaaS con CASB integrado para la seguridad de las aplicaciones en la nube.
- **Cloud Data Loss Prevention (DLP):** proteja los datos en movimiento mediante una inspección completa en línea y medidas avanzadas como la coincidencia exacta de datos (EDM), el reconocimiento óptico de caracteres (OCR) y el aprendizaje automático.
- **Firewalls e IPS en la nube de Zscaler:** extienda la protección líder del sector a todos los puertos y protocolos, y reemplace los firewalls perimetrales y de sucursal por una plataforma nativa en la nube.
- **Zscaler Sandbox:** detenga el malware nunca antes visto y elusivo en los protocolos web y de transferencia de archivos con cuarentena impulsada por la IA, compartiendo protección uniforme y global entre todos los usuarios en tiempo real.
- **Navegador Zero Trust potenciado por IA:** desarticule los ataques basados en la web y evite la pérdida de datos creando un vacío virtual entre los usuarios, la web y el SaaS.

VENTAJAS:

- **Evite las ciberamenazas y la pérdida de datos con IA:** proteja su organización contra amenazas avanzadas con un conjunto de servicios de protección de datos y ciberamenazas impulsados por la IA, enriquecidos con actualizaciones en tiempo real provenientes de 500 billones de señales de amenazas diarias de la nube de seguridad más grande del mundo.
- **Obtenga una experiencia de usuario inigualable:** acceda a Internet y SaaS más rápido que el resto del mundo (hasta un 40 % más rápido que las arquitecturas de seguridad heredadas) para aumentar la productividad y la rapidez de sus operaciones.
- **Reduzca costos y complejidad:** obenga un retorno de la inversión del 139 % con Zscaler reemplazando el 90 % de sus dispositivos costosos, complejos y lentos con una plataforma Zero Trust totalmente nativa de la nube.
- **Asegure su fuerza de trabajo híbrida:** permita que empleados, clientes y terceros accedan de manera segura a las aplicaciones web y los servicios en la nube desde cualquier lugar y dispositivo, con una gran experiencia digital.
- **Unifique los esfuerzos de SecOps y NetOps:** impulse resultados de seguridad más rápidos y colaborativos con herramientas compartidas como perspectivas de tráfico en tiempo real, integraciones API-first y RBAC granular.
- **Consiga una soberanía total de datos y contenidos:** imponga el cumplimiento de la normativa para un acceso seguro y localizado sin mermas en el rendimiento mediante NAT de salida, contenido geolocalizado y registro de datos en el país.
- **IA segura en su entorno:** habilite el uso seguro de Microsoft Copilot y otras aplicaciones de IA.
- **Proteja los entornos de los desarrolladores a escala:** automatice la inspección SSL/TLS de más de 30 herramientas para desarrolladores, a la vez que protege el código y los archivos desconocidos o de gran tamaño con veredictos de IA instantáneos, todo ello sin ralentizar la innovación.

©2025 Zscaler, Inc. Todos los derechos reservados.

- **Supervisión de la experiencia digital:** reduzca la sobrecarga operativa de TI y acelere la resolución de tickets de asistencia con una visión unificada de las métricas de rendimiento de las aplicaciones, la ruta de la nube y los puntos finales para el análisis y la resolución de problemas.

- **Conectividad de sucursales Zero Trust:** reduzca el riesgo y la complejidad con la conectividad no enrutable de sucursales y centros de datos para usuarios, servidores y dispositivos IOT/OT.

- **Seguridad DNS:** optimice la seguridad y el rendimiento del DNS para todos los usuarios, dispositivos y aplicaciones, en todos los puertos y protocolos, en cualquier lugar del mundo.

Zscaler Internet Access para usuarios y cargas de trabajo

Elimine el riesgo de las cargas de trabajo en la nube que accedan a cualquier destino de Internet o SaaS con Zscaler Internet Access. Al eliminar la necesidad de que las cargas de trabajo accedan a Internet utilizando herramientas heredadas y centradas en la red, como VPN, firewalls (incluidos firewalls virtuales) o tecnologías WAN, puede evitar el compromiso y detener el movimiento lateral sin la necesidad de un mosaico de herramientas de seguridad. Al aplicar el conjunto integral de capaci-dades de seguridad y protección de datos de ZIA a las cargas de trabajo, puede unificar la seguridad Zero Trust para sus usuarios y cargas de trabajo con una única plataforma integrada.

Al combinar ZIA con Zscaler Private Access, puede extender la protección a sus aplicaciones y cargas de trabajo privadas, ya sea que residan en la nube pública o en un centro de datos privado.

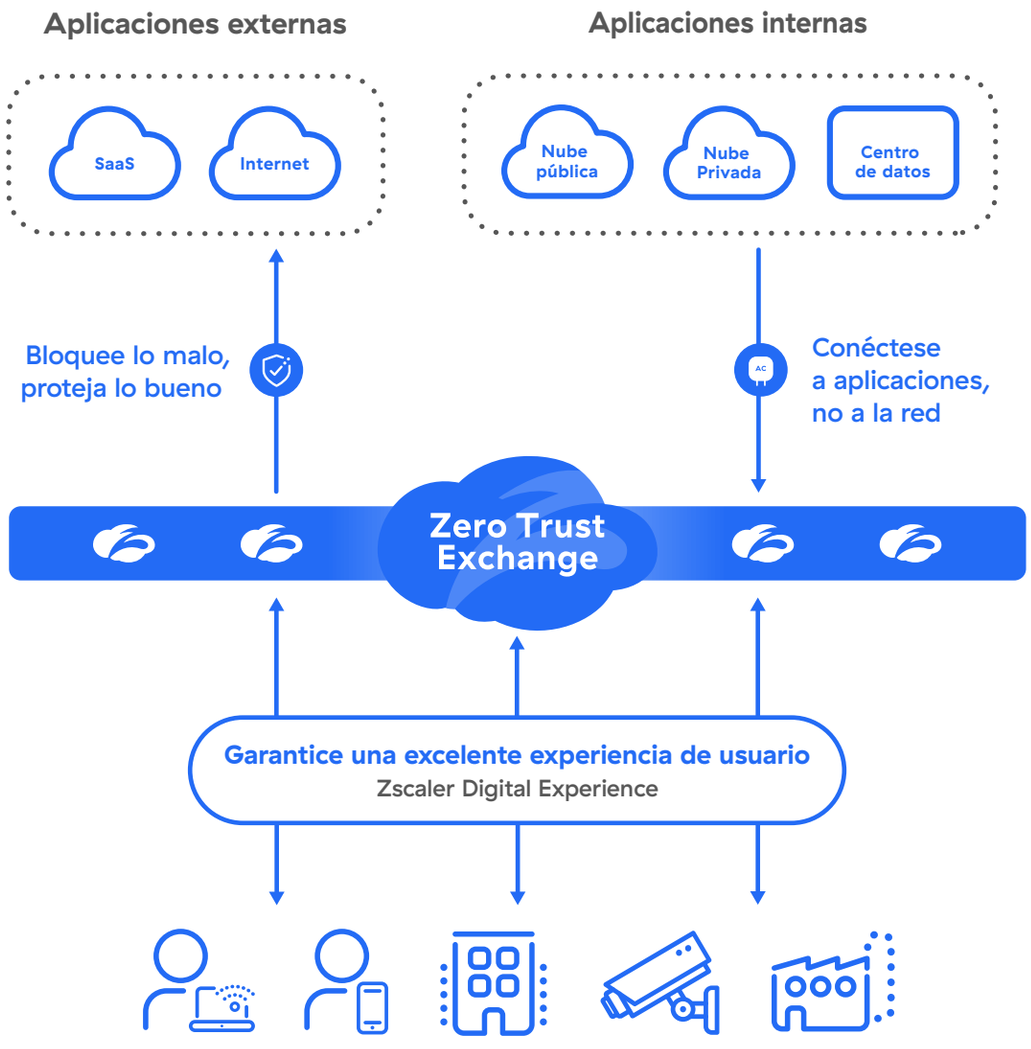


Figura 1: Zero Trust Exchange

*Gartner®, Magic Quadrant for Security Service Edge, 15 de abril de 2024, Charlie Winckless, y col.

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.

Gartner®

Zscaler designado uno de los líderes en el Gartner® Magic Quadrant™ de 2024 para Security Service Edge.

MÁS INFORMACIÓN

©2025 Zscaler, Inc. Todos los derechos reservados.

Casos de uso

PROTECCIÓN CONTRA CIBERAMENAZAS Y RANSOMWARE

Pase de la seguridad de red tradicional a la revolucionaria arquitectura Zero Trust de Zscaler, que evita los riesgos, elimina la superficie de ataque, detiene el movimiento lateral y mantiene los datos seguros.

Más información

FUERZA DE TRABAJO HÍBRIDA Y SEGURA

Permita a empleados, socios, clientes y proveedores acceder de manera segura a aplicaciones web y servicios en la nube desde cualquier lugar, en cualquier dispositivo y garantice una magnífica experiencia digital.

Más información

PROTECCIÓN DE DATOS

Detenga la pérdida de datos de usuarios, aplicaciones SaaS e infraestructura de nube pública por exposición accidental, robo de datos o ransomware de doble extorsión.

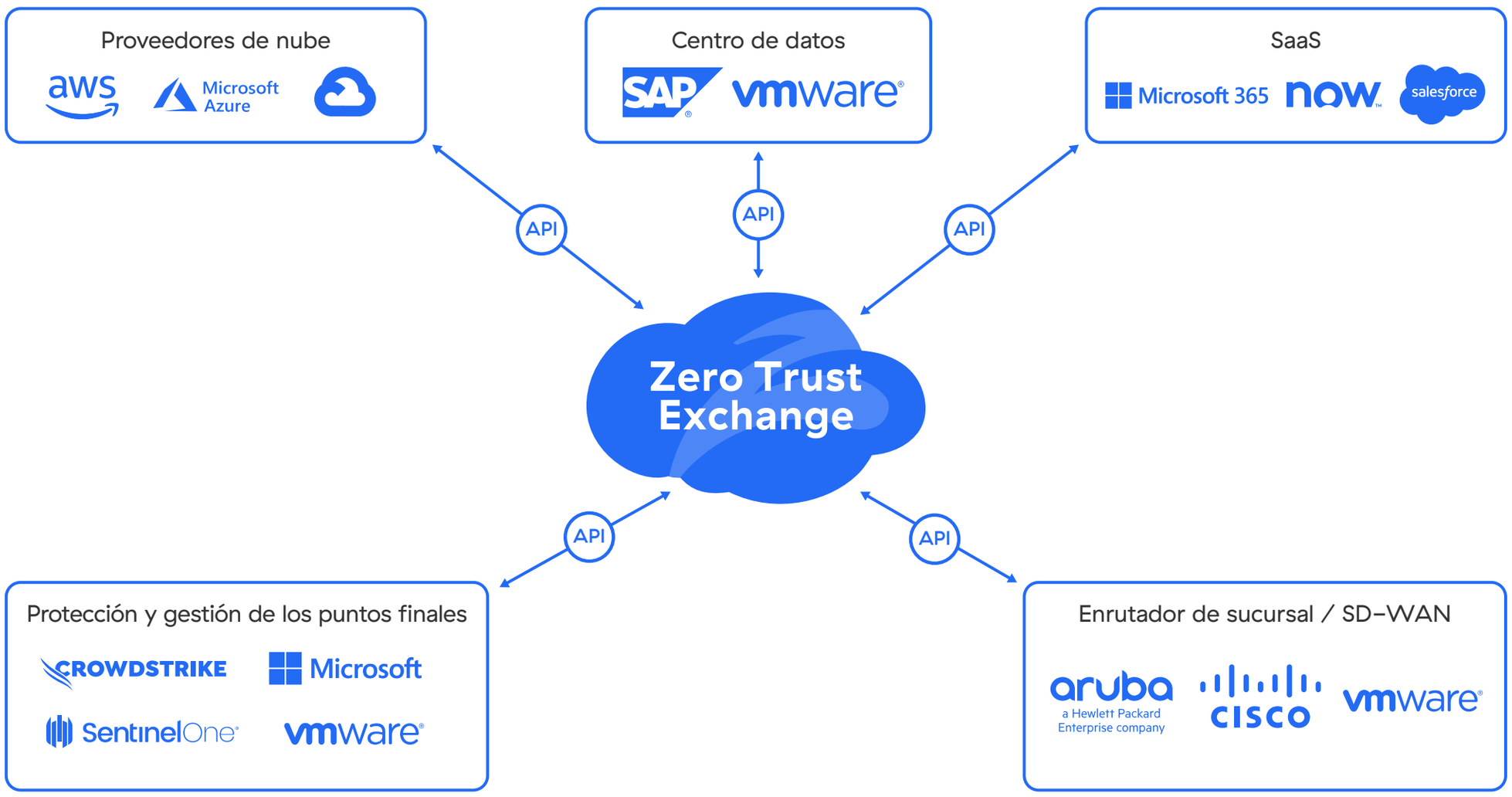
Más información

MODERNIZACIÓN DE LA INFRAESTRUCTURA

Elimine las costosas y complejas redes con un acceso rápido, confiable, seguro y directo a la nube que elimina la necesidad de firewalls en el perímetro y en las sucursales.

Más información

El ecosistema de Zscaler Zero Trust Exchange



©2025 Zscaler, Inc. Todos los derechos reservados.

TABLA 1: FUNCIONES Y CAPACIDADES DE ZSCALER INTERNET ACCESS	
CARACTERÍSTICAS	**DETALLES**
CAPACIDADES	
Filtrado de URL	Autorice, bloquee, advierta o aísle el acceso de los usuarios a categorías o destinos web específicos para detener las amenazas basadas en la web y garantizar el cumplimiento de las políticas de la organización.
Inspección de SSL	Obtenga una inspección ilimitada del tráfico TLS/SSL para identificar amenazas y pérdida de datos que se ocultan en el tráfico cifrado. Especifique qué categorías web o aplicaciones deben inspeccionarse en función de los requisitos de privacidad o normativos. Integre la inspección con la herramienta de desarrollo para asegurar los flujos de trabajo de los desarrolladores.
Seguridad de DNS	Identifique y dirija las conexiones sospechosas de comando y control a los motores de detección de amenazas de Zscaler para que inspeccionen todo el contenido.
IP dedicada	Proporcione acceso a las aplicaciones que permiten direcciones IP con direcciones IP dedicadas a su organización. También permite una transición fácil de la arquitectura tradicional a Zero Trust.
Control de archivos	Bloquee o autorice la carga/descarga de archivos en las aplicaciones en función de la aplicación, el usuario o el grupo de usuarios.
Traiga su propia IP	Mantenga la consistencia y el control sobre la identidad de su red y garantice a las aplicaciones de terceros o a la infraestructura dependiente que el tráfico procede únicamente de su organización.
Control de ancho de banda	Aplique políticas de ancho de banda para priorizar el tráfico de las aplicaciones empresariales en vez del tráfico recreativo.
Registro basado en el país	Almacene y gestione los registros dentro de las fronteras de un país concreto para cumplir los requisitos de soberanía de datos que exigen que los datos relacionados con los ciudadanos se procesen de acuerdo con las leyes locales.
Protección contra Amenazas Avanzadas	Detenga los ciberataques avanzados, como el malware, el ransomware, los ataques a la cadena de suministro, el phishing y muchos más, con una protección avanzada patentada contra las amenazas. Fije políticas granulares basadas en la tolerancia al riesgo de su organización.
Protección de datos en línea (datos en movimiento)	Utilice las capacidades de proxy de reenvío e inspección SSL para controlar el flujo de información confidencial a destinos web y aplicaciones en la nube peligrosos en tiempo real, deteniendo las amenazas internas y externas a los datos. La protección avanzada en línea se proporciona ya sea que una aplicación esté autorizada o no administrada sin que requiera registros de dispositivos de red.
Protección de datos fuera de banda (datos en reposo)	Utilice las integraciones de API para examinar las aplicaciones SaaS, las plataformas en la nube y sus contenidos, identificar los datos confidenciales en reposo y hacer correcciones automáticamente cancelando los recursos compartidos o externos que supongan un riesgo.
Prevención de intrusiones	Obtenga una protección completa contra amenazas de botnets, amenazas avanzadas y días cero, junto con información contextual sobre el usuario, la aplicación y la amenaza. IPS de nube y web que funcionan a la perfección en Firewall, Sandbox, DLP y CASB. Implemente firmas de amenazas a medida utilizando el IPS personalizado en la nube para detectar y detener ataques dirigidos.
Política de acceso y seguridad dinámica y basada en los riesgos	Adapte automáticamente la política de seguridad y el acceso a los riesgos de usuario, dispositivo, aplicación y contenido.

©2025 Zscaler, Inc. Todos los derechos reservados.

Captura de tráfico	Captura de paquetes sin interrupciones: capture fácilmente el tráfico descifrado utilizando criterios específicos en los motores de políticas de Zscaler, con lo que podrá realizar análisis detallados de seguridad eficientes sin necesidad de dispositivos adicionales.
Análisis de malware	Detecte, prevenga y ponga en cuarentena amenazas desconocidas que se ocultan en cargas útiles maliciosas en línea con IA/aprendizaje automático avanzados para detener los ataques de paciente cero.
Filtrado de DNS	Controle y bloquee las solicitudes de DNS contra destinos conocidos y maliciosos.
Navegador Zero Trust (aislamiento web)	Haga obsoletas las amenazas basadas en la web distribuyendo el contenido activo como un flujo benigno de píxeles en el navegador del usuario final.
Información sobre amenazas correlacionadas	Acelere la investigación y los tiempos de respuesta con alertas contextualizadas y correlacionadas con las observaciones acerca de la puntuación de la amenaza, el activo afectado, la gravedad, etc.
Aislamiento de aplicaciones	Autorice el acceso seguro, sin agentes y sin administración de los dispositivos a SaaS, la nube y las aplicaciones privadas con un control granular de las acciones de los usuarios, tales como copiar/pegar, cargar/descargar e imprimir para detener la pérdida de datos confidenciales.
Supervisión de la experiencia digital (ZDX)	Obtenga una visión unificada de las métricas de rendimiento de las aplicaciones, la ruta de la nube y los puntos finales para el análisis y la resolución de problemas.
Conectividad de sucursal Zero Trust	Modernice la conectividad de sucursales mediante Zero Trust Exchange para eliminar la superficie de ataque y evitar el movimiento lateral.
Protección de la comunicación de la carga de trabajo a Internet	Evite el compromiso y detenga el movimiento lateral para las comunicaciones de carga de trabajo a Internet. Incluye inspección SSL, IPS, filtrado de URL y protección de datos para todas las comunicaciones.
Visibilidad de los dispositivos IoT	Obtenga una visión integral de todos los dispositivos IoT, servidores y dispositivos de usuario no administrados en toda su empresa, con detección automatizada, supervisión continua y clasificación AI/ML con capacidades de etiquetado automático pioneras en el sector.
Control de acceso basado en roles (RBAC)	Permisos dimensionados correctamente para controlar la política de lo qué los administradores pueden editar y ver, y los informes analíticos dentro de la plataforma Zscaler para evitar conflictos y mejorar la gobernanza.

©2025 Zscaler, Inc. Todos los derechos reservados.

CARACTERÍSTICAS	DETALLES
CARACTERÍSTICAS DE LA PLATAFORMA	
Opciones de conectividad flexibles	• Zscaler Client Connector (ZCC): redirija el tráfico a Zero Trust Exchange a través de un agente liviano compatible con Windows, macOS, iOS, iPadOS, Android y Linux. • Túneles GRE o IPsec: utilice túneles GRE y IPsec para enviar tráfico al Zero Trust Exchange para los dispositivos sin ZCC. • Aislamiento del navegador: conecte sin problemas cualquier dispositivo BYOD o no gestionado con el aislamiento del navegador Zero Trust integrado. • Encadenamiento de proxy: Zscaler admite el reenvío de tráfico de un servidor proxy a otro, pero no se recomienda en entornos de producción. • Archivos PAC: envía tráfico al Zero Trust Exchange con archivos PAC para dispositivos sin ZCC.
Implementación en la nube	Plataforma 100 % nativa de la nube distribuida como un servicio SaaS. Para la planificación de la continuidad empresarial y otros casos de uso especial, se dispone de perímetros de servicio privados y virtuales.
Privacidad y retención de datos	Cuando se registran los datos, el contenido nunca se escribe en el disco y existen controles granulares para determinar dónde se realiza exactamente el registro. Utilice el control de acceso basado en roles (RBAC) para proporcionar acceso de solo lectura, anonimización/obfuscación del nombre de usuario y derechos de acceso separados por departamento o función, de acuerdo con las normas de cumplimiento importantes. Los datos se retienen durante un período de seis meses consecutivos o menos, según el producto. Puede adquirir almacenamiento adicional para retener los datos durante el tiempo que desee.
Certificaciones de cumplimiento clave	Las certificaciones incluyen: • FedRAMP • ISO 27001 • SOC 2 tipo II • SOC 3 • NIST 800-63C Vea la lista completa de nuestras certificaciones de cumplimiento aquí.
Compatibilidad granular de API	Mantenemos integraciones REST API con numerosos proveedores de identidad, redes y seguridad. Por ejemplo, puede compartir registros entre Zscaler y su SIEM basado en la nube o local (ej., Splunk). Más información
Intercambio de tráfico directo	El intercambio directo con los principales proveedores de Internet y SaaS y los destinos de la nube pública garantiza la ruta de tráfico más rápida posible.

©2025 Zscaler, Inc. Todos los derechos reservados.

CARACTERÍSTICAS	DETALLES
ACUERDOS DE NIVEL DE SERVICIO (SLA)	
Disponibilidad	99.999 %, medida según las transacciones perdidas
Latencia del proxy	<100 ms, incluso cuando el análisis DLP y de amenazas están activos
Detección de virus	100 % de los virus y malware conocidos
PLATAFORMAS Y SISTEMAS COMPATIBLES	
Client Connector	Compatible con: • iOS 9 o posterior • Android 8 o posterior • Windows 8 o posterior • Mac OS X 10.14 o posterior • CentOS 9 • Ubuntu 20.04 Más información
Branch Connector	Compatible con: • VMware vCenter o vSphere Hypervisor • Centos • Redhat

©2025 Zscaler, Inc. Todos los derechos reservados.

Zscaler Internet Access: Múltiples opciones para dar los primeros pasos

	PLATAFORMA ESSENTIALS Comience su camino hacia Zero Trust con un acceso seguro y confiable a Internet y un acceso privado limitado, con otras innovaciones de Zscaler.	PLATAFORMA ZSCALER Obtenga la solución SASE/SSE completa, que incluye acceso pleno a Internet, acceso privado y protección de datos.
SERVICIOS DE PLATAFORMA		
Redireccionamiento de tráfico – Conector de cliente, GRE, PAC, encadenamiento de proxy, IPsec	comprobar	comprobar
Múltiples proveedores de identidad (IdP), acceso a API, postura del dispositivo	comprobar	comprobar
Autenticación: SAML, LDAP seguro, Kerberos	comprobar	comprobar
Entorno de prueba ZS	–	–
Acceso a los controladores de dominio públicos de Zscaler	comprobar	comprobar
Acceso a centros de datos públicos de alto costo de Zscaler (Australia, Nueva Zelanda, Dubái (no regulado), Sudamérica, África, Corea del Sur, Taiwán y China continental)	–	comprobar
China Premium / Acceso regulado a centros de datos en Oriente Medio	–	–
ACCESO A INTERNET		
Filtrado de contenidos	comprobar	comprobar
Control de tipo de archivo	comprobar	comprobar
Inspección TLS/SSL	comprobar	comprobar
Certificado privado SSL	comprobar	comprobar
Control del ancho de banda	comprobar	comprobar
Transmisión a SIEM local (servicio de transmisión Nanolog con gestión en directo)	comprobar	comprobar
NSS en la nube (para más de 500 usuarios)	comprobar	comprobar
Anclaje IP de origen	–	comprobar
ZIA Private Service Edge – Dispositivo virtual	–	comprobar
Hardware: ZIA Private Service Edge: 3 instancias, 5 instancias	–	–

©2025 Zscaler, Inc. Todos los derechos reservados.

PROTECCIÓN CONTRA CIBERAMENAZAS		
Cyberthreat Protection Standard: Advanced Threat Protection, Sandbox Standard, Zero Trust Firewall Standard, Zero Trust Browser Standard	comprobar	comprobar
Antivirus y antispyware en línea	comprobar	comprobar
Sandbox Advanced	–	–
Zero Trust Firewall Advanced	–	–
Zero Trust Browser Advanced (1.5 GB de tráfico/ usuario/mes, medido entre todos los usuarios de Zero Trust Browser)	–	–
Navegador Zero Trust Unlimited (sin límites de tráfico)	–	–
ACCESO PRIVADO (ZPA)		
Acceso seguro a aplicaciones privadas (en la nube, centros de datos): transmisión de registros, anclaje de IP de origen, múltiples IdP, supervisión de estado)	1 usuario por cada 20 usuarios suscritos (Mínimo: 500 usuarios suscritos)	comprobar
Conectores de aplicaciones	Tantos como sea necesario (hasta el máximo del sistema)	Tantos como sea necesario (hasta el máximo del sistema)
PROTECCIÓN DE DATOS		
Estándar de protección de datos: control de aplicaciones en la nube, informe de TI oculta, restricción de usuarios, web en línea (modo de supervisión), API SaaS (1 apli-cación), seguridad de IA generativa	comprobar	comprobar
Web en línea y DLP de Gen AI, todas las aplicaciones (Internet y Private Access)	–	comprobar
GESTIÓN DE RIESGOS		
Risk Management Standard: Deception Standard	–	comprobar
ZERO TRUST FOR WORKLOADS		
Zero Trust for Workloads Standard: Filtrado de estado, DNS, inspección TLS	1 GB de tráfico mensual de carga de trabajo por usuario suscrito	2 GB de tráfico mensual de carga de trabajo por usuario suscrito
ZSCALER DIGITAL EXPERIENCE (ZDX)		
ZDX Standard: Pre-Set	comprobar	–
ZDX Standard	–	comprobar
SOPORTE		
Standard Support	comprobar	comprobar
Support Plus	–	–

©2025 Zscaler, Inc. Todos los derechos reservados.

MODELO DE LICENCIA

Todas las ediciones de Zscaler Internet Access tienen un precio por usuario. Para determinados productos dentro de la edición de su plataforma, los precios pueden variar fuera del recuento de usuarios. Para obtener más información sobre los precios, hable con su equipo de cuentas de Zscaler.

Parte del Zero Trust Exchange integral

Zero Trust Exchange facilita las conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier sitio, utilizando Internet como red corporativa. Proporciona seguridad integral basada en el principio Zero Trust de acceso con privilegios mínimos, mediante la aplicación de políticas e identidad basadas en contexto.

> Lo fantástico de Zscaler es que ofrece todo lo que necesitamos en una plataforma Zero Trust: inspección escalable del tráfico SSL, otras funciones de prevención de amenazas y protección de datos.
>
> **NITIN NEGI**
> Director de Ingeniería y Operaciones de Ciberseguridad de Micron Technology

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 160 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

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

zscaler™

Zero Trust Everywhere