Zscaler Internet Access

Protección con tecnología IA para todos los usuarios, todas las aplicaciones y todas las ubicaciones

FICHA DE DATOS

Zscaler Internet Access™ define un acceso a Internet y SaaS seguro y rápido con la plataforma zero trust más completa del sector.

La seguridad de la red heredada se ha vuelto ineficaz en un mundo que prioriza la nube y los dispositivos móviles.

Las arquitecturas tradicionales de tipo radial eran eficaces cuando los usuarios estaban principalmente en la sede central o en una sucursal, las aplicaciones residían únicamente en el centro de datos corporativo y su superficie de ataque estaba limitada a lo que su organización autorizaba. 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 la red heredada. 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

Proteger la empresa que da prioridad a la nube y la comunicación móvil de hoy en día requiere un enfoque fundamentalmente diferente basado en zero trust. Zscaler Internet Access, parte de Zscaler Zero Trust Exchange™, es la plataforma de perímetro de servicio de seguridad (SSE) más implementada del mundo, basada en una década de liderazgo en pasarelas web seguras.

Suministrada como una plataforma SaaS escalable desde la mayor nube de seguridad del mundo, elimina las soluciones de seguridad de red heredadas para detener los ataques avanzados y evitar la pérdida de datos con un enfoque integral zero trust, ofreciendo:

La mejor y más uniforme seguridad de su clase para el personal híbrido de hoy en día: cuando se traslada la seguridad a la nube, todos los usuarios, las aplicaciones, los dispositivos y las ubicaciones obtienen protección contra amenazas siempre activa basada en la identidad y el contexto. Su política de seguridad va a cualquier lugar donde vayan 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, mejora el rendimiento y la experiencia del usuario, y simplifica la administración de la red, sin necesidad de infraestructura física.

Protección impulsada por IA desde la mayor nube de seguridad 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 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 con inteligencia artificial, menos hardware para administrar, automatización para optimizar los flujos de trabajo y creación de políticas centradas en el negocio permiten liberar tiempo valioso para que su equipo se concentre en objetivos estratégicos.

Servicios integrados de seguridad y protección de datos basados en IA

Zscaler Internet Access incluye un conjunto completo de servicios de seguridad y protección de datos impulsados por IA para ayudarle a detener los ataques cibernéticos y la pérdida de datos. Como una solución SaaS totalmente provista 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):** brinde una experiencia web rápida y segura que elimine ransomware, malware y otros ataques avanzados con análisis en tiempo real impulsado por IA y filtrado de URL.

- **Cloud Access Security Broker (CASB):** proteja las aplicaciones en la nube con CASB integrado para proteger los datos, detener las amenazas y garantizar el cumplimiento en todos sus entornos SaaS e IaaS.

- **Prevención de pérdida de datos en la nube (DLP):** proteja los datos en movimiento con 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.

- **Zscaler Firewall y Cloud IPS:** amplíe la protección líder del sector a todos los puertos y protocolos, y sustituya los cortafuegos de perímetro 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 IA, compartiendo protección consistente y global entre todos los usuarios en tiempo real.

- **Zero Trust Browser con tecnología de IA:** haga que los ataques basados en la web sean fenómenos obsoletos y evite la pérdida de datos creando una brecha 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 IA, enriquecidos con actualizaciones en tiempo real procedentes de 500 billones de señales de amenazas diarias de la mayor nube de seguridad del mundo.

- **Obtenga una experiencia de usuario incomparable:** consiga la experiencia de Internet y SaaS más rápida del mundo (hasta un 40 % más rápida que con las arquitecturas de seguridad heredadas) para aumentar la productividad y la agilidad de su empresa.

- **Reduzca costes y complejidad:** obtenga un retorno de la inversión del 139 % con Zscaler reemplazando el 90 % de sus dispositivos caros, complejos y lentos con una plataforma zero trust totalmente nativa de la nube.

- **Proteja a su plantilla híbrida:** permita que los empleados, clientes y terceros accedan de forma segura a aplicaciones web y servicios en la nube desde cualquier lugar y en cualquier dispositivo, con una excelente experiencia digital.

- **Unifique los esfuerzos de SecOps y NetOps:** obtenga resultados de seguridad más rápidos y colaborativos con herramientas compartidas, como información sobre el tráfico en tiempo real, integraciones API-first y RBAC granular.

- **Logre una soberanía total sobre datos y contenido:** imponga el cumplimiento para un acceso seguro y localizado sin sacrificar 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 desarrollo a escala:** automatice la inspección SSL/TLS de más de 30 herramientas para desarrolladores mientras se aísla código y archivos grandes o desconocidos con veredictos instantáneos de IA, todo ello sin frenar la innovación.

©2025 Zscaler, Inc. Todos los derechos reservados.

- **Digital Experience Monitoring:** reduzca la sobrecarga operativa de TI y acelere la resolución de solicitudes 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 sucursal de confianza cero:** reduzca el riesgo y la complejidad con conectividad no enrutable del centro de datos y las sucursales para usuarios, servidores y dispositivos IOT/TO.

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

Zscaler Internet Access para usuarios y cargas de trabajo

Elimine el riesgo de que las cargas de trabajo en la nube 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 a través de herramientas heredadas y centradas en la red, como las VPN, los cortafuegos (incluidos los cortafuegos virtuales) o las tecnologías WAN, puede evitar riesgos y detener el movimiento lateral sin necesidad de un entramado de herramientas de seguridad. Al aplicar el conjunto completo de capacidades de seguridad y protección de datos de ZIA a las cargas de trabajo, puede unificar la seguridad de confianza cero 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 residan en la nube pública o en un centro de datos privado.

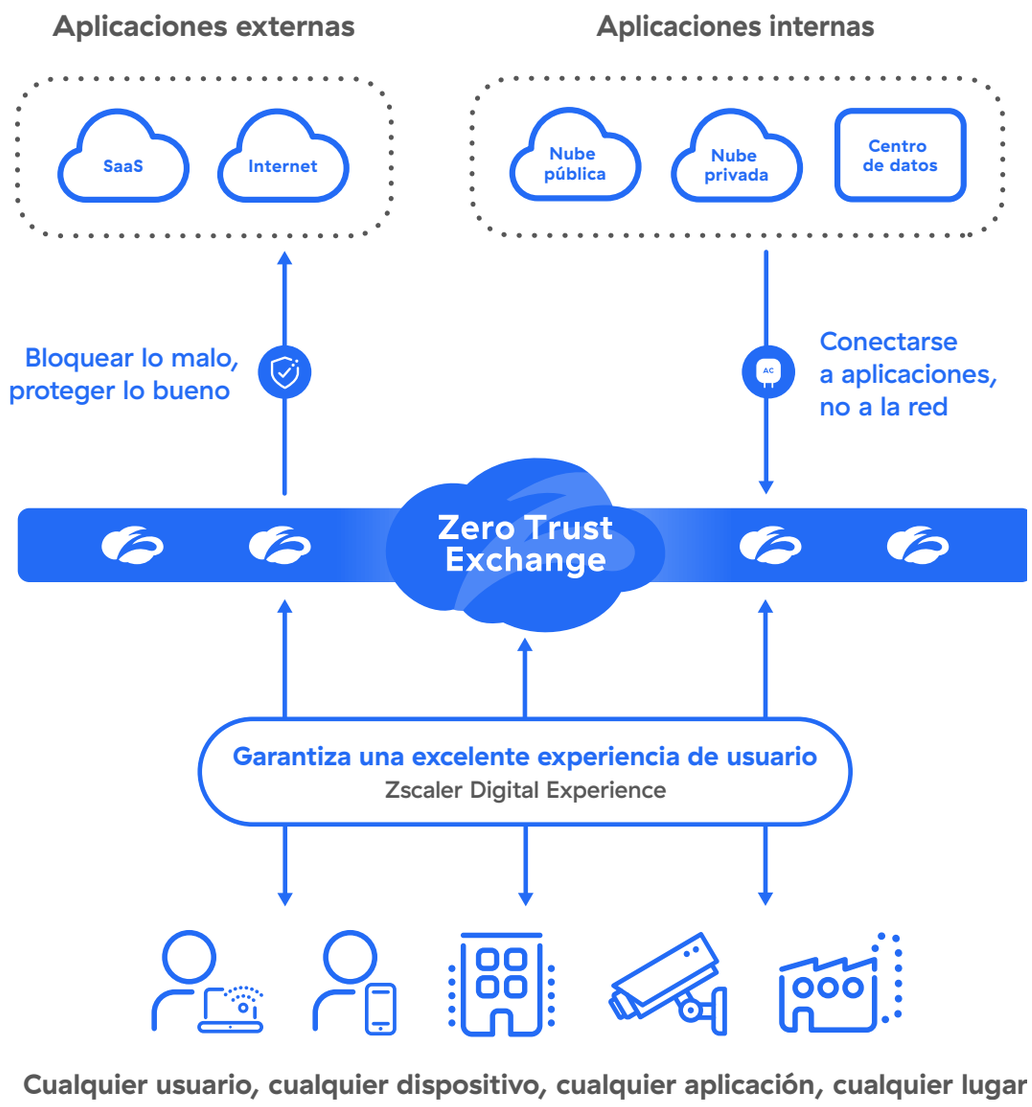


Figura 1: Zero Trust Exchange

*Gartner, Magic Quadrant for Security Service Edge, 15 de abril de 2024, Charlie Winckless, et al.

Gartner no avala ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no aconseja a los usuarios de tecnología que seleccionen solo a los proveedores con las calificaciones más altas u otra designación. Las publicaciones de investigación de Gartner recogen las opiniones de la organización de investigación de Gartner y no deben interpretarse como declaraciones de hecho. Gartner renuncia a toda garantía, expresa o implícita, con respecto a este análisis, incluida cualquier garantía de comerciabilidad o adecuación a un fin determinado.

GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en EE. UU. e internacionalmente, y MAGIC QUADRANT es una marca comercial registrada de Gartner, Inc. y/o sus filiales y se utilizan aquí con autorización. Todos los derechos reservados.

Gartner

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

VER MÁS

©2025 Zscaler, Inc. Todos los derechos reservados.

Casos de uso

PROTECCIÓN FRENTE A AMENAZAS CIBERNÉTICAS 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 la seguridad de los datos.

Más información

PERSONAL HÍBRIDO SEGURO

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

Más información

PROTECCIÓN DE DATOS

Ponga fin a la pérdida de datos de usuarios, aplicaciones SaaS e infraestructuras de nube pública por exposición accidental, robo de datos o ransomware de doble extorsión.

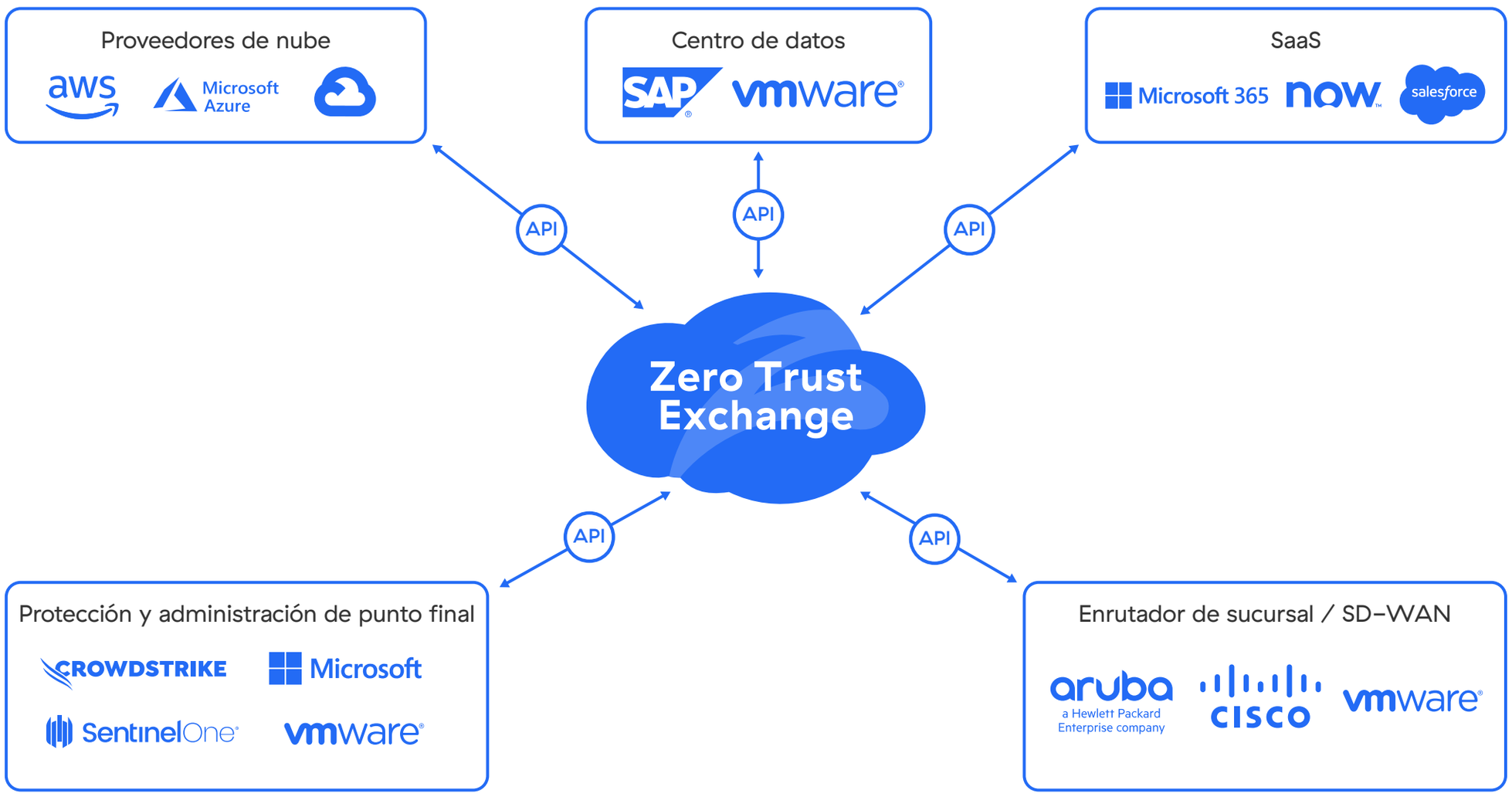
Más información

MODERNIZACIÓN DE LA INFRAESTRUCTURA

Elimine redes costosas y complejas mediante un acceso rápido, fiable, seguro y directo a la nube que elimina la necesidad de tener cortafuegos periféricos y en las sucursales.

Más información

El ecosistema Zscaler Zero Trust Exchange



©2025 Zscaler, Inc. Todos los derechos reservados.

TABLA 1: CARACTERÍSTICAS Y CAPACIDADES DE ZSCALER INTERNET ACCESS	
CARACTERÍSTICA	**DETALLES**
CAPACIDADES	
Filtrado URL	Permita, bloquee, advierta o aísle el acceso de los usuarios a categorías web o destinos específicos para detener las amenazas basadas en la web y garantizar el cumplimiento de las políticas de la organización.
Inspección 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 inspeccionar en función de los requisitos normativos o de privacidad. Integre la inspección con la herramienta para desarrolladores para proteger los flujos de trabajo de los desarrolladores.
Seguridad DNS	Identifique y dirija las conexiones que se sospecha que son de comando y control a los motores de detección de amenazas de Zscaler para una inspección completa del contenido.
IP dedicada	Proporcione acceso a aplicaciones que permitan incluir en la lista de direcciones IP aquellas direcciones IP dedicadas a su organización. También permite una transición fácil de la arquitectura heredada a Zero Trust.
Control de archivos	Bloquee o permita la descarga/carga de archivos en aplicaciones en función de aplicaciones, usuarios o grupos de usuarios.
Use su propia dirección IP	Mantenga la coherencia y el control sobre la identidad de su red y asegúrese de que en el caso de las aplicaciones de terceros o la infraestructura dependiente el tráfico se origine solo en su organización.
Control de ancho de banda	Aplique políticas de ancho de banda y dé prioridad a las aplicaciones esenciales para la empresa frente al tráfico recreativo.
Registro basado en el país	Almacene y administre registros dentro de las fronteras de un determinado país para cumplir con los requisitos de soberanía de datos que exigen que los datos relacionados con los ciudadanos se procesen de acuerdo con las leyes locales.
Protección avanzada contra amenazas	Detenga los ciberataques avanzados, como el malware, el ransomware, los ataques a la cadena de suministro, el phishing y otros, con una protección específica contra amenazas avanzadas. Establezca políticas granulares basadas en la tolerancia al riesgo de su organización.
Protección de datos en línea (datos en movimiento)	Utilice las funciones de proxy de reenvío e inspección SSL para controlar el flujo de información confidencial a destinos web y aplicaciones en la nube de riesgo en tiempo real, deteniendo las amenazas internas y externas a los datos. La protección avanzada en línea se proporciona tanto si una aplicación está sancionada como si no lo está, sin requerir registros de dispositivos de red.
Protección de datos fuera de banda (datos en reposo)	Utilice las integraciones de API para analizar las aplicaciones de SaaS, las plataformas en la nube y sus contenidos para identificar los datos confidenciales en reposo y corregirlos automáticamente revocando los recursos compartidos de riesgo o externos, por ejemplo.
Prevención de intrusiones	Obtenga una protección completa contra amenazas de botnets, amenazas avanzadas y día cero, junto con información contextual sobre el usuario, la aplicación y la amenaza. El IPS web y en la nube funciona a la perfección en Firewall, Sandbox, DLP y CASB. Implemente firmas de amenazas personalizadas utilizando Cloud Custom IPS para detectar y detener ataques dirigidos.
Política dinámica de acceso y seguridad basada en riesgos	Adapte automáticamente la seguridad y la política de acceso a los riesgos de usuario, dispositivo, aplicación y contenido.
Captura de tráfico	Captura de paquetes sin fisuras: capture fácilmente el tráfico descifrado mediante criterios específicos en los motores de políticas de Zscaler, con análisis detallados de seguridad eficientes y 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/ML avanzadas para detener los ataques de paciente cero.

©2025 Zscaler, Inc. Todos los derechos reservados.

Filtrado DNS	Controle y bloquee las solicitudes DNS frente a destinos conocidos y maliciosos.
Zero Trust Browser (aislamiento web)	Erradique las amenazas basadas en la web al entregar contenido activo como un flujo benigno de píxeles al navegador del usuario final.
Información de la correlación de amenazas	Acelere la investigación y los tiempos de respuesta con alertas contextualizadas y correlacionadas con información sobre la puntuación de la amenaza, el activo afectado, la gravedad, etc.
Aislamiento de aplicaciones	Permita un acceso seguro y sin agente desde dispositivos no gestionados a aplicaciones SaaS, en la nube y privadas con control granular sobre las acciones de los usuarios, como copiar/pegar, cargar/descargar e imprimir para detener la pérdida de datos confidenciales.
Digital Experience Monitoring (ZDX)	Obtenga una vista unificada de las métricas de rendimiento de la aplicación, la ruta de la nube y los terminales para el análisis y la resolución de problemas.
Conectividad de sucursal de confianza cero	Supervise la conectividad de sucursales a través de Zero Trust Exchange, eliminando la superficie de ataque y evitando el movimiento lateral.
Protección de la comunicación de carga de trabajo a Internet	Impida la vulneración 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 dispositivos IoT	Obtenga una vista completa de todos los dispositivos, servidores y dispositivos de usuario no administrados IoT en su empresa, con detección automatizada, supervisión continua y clasificación con AI/ML, y capacidades de etiquetado automático líderes en el sector.
Control de acceso basado en roles (RBAC)	Permisos adecuados para controlar lo que los administradores pueden editar y ver en los informes de políticas y análisis dentro de la plataforma Zscaler para evitar conflictos y mejorar la gobernanza.

©2025 Zscaler, Inc. Todos los derechos reservados.

CARACTERÍSTICA	DETALLES
CARACTERÍSTICAS DE LA PLATAFORMA	
Opciones de conectividad flexibles	• Zscaler Client Connector (ZCC): reenvía tráfico a Zero Trust Exchange a través de un agente ligero compatible con Windows, macOS, iOS, iPadOS, Android y Linux. • Túneles GRE o IPsec: utilice los túneles GRE e IPsec para enviar tráfico a Zero Trust Exchange para dispositivos sin ZCC. • Aislamiento del navegador: conecte sin problemas cualquier dispositivo BYOD o no administrado con el aislamiento integrado de Zero Trust Browser. • Encadenamiento de proxy: Zscaler admite el reenvío de tráfico de un servidor proxy a otro, pero esto no se recomienda en entornos de producción. • Archivos PAC: envíe tráfico a Zero Trust Exchange con archivos PAC para dispositivos sin ZCC.
Implementación en la nube	Plataforma 100 % nativa en la nube entregada como servicio SaaS. Para la planificación de la continuidad del negocio y otros casos de uso especiales, se encuentran disponibles perímetros de servicio privados y virtuales.
Privacidad y conservación de datos	Cuando se registran los datos, el contenido nunca se escribe en el disco y hay controles granulares para determinar dónde tiene lugar exactamente el registro. Utilice el control de acceso basado en roles (RBAC) para dar acceso de solo lectura, anonimización/ofuscación del nombre de usuario y derechos de acceso separados por departamento o función, de acuerdo con las normas de cumplimiento clave. Los datos se conservan durante un período de seis meses consecutivos o menos, dependiendo del producto. Puede comprar almacenamiento adicional que conserve los datos durante el tiempo que desee.
Certificaciones clave de cumplimiento	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.
Soporte granular de API	Mantenemos integraciones de API REST con numerosos proveedores de identidad, redes y seguridad. Por ejemplo, puede compartir registros entre Zscaler y su SIEM basado en la nube o local (como Splunk, entre otros). Más información
Interconexión directa	La interconexión directa 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.

CARACTERÍSTICA	DETALLES
ACUERDOS DE NIVEL DE SERVICIO (SLA)	
Disponibilidad	99 999 %, medido por las transacciones perdidas
Latencia del proxy	< 100 ms, incluso cuando el análisis de amenazas y DLP está activado
Captura 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 y posterior • Mac OS X 10.14 y 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 comenzar

	PLATAFORMA ESSENTIALS Comience su viaje zero trust con acceso a Internet seguro y confiable y acceso privado limitado, con otras innovaciones de Zscaler.	PLATAFORMA ZSCALER Desbloquee la solución SASE/SSE completa, que incluye acceso completo a Internet, acceso privado y protección de datos.
SERVICIOS DE PLATAFORMA		
Reenvío de tráfico: Client Connector, GRE, PAC, encadenamiento de proxy, IPsec	✓	✓
Múltiples proveedores de identidad (IdP), acceso a API, postura del dispositivo	✓	✓
Autenticación: SAML, LDAP seguro, Kerberos	✓	✓
Entorno de prueba ZS	–	–
Acceso a los controladores de dominio públicos de Zscaler	✓	✓
Acceso a centros de datos públicos de alto coste de Zscaler (Australia, Nueva Zelanda, Dubái (no regulado), Sudamérica, África, Corea del Sur, Taiwán y China continental)	–	✓
China Premium / Acceso regulado a centros de datos en Oriente Medio	–	–
ACCESO A INTERNET		
Filtrado de contenidos	✓	✓
Control de tipo de archivo	✓	✓
Inspección TLS/SSL	✓	✓
Certificado privado SSL	✓	✓
Control de ancho de banda	✓	✓
Transmisión a SIEM local (servicio de transmisión de Nanolog con gestión en vivo).	✓	✓
Nube NSS (para más de 500 usuarios)	✓	✓
Anclaje IP de origen	–	✓
Perímetro de servicio privado ZIA: dispositivo virtual	–	✓
Hardware: Perímetro de servicio privado ZIA, 3 instancias, 5 instancias	–	–

©2025 Zscaler, Inc. Todos los derechos reservados.

PROTECCIÓN CONTRA AMENAZAS CIBERNÉTICAS		
Estándar de protección contra amenazas cibernéticas: protección avanzada contra amenazas, estándar sandbox, estándar de cortafuegos Zero Trust, estándar de navegador Zero Trust	✓	✓
Antivirus y antispyware en línea	✓	✓
Advanced Sandbox	–	–
Zero Trust Firewall Advanced	–	–
Navegador Zero Trust avanzado (1,5 GB de tráfico/usuario/mes, medido en todos los usuarios del navegador Zero Trust)	–	–
Navegador Zero Trust ilimitado (sin límites de uso 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 suscritos (500 usuarios suscritos como mínimo)	✓
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 en la sombra, restricción de arrendamiento, web en línea (modo de supervisión), API SaaS (1 aplicación), seguridad de IA generativa	✓	✓
DLP en línea para web y Gen AI, todas las aplicaciones (Internet y acceso privado)	–	✓
GESTIÓN DE RIESGOS		
Estándar de gestión de riesgos: estándar de engaño	–	✓
ZERO TRUST FOR WORKLOADS		
Zero Trust for Workloads Standard: filtrado de estado, DNS, inspección TLS	1 GB de tráfico de carga de trabajo mensual por usuario suscrito	2 GB de tráfico de carga de trabajo mensual por usuario suscrito
DIGITAL EXPERIENCE (ZDX)		
ZDX Standard: preconfigurado	✓	–
ZDX Standard	–	✓
SOPORTE		
Soporte estándar	✓	✓
Soporte Plus	–	–

©2025 Zscaler, Inc. Todos los derechos reservados.

MODELO DE LICENCIA

Todas las versiones de Zscaler Internet Access tienen precio por usuario. Para ciertos productos dentro de la versión de su plataforma, los precios pueden variar independientemente del número de usuarios. Para obtener más información sobre los precios, hable con su equipo de cuentas de Zscaler.

Parte de Zero Trust Exchange global

Zero Trust Exchange habilita conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar utilizando Internet como red corporativa. Basado en el principio de confianza cero de acceso con menos privilegios, proporciona una seguridad integral utilizando la identidad basada en el contexto y la aplicación de políticas.

Lo mejor 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
Gerente sénior 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. La plataforma Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 160 centros de datos en todo el mundo, Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **zscaler.com/es** o síganos en Twitter**@zscaler.**

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/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 registrada es propiedad de sus respectivos dueños.

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

zscaler™

Zero Trust Everywhere