FICHA DE DATOS

Zscaler Internet Access

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

Zscaler Internet Access™ define el acceso a Internet y SaaS seguro y rápido con la plataforma de confianza cero más completa del sector.

La seguridad de la red heredada se ha vuelto ineficaz en un mundo que da prioridad a la nube y a los dispositivos móviles

Las arquitecturas heredadas de tipo radial 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 su organización autorizaba. Hoy en día, vivimos en un mundo completamente 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 traspasan las defensas de la red heredada. Ha llegado el momento de encontrar una solución de seguridad nativa de la nube que reduzca de forma integral el riesgo y la complejidad y que, al mismo tiempo, permita una flexibilidad que ayude a impulsar las iniciativas empresariales.

Zscaler Internet Access

Proteger la empresa de hoy en día que prioriza la nube y lo móvil requiere un enfoque fundamentalmente diferente basado en la confianza cero. Zscaler Internet Access, parte de Zscaler Zero Trust Exchange™, es la plataforma de perímetro de servicio de seguridad (SSE) más implementada del mundo, construida sobre una década de liderazgo en pasarelas web

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.
- **Modernice su arquitectura de seguridad:** obtenga un 139 % de retorno de inversión con Zscaler sustituyendo el 90 % de sus caros, complejos y lentos dispositivos por una plataforma de confianza cero totalmente nativa en la nube.

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 de confianza cero, 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 fluida que elimina el retorno, mejora el rendimiento y la experiencia de usuario, y simplifica la administración de la red, sin necesitar ninguna 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 en la nube con IA, sin hardware que gestionar, con flujos de trabajo optimizados y creación de políticas centradas en la empresa libera tiempo valioso para que su equipo se centre en objetivos estratégicos.

Servicios integrados de seguridad y protección de datos basados en la IA

Zscaler Internet Access incluye un conjunto completo de servicios de seguridad y protección de datos basados en la 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.
- **Agente de seguridad de acceso a la nube (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 la 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.

*Gartner Magic Quadrant para Security Service Edge, 10 de abril de 2023, Charlie Winckless, et al.

- **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 nuevo y elusivo malware a través protocolos de web y de transferencia de archivos con la cuarentena propiciada por la IA, compartiendo una protección uniforme y global para todos los usuarios en tiempo real.
- **Cloud Browser Isolation impulsado por IA:** erradique los ataques basados en la web y evite la pérdida de datos creando un vacío virtual entre los usuarios, la web y el SaaS.
- **Supervisión de la experiencia digital:** 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 el peligro 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 emparejar ZIA con Zscaler Private Access, puede ampliar la protección a sus aplicaciones y cargas de trabajo privadas, tanto si residen en la nube pública como en un centro de datos privado.

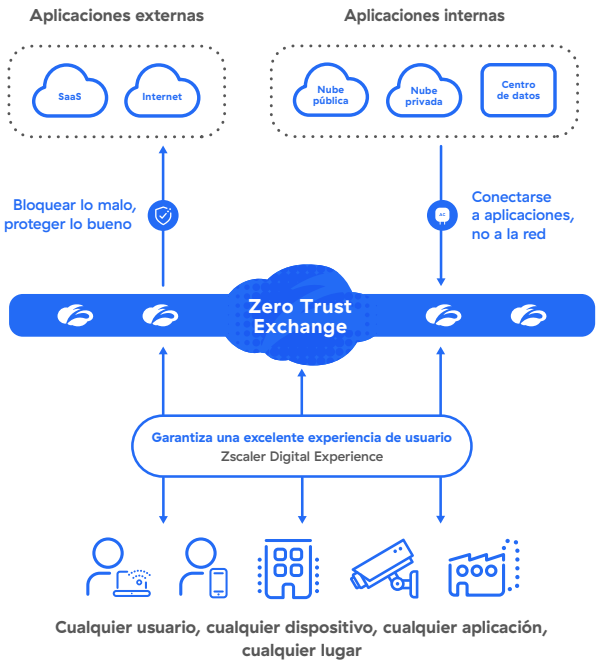

Figura 1: Zero Trust Exchange

Casos de uso

Protección frente a amenazas cibernéticas y ransomware

Pase de la seguridad de red heredada a la revolucionaria arquitectura de confianza cero de Zscaler que evita las situaciones de riesgo, elimina la superficie de ataque, detiene el movimiento lateral y protege los datos.

Más información →

Personal híbrido seguro

Capacite a empleados, socios, clientes y proveedores para que accedan de forma segura a aplicaciones web y servicios en la nube desde cualquier lugar y en cualquier dispositivo, y garantice una gran experiencia digital.

Más información →

Protección de datos

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

Más información →

Modernización de la infraestructura

Elimine las caras y complejas redes con un acceso rápido, seguro y directo a la nube que acaba con la necesidad de cortafuegos en el perímetro y en las sucursales.

Más información →

El ecosistema Zscaler Zero Trust Exchange

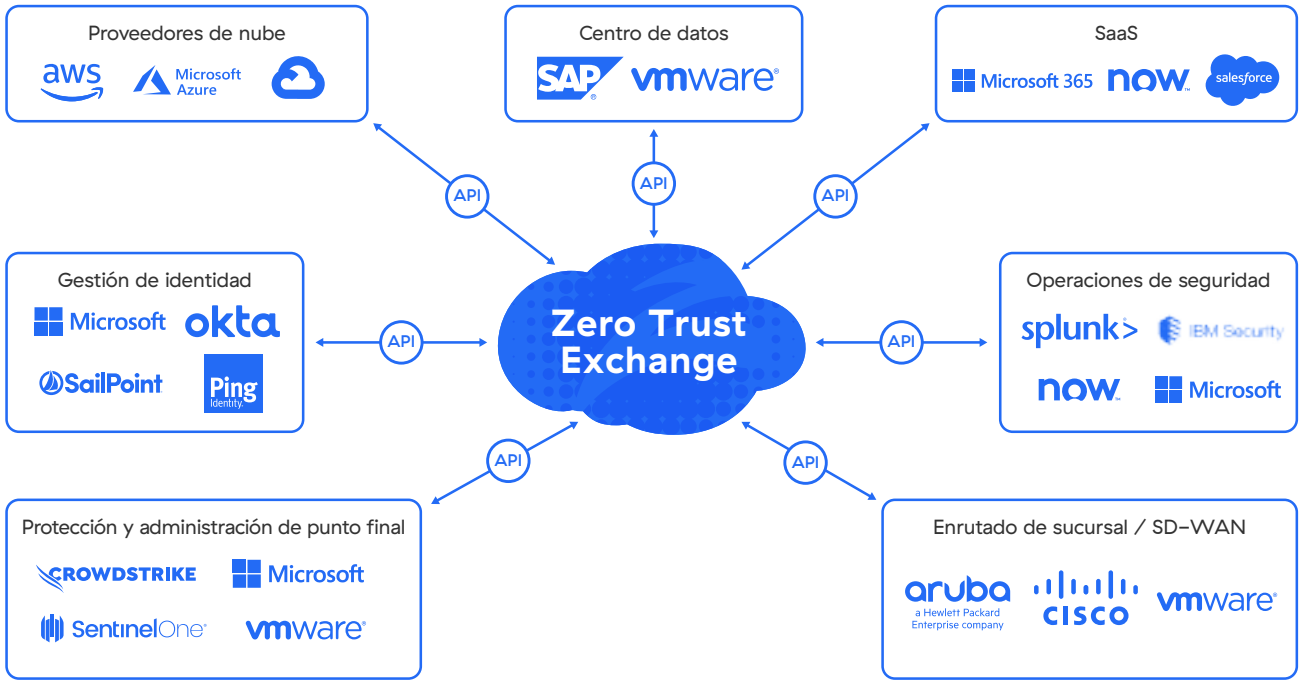

Figura 2: Ecosistema de socios de Zscaler Internet Access

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 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.
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.
Control de archivos	Bloquee o permita la descarga/carga de archivos en aplicaciones en función de aplicaciones, usuarios o grupos de usuarios.
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.
Protección avanzada frente a amenazas	Detenga los ciberataques avanzados, como el malware, el ransomware, los ataques a la cadena de suministro, el phishing, etc., con una protección patentada 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 capacidades 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 para detener 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 remediarlos 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.
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 avanzados a fin de detener los ataques de paciente cero.
Filtrado DNS	Controle y bloquee las solicitudes DNS frente a destinos conocidos y maliciosos.
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.
Supervisión de la experiencia digital	Obtenga una vista unificada de las métricas de rendimiento de la aplicación, la ruta de la nube y los extremos para el análisis y la resolución de problemas.
Conectividad de sucursal de confianza cero	Modernice 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 descubrimiento automatizado, supervisión continua y clasificación AI/ML con capacidades de etiquetado automático líderes en el sector.

CARACTERÍSTICA	DETALLES
Características de la plataforma	
Opciones de conectividad flexibles	• **Zscaler Client Connector (ZCC):** envíe 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 y/o IPsec para enviar tráfico a Zero Trust Exchange para dispositivos sin ZCC. • **Aislamiento del navegador:** conecte sin problemas cualquier dispositivo propio del usuario o no gestionado con Cloud Browser Isolation integrado. • **Encadenamiento de proxies:** Zscaler admite el reenvío de tráfico de un servidor proxy a otro, pero 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 casos de uso únicos, hay 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, anonimizar/ocultar el nombre de usuario y separar los derechos de acceso 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, en función del producto. Puede comprar almacenamiento adicional para conservar 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 Consulte la lista completa de nuestras certificaciones de cumplimiento aquí.
Soporte granular de API	Tenemos 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 (por ejemplo, Splunk). 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.
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 5 o posterior • Windows 7 y posterior • Mac OSX 10.10 y posterior • CentOS 8 • Ubuntu 20.04 Más información
Branch Connector	Compatible con: • VMware vCenter o vSphere Hypervisor • Centos • Redhat

Ediciones de Zscaler Internet Access

	Capacidades	Lo esencial	Negocios	Transformación	Ilimitado
Servicios de plataforma		Filtrado de contenido, AV en línea, inspección TLS/SSL, transmisión nanológica	Certificado privado(+) SSL	(+) Nube NSS, recuperación de registros NSS, acceso extendido a DC, túnel IPSec, alertas contextuales, ZIA Virtual Private Service Edge (8)	(+) Anclaje de IP de origen, entorno de prueba, categorización de prioridades, perímetro de servicio privado virtual ZIA (32), protección de servidor y de IoT (1 GB/10 usuarios)
Protección contra amenazas	**Protección contra amenazas avanzadas (incluye Detección de C2 y phishing impulsado por IA)** Protección contra amenazas conocidas y desconocidas (URL, AV, Botnet/C2, phishing)	comprobar	comprobar	comprobar	comprobar
	Cloud Sandbox Prevención de ataques de día cero mediante el análisis de archivos sospechosos con cuarentena impulsada por IA	Complemento	Complemento	comprobar	comprobar
	Aislamiento: protección contra amenazas cibernéticas Protección contra ataques de día cero contra contenido web sospechoso. Aislamiento basado en riesgos impulsado por IA	Complemento	Complemento	Aislamiento para protección cibernética: Estándar (100 MB/usuario/mes)	Aislamiento para protección cibernética: Standard (1,5 GB/usuario/mes)
	Información de la correlación de amenazas Acelere las investigaciones y el tiempo de respuesta con inteligencia de amenazas contextual	–	comprobar	comprobar	comprobar
	Política dinámica basada en el riesgo Adapta y recomienda automática-mente políticas de seguridad basadas en diversos factores de riesgo.	–	–	comprobar	comprobar
	Engaño integrado Impulse su postura de seguridad de confianza cero atrayendo, detectando e interceptando de forma proactiva a los atacantes activos	–	–	Estándar[1]	Estándar[1]
Transformación de red	**Resolución y filtrado de DNS** Resolvedor de DNS confiable para una resolución de DNS óptima y geocéntrica	hasta 64 reglas	hasta 64 reglas	comprobar	comprobar
	Detección de túnel DNS Detecte y prevenga ataques basados en DNS y filtración de datos a través de túneles DNS	–	–	comprobar	comprobar
	Control de ancho de banda Control de tráfico y priorización de ancho de banda, limitación de velocidad para el tráfico web		comprobar	comprobar	comprobar
	Cloud Firewall Protección de trabajo desde cualquier lugar para todos los usuarios y el tráfico (tanto web como no web) con inspección SSL infinita	Red, servicios de aplicaciones, ubicaciones, FQDN hasta 10 reglas	Red, servicios de aplicaciones, ubicaciones, FQDN hasta 10 reglas	(+) usuarios que trabajan desde cualquier lugar + ubicaciones, inspección profunda de aplicaciones de paquetes	(+) usuarios que trabajan desde cualquier lugar + ubicaciones, inspección profunda de aplicaciones de paquetes
	Protección para tráfico no autenticado Proteja las redes con seguridad de nivel de operador totalmente automatizada y con limitaciones	0,5 GB/usuario/mes	1 GB/usuario/mes	1,5 GB/usuario/mes	2 GB/usuario/mes

	Capacidades	Lo esencial	Negocios	Transformación	Ilimitado
Proteja los datos y evite la pérdida de datos	**Control de aplicaciones en la nube + Restricciones de arrendamiento** Encuentre y controle el uso de aplicaciones de riesgo o no autorizadas (TI en la sombra)	comprobar	comprobar	comprobar	comprobar
	Aislamiento – Protección de datos (SaaS) Evite la pérdida de datos de aplicaciones SaaS en dispositivos propios del usuario o puntos finales no administrados (sin cliente)	Complemento	Complemento	Complemento	Aislamiento para Protección de datos (SaaS): Std. (100 MB/ usuario/mes)
	DLP, CASB, Inline Web Essentials, API SaaS (1 aplicación) Evite la pérdida de datos confidenciales a Internet. Analice 1 aplicación SaaS en busca de intercambio peligroso de datos confidenciales o malware	–	Estándar de protección de datos (DLP y CASB Essentials)	(+) Análisis retro de API de SaaS	comprobar
	API SaaS, seguridad de la cadena de suministro SaaS, dispositivos no administrados, clasificación, gestión de incidentes Ventajas de Standard Data Protection plus: control de riesgos con transmisión de datos como píxeles, análisis SaaS para detectar intercambios peligrosos/malware, personalización de DLP con EDM, IDM, OCR, gestión de incidentes y automatización de flujos.	Complemento	Complemento	Complemento	comprobar
Supervisión de la experiencia digital	Supervise las experiencias digitales desde la perspectiva del usuario final para optimizar el rendimiento y solucionar rápidamente los problemas de aplicaciones, red y dispositivos.	–	Estándar	Estándar	Estándar
Premium Support Plus		Complemento	Complemento	Complemento	comprobar

Modelo de licencia

Todas las ediciones de Zscaler Internet Access tienen un precio por usuario. Para ciertos productos dentro de su edición, los precios pueden variar al margen del número de usuarios. Para obtener más información sobre los precios, hable con su equipo de cuenta 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.

> “Cuando otras empresas sufren ataques de ransomware, miles de sistemas en su entorno se debilitan, además de sufrir las graves consecuencias de tener que pagar un rescate. Cuando este tipo de suceso llega a las noticias, los ejecutivos me llaman preocupados y me siento de maravilla al decirles: "Lo tenemos controlado"”.
>
> **Ken Athanasiou,** vicepresidente y CISO de AutoNation

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