Libro electrónico

Los principales casos de uso de SSE para la protección de datos

Cómo detener las infracciones de datos en el mundo empresarial moderno con Zscaler SSE

Índice

El aumento de SSE

En el pasado, los usuarios y las aplicaciones de las organizaciones se encontraban en las instalaciones, lo que daba lugar a una seguridad de tipo castillo y foso a través de costosos dispositivos que creaban perímetros de red para proteger los datos que se encontraban dentro de ellos.

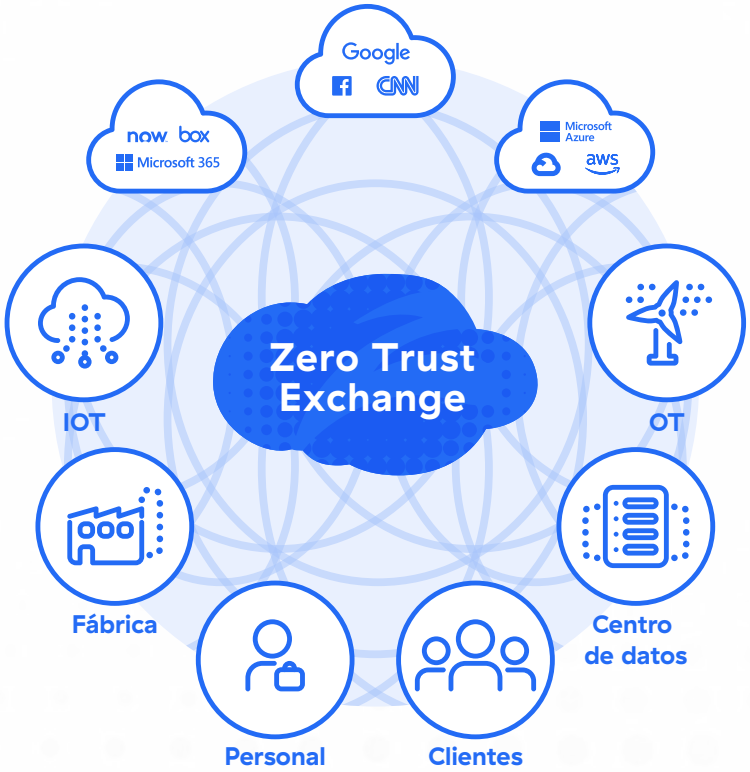
Con la nube, la web y el trabajo a distancia, el castillo ha desaparecido, pero muchos siguen confiando en las arquitecturas de castillo y foso. Lamentablemente, las pilas complejas de dispositivos no pueden abordar las necesidades modernas de protección de datos y la revisión del tráfico genera un rendimiento deficiente, limita la escalabilidad y dificulta la productividad del usuario.

Muchas herramientas modernas de protección de datos también se quedan cortas, concretamente cuando se centran en las amenazas internas e ignoran las externas que tienen como objetivo los datos. En otras palabras, una protección adecuada de los datos debe ser integral con una seguridad sólida.

Security Service Edge (SSE) es la solución a estos desafíos. Se refiere a plataformas completas que reducen la complejidad y llenan las lagunas modernas de protección de datos mediante la integración de CASB, SWG, ZTNA, y más. A través de la seguridad en el perímetro proporcionada por la nube, SSE ofrece el máximo rendimiento, escalabilidad y experiencia del usuario.

Zscaler**Zero Trust Exchange**™ es la mayor nube de seguridad del mundo y fue diseñada para asegurar cualquier transacción mucho antes de la creación de SSE. Detiene todos los riesgos internos y externos que tienen como objetivo datos.

Continúe leyendo para conocer los casos de uso de protección de datos en los que los clientes aprovechan nuestro SSE.



Lograr la seguridad de confianza cero

Las herramientas de seguridad heredadas amplían el acceso sin restricciones a la red en su conjunto (y a todos los datos y aplicaciones que contiene). Pero esto permite el movimiento lateral de amenazas entre los recursos, que puede potenciar los efectos de las infracciones de datos. Incumple el principio de confianza cero de privilegios mínimos, según el cual los usuarios autorizados solo reciben acceso al recurso que necesitan, en el momento en que lo necesitan.

El intercambio de confianza cero

Zero Trust Exchange adopta un enfoque fundamentalmente diferente y ofrece una protección de datos moderna y de confianza cero. Al servir como conmutador inteligente entre usuarios, aplicaciones SaaS, aplicaciones privadas, IoT/OT y más, Zscaler extiende el acceso seguro solo a los recursos individuales según corresponda, todo ello mientras aplica medidas de prevención de pérdida de datos (DLP) para obtener una granularidad adicional.

La ventaja de Zscaler

- Oculta todos los recursos de TI detrás de Zero Trust Exchange para eliminar la superficie de ataque
- Evita el movimiento lateral de amenazas conectando a los usuarios directamente a las aplicaciones, no a la red
- Detiene los riesgos protegiendo todas las transacciones entre usuarios, aplicaciones y máquinas

Evitar la pérdida de datos mediante el tráfico cifrado

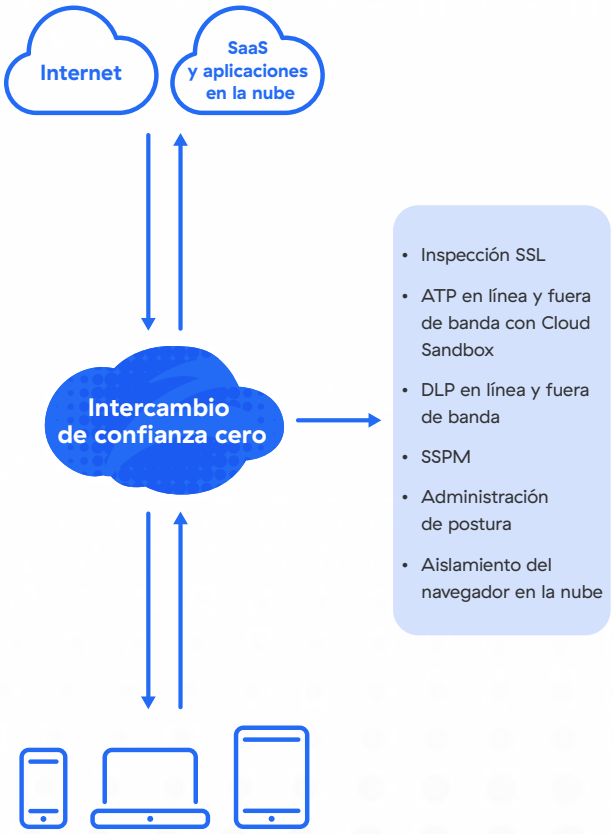
Los dispositivos de seguridad heredados (ya sean virtuales o de hardware) a menudo se utilizan para inspeccionar el tráfico web en busca de pérdida de datos. Pero los dispositivos tienen capacidades fijas para prestar servicio a los usuarios, no pueden manejar el tráfico cifrado a escala y, como resultado, proporcionan poca o ninguna inspección SSL. Con más del 95 % del tráfico web cifrado, esto es una debilidad peligrosa.

Una verdadera arquitectura en la nube

Basado en la mayor nube de seguridad del mundo, el perímetro de servicio de seguridad Zscaler ofrece el rendimiento necesario para inspeccionar el tráfico cifrado a escala para corporaciones globales con cientos de miles de usuarios. Esto garantiza que cualquier posible pérdida de datos oculta a través de SSL se detecte y corrija correctamente en tiempo real.

La ventaja de Zscaler

- Un perímetro de servicio de seguridad con escalabilidad y rendimiento incomparables que procesa más de 200 000 millones de ransacciones diarias
- Una plataforma construida sobre una arquitectura probada en línea que utiliza más del 25 % de las empresas de la lista Forbes Global 2000
- Una presencia global de más de 150 centros de datos que ofrecen seguridad en el perímetro para una experiencia de usuario excepcional



Detener el ransomware de doble extorsión

Además de cifrar los dispositivos, el ransomware de doble extorsión roba datos y amenaza con filtrarlos si no se paga un rescate. Estas amenazas utilizan blancos fáciles (como datos en reposo no protegidos y aplicaciones mal configuradas) para propagar y exfiltrar datos. Desafortunadamente, los dispositivos de seguridad heredados no pueden evitar esto en nuestro mundo que prioriza la nube.

Protección total de datos y frente a amenazas

Zscaler ofrece una protección completa frente a amenazas para detener el ransomware en el momento de la carga y en reposo en todo el ecosistema de TI. Además, DLP y CASB examinan todos los canales de datos en la nube para detener la exfiltración, mientras que la gestión de la postura y SSPM descubren los errores de configuración de las aplicaciones en la nube que exponen los datos.

La ventaja de Zscaler

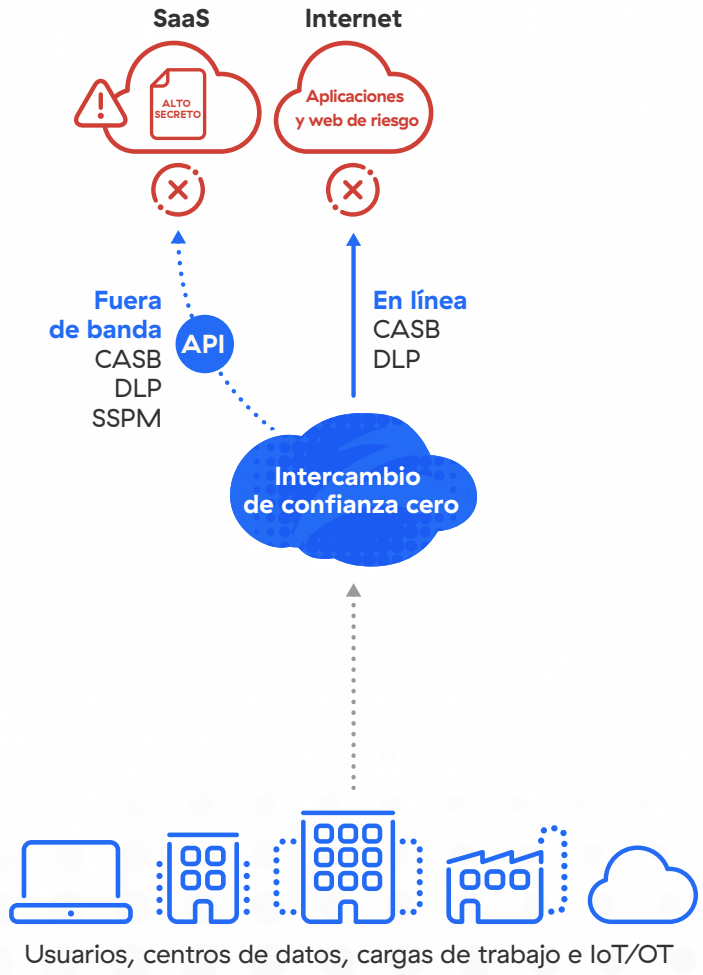
- Inspección SSL completa y escalable para identificar en tiempo real la exfiltración de datos y el ransomware en tránsito
- Tecnología de sandboxing en la nube para detener el ransomware de día cero tanto en línea como fuera de banda
- El poder de la mayor nube de seguridad del mundo: las amenazas que se encuentran en cualquier lugar se bloquean en todas partes

Proteger las aplicaciones SaaS

Las aplicaciones SaaS ofrecen una productividad y flexibilidad sin precedentes, pero pueden conducir fácilmente a la pérdida de datos si no se protegen adecuadamente. Esto se debe a que los usuarios suben regularmente datos a aplicaciones no autorizadas, los archivos en reposo se pueden compartir fácilmente con partes no autorizadas y las malas configuraciones pueden comprometer la postura de seguridad de la aplicación y exponer los datos.

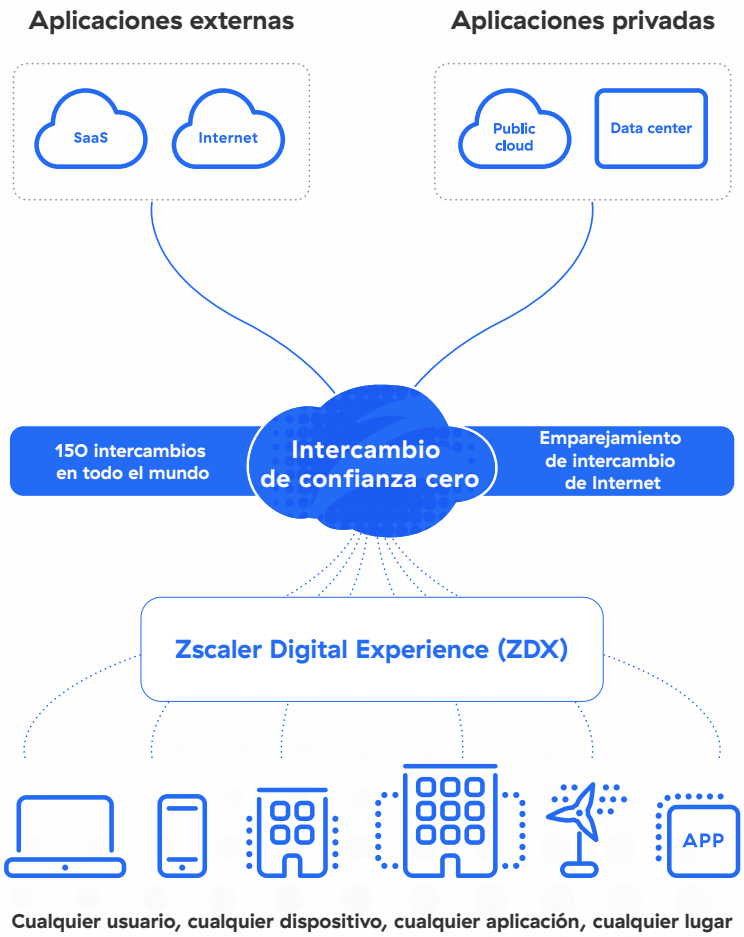
CASB con DLP

Zscaler asegura el uso de las aplicaciones SaaS al descubrir automáticamente la TI en la sombra, controlar las cargas de datos en aplicaciones en la nube no autorizadas y proteger los datos en reposo en aplicaciones en la nube sancionadas. Además, la gestión de la postura de seguridad de SaaS analiza las aplicaciones en busca de configuraciones erróneas que podrían exponer los datos o comprometer el cumplimiento.



La ventaja de Zscaler

- Protección de datos unificada que protege de manera sistemática todos los canales de datos SaaS y en la nube con una única política
- Funcionalidad CASB de alto rendimiento como parte del perímetro de servicio de seguridad más probado e integrado
- DLP en la nube completa con capacidades avanzadas como EDM y OCR para proteger valores específicos y datos de imagen



Proteger los datos para usuarios remotos

El trabajo a distancia ha llegado para quedarse, pero la seguridad heredada no fue diseñada para este nuevo estilo de actividad empresarial. El aprovechamiento de la VPN y el retorno del tráfico de los usuarios a los dispositivos de seguridad genera una escalabilidad insuficiente, perjudica la productividad de los usuarios y no aborda los casos de uso modernos de protección de datos que las empresas que priorizan la nube necesitan resolver.

Seguridad entregada en la nube en el perímetro

Con la nube de seguridad más grande y más probada del mundo, Zscaler cuenta con la escala y la experiencia necesarias para defender los datos a la vez que habilita el trabajo remoto en todo el mundo. Zscaler es capaz de asegurar el uso de SaaS, IaaS, PaaS, la web y las aplicaciones privadas sin tener que retornar el tráfico a un dispositivo, garantizando la protección global de los datos con el máximo rendimiento.

La ventaja de Zscaler

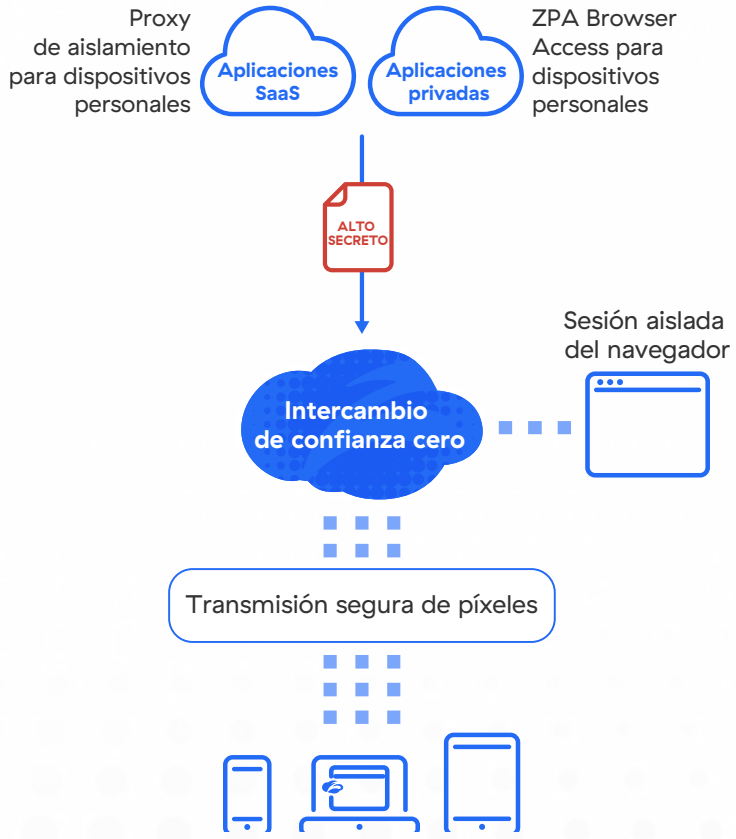
- Una nube de seguridad global con más de 150 centros de datos proporciona una seguridad de datos de alto rendimiento en el perímetro
- Una oferta de seguridad como servicio elimina la necesidad de retornar datos a los dispositivos de hardware y virtuales
- Una arquitectura de paso único con CASB, SWG, ZTNA y más ofrece una protección completa y eficiente, en cualquier lugar

Asegurar los dispositivos personales y otros no gestionados

Los puntos finales no corporativos o no gestionados, como los dispositivos personales y B2B, suelen tener motivos válidos para acceder a las aplicaciones corporativas, pero el departamento de TI pierde el control una vez que descargan los datos. Desafortunadamente, bloquear estos dispositivos interrumpe la productividad, las instalaciones de agentes de software generalmente no son viables y los proxies inversos con frecuencia se rompen. Entonces, ¿qué debe hacer TI?

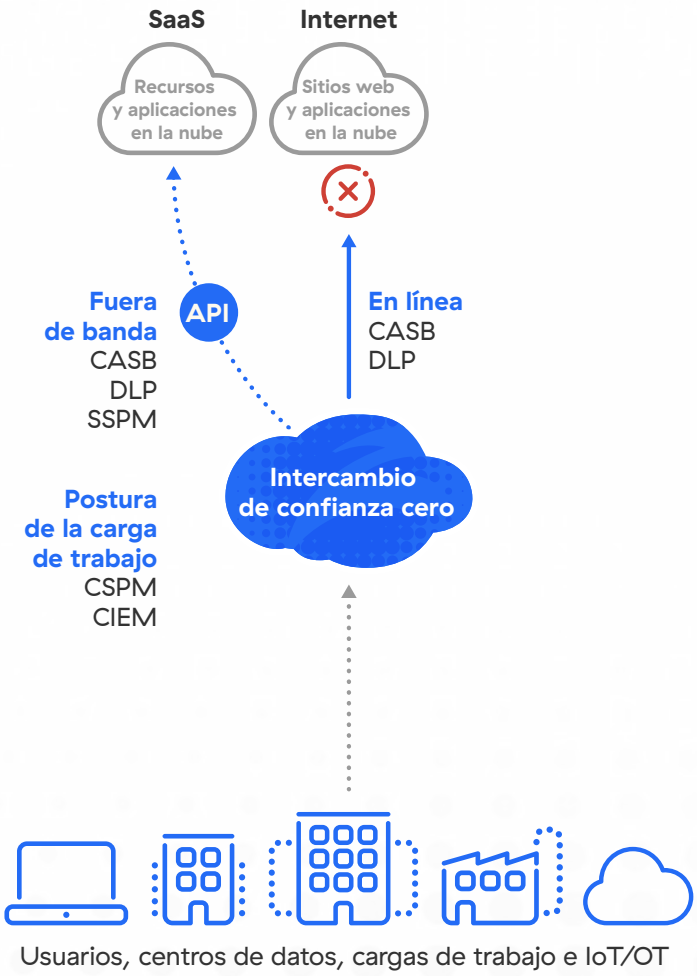
Aislamiento del navegador en la nube

Con el aislamiento del navegador sin agentes, Zscaler virtualiza la sesión de la aplicación de un usuario en un entorno aislado y transmite exclusivamente los píxeles al punto final, impidiendo la descarga, la copia, el pegado y la impresión. Esto significa que TI puede permitir el acceso no gestionado a los dispositivos mientras mantiene los datos seguros y evita los desafíos de los agentes y los proxies inversos. También evita la carga de archivos infectados desde puntos finales de riesgo.



La ventaja de Zscaler

- Aislamiento del navegador en la nube basado en la nube de seguridad más grande y con el mayor rendimiento del mundo
- Proxy de aislamiento para una seguridad sin agentes en cualquier dispositivo que acceda a cualquier aplicación SaaS
- ZPA Browser Access para un acceso seguro a las aplicaciones privadas sin instalaciones de software en el cliente



Alcanzar el cumplimiento normativo

Los datos regulados por el RGPD o la HIPAA, entre otros, salen de las instalaciones con el resto de la información confidencial de la empresa, pero las herramientas heredadas son incapaces de protegerlos y mantener el cumplimiento en la nube. Esto es de vital importancia, ya que el incumplimiento de leyes de privacidad como la CCPA y marcos como el PCI DSS puede dar lugar a multas, a la pérdida de confianza de los consumidores y a la reducción de los ingresos.

Garantía de cumplimiento total

Creamos el perímetro de servicio de seguridad Zscaler teniendo en cuenta el cumplimiento normativo. La solución brinda visibilidad y control completos en todo el ecosistema de TI para garantizar que los datos regulados estén seguros, que las aplicaciones no contengan vulnerabilidades que obstaculicen el cumplimiento y que los principios de la confianza cero se apliquen en todas partes.

La ventaja de Zscaler

- DLP en la nube con funcionalidad CASB multimodo que protege los datos regulados en movimiento y en reposo
- Se mantiene el cumplimiento: Zscaler no descarga datos para inspección, ni siquiera para medidas como la coincidencia exacta de datos
- Zscaler SSPM y administración de postura para encontrar y corregir errores de configuración y derechos que conduzcan a incumplimiento

Conseguir una protección de datos consistente y manejable

Confiar en una mezcla de productos específicos inconexos con capacidades dispares crea una serie de desafíos. En particular, genera una protección de datos incoherente en un ecosistema informático cada vez más complejo. Además, los administradores que supervisan innumerables soluciones en silos se enfrentan a una enorme carga de gestión.

Una plataforma todo en uno

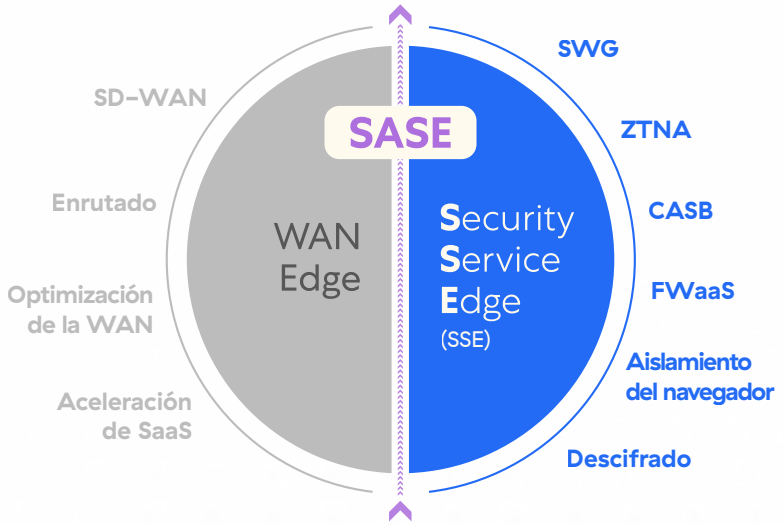
Zscaler SSE integra tecnologías líderes que pueden proteger cualquier transacción y defender los datos dondequiera que vayan, de manera consistente y completa. A través de una oferta integral en la nube con una arquitectura de paso único, la empresa también puede reducir la complejidad de la TI al tiempo que alivia la carga de gestión para los administradores.

La ventaja de Zscaler

- Protección consistente de los datos para todas las aplicaciones SaaS, de nube, web y privadas
- Simplificación de la arquitectura que reduce los productos y dispositivos puntuales
- Facilidad de gestión consolidada que evita la duplicación de políticas y ahorra tiempo a los administradores

Política de seguridad consistente

Protección de datos y frente a amenazas



Experiencia de usuario consistente

Acceso de confianza cero

La nube y la movilidad ofrecen innumerables beneficios de productividad y flexibilidad, pero para aprovecharlos sin comprometer la seguridad de los datos, debe adoptar un nuevo enfoque de ciberseguridad. El perímetro de servicio de seguridad Zscaler potencia a su empresa para que adopte la transformación digital y, al mismo tiempo, protege los datos dondequiera que vayan.

- **Conozca lo que opinan los clientes sobre Zscaler SSE**
- **Lea el Cuadrante Mágico para Security Service Edge**

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 basado en SASE 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