FICHA DE DATOS

Zero Trust Cloud

Proteja el tráfico de carga de trabajo a Internet y de carga de trabajo a carga de trabajo con Zscaler Zero Trust Exchange™.

La transformación digital está impulsando la utilización de cargas de trabajo en una amplia gama de entornos de infraestructura local, de nube privada y de nube pública. Su empresa funciona con estas cargas de trabajo, por lo que prevenir los ciberataques y la pérdida de datos es esencial.

Las arquitecturas de soluciones tradicionales son inadecuadas: brindan protección de datos y frente a amenazas inconsistente, aumentan la superficie de ataque, dejan la puerta abierta al movimiento lateral y aumentan la complejidad y los costes operativos.

Zscaler Zero Trust Cloud simplifica radicalmente la seguridad de la carga de trabajo híbrida. Con el poder de la plataforma Zero Trust Exchange, protege el tráfico de salida de carga de trabajo a Internet y de carga de trabajo a carga de trabajo a través de la nube pública y los centros de datos locales para sus cargas de trabajo y servidores de misión crítica.

Zero Trust Cloud proporciona protección de datos y frente a amenazas uniforme, elimina la superficie de ataque, detiene el movimiento lateral, reduce la complejidad y disminuye los costes operativos.

> “Con Workload Communications de Zscaler, podemos estandarizar fácilmente las políticas de seguridad tanto para los usuarios como para las aplicaciones, independientemente de dónde se encuentren.”
>
> **Rui Cabeço,** director de Conectividad Saliente, Siemens

Desafíos con la seguridad heredada de carga de trabajo y del servidor

Muchas empresas dependen de arquitecturas heredadas para proteger sus cargas de trabajo en la nube. La mayoría hará una combinación de lo siguiente:

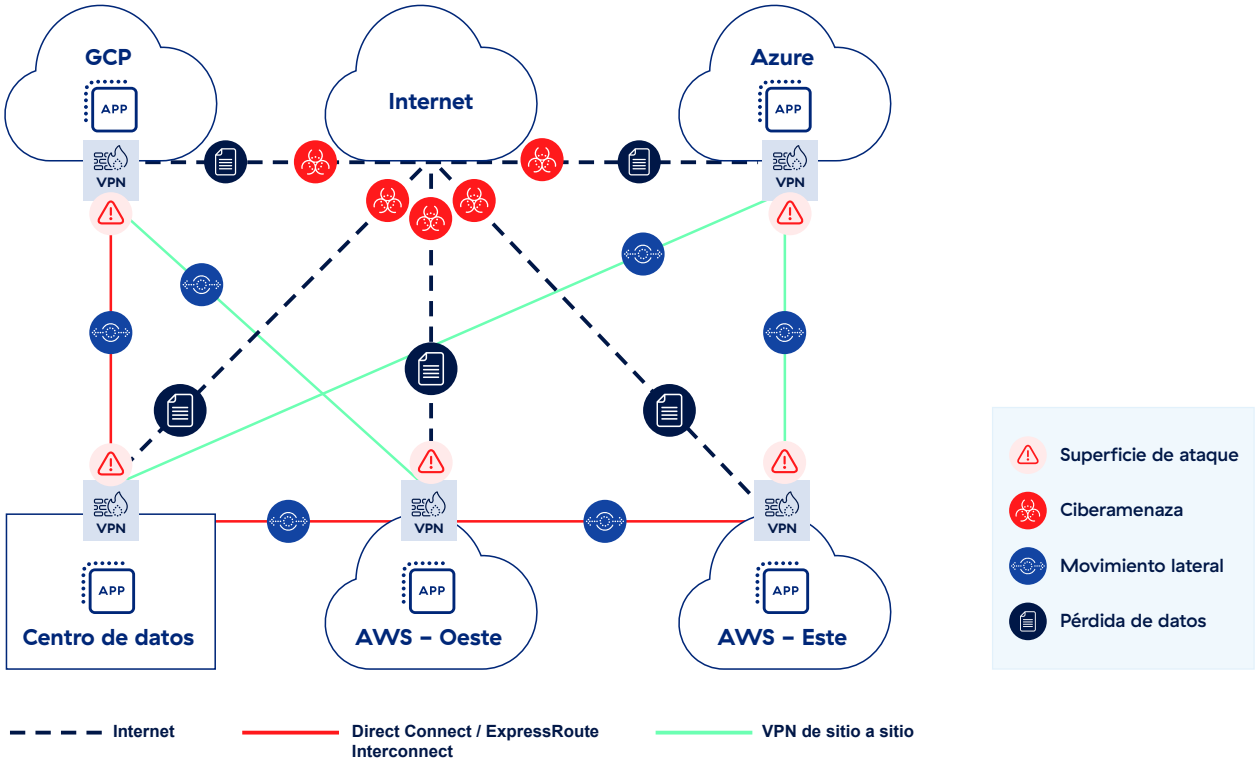
Configurar soluciones de seguridad nativas ofrecidas por proveedores de servicios de nube pública

Desplegar herramientas de terceros (cortafuegos, inspección TLS/SSL, DLP, etc.) para obtener capas adicionales de protección

Retornar el tráfico a la infraestructura de seguridad de red local para inspección y protección

El uso de estos métodos supone varios desafíos, entre ellos:

- **Aumento de la superficie de ataque y oportunidad de movimiento lateral.** Las soluciones como los cortafuegos extienden la red a las cargas de trabajo y los servidores, lo que amplifica los riesgos de movimiento lateral. Cada cortafuegos en contacto con Internet también aumenta la superficie de ataque. Esto puede extender Internet a diferentes nubes y entornos locales. Además, un mosaico de dispositivos virtuales, herramientas operativas y políticas no estándar introduce brechas tanto conocidas como desconocidas en la cobertura de seguridad, lo que aumenta el riesgo de seguridad.
- **Brechas de visibilidad de TLS.** La inspección de TLS puede utilizar recursos informáticos significativos y plantear desafíos, como la degradación del rendimiento, cuando está habilitada. La gestión de certificados distribuidos o la aplicación de exclusiones a cargas de trabajo ancladas genera desafíos operativos. Además, suele generar mayores costes de infraestructura de ciberseguridad para acomodarse a la escala.
- **Mayor complejidad y bajo rendimiento.** Debido a que las soluciones de seguridad y redes heredadas no se diseñaron teniendo en cuenta las cargas de trabajo en la nube, se deben incorporar productos puntuales como cortafuegos virtuales, servidores proxy y puertas de enlace NAT. Algunas soluciones pueden utilizar máquinas virtuales independientes para cada función de seguridad, lo que da lugar a una inspección secuencial al estilo de una línea de ensamblaje que aumenta la latencia. Esto genera complejidades operativas significativas cuando se aplica en entornos multinube.
- **Costes elevados.** El uso de productos de seguridad de red heredados (por ejemplo, cortafuegos, IPS, enrutadores), el exceso de aprovisionamiento de infraestructura de seguridad de red para compensar la falta de escalabilidad y el uso creciente de servicios nativos de la nube contribuyen a un aumento de los gastos de capital y operativos.
- **Falta de un registro común.** Los mandatos legales y reglamentarios pueden exigir que las organizaciones almacenen registros durante períodos prolongados. Acceder a estos registros desde diferentes entornos de nube y almacenarlos en una infraestructura SIEM central puede ser complejo y caro.



Ampliar la arquitectura zero trust a las nubes públicas y a los centros de datos locales

Zero Trust Cloud elimina la superficie de ataque de la red al conectar cargas de trabajo y servidores a Internet y aplicaciones privadas con una arquitectura zero trust. Esto simplifica drásticamente la conectividad al reducir la dependencia de su organización de soluciones heredadas como cortafuegos, al tiempo que permite un reenvío flexible y facilita la gestión de políticas con el marco de políticas probado de Zscaler Internet Access™ (ZIA) y Zscaler Private Access™ (ZPA).

Todo esto es posible gracias a la plataforma Zero Trust Exchange, que opera a hiperescala y puede manejar cualquier aumento en la carga de trabajo o el tráfico del servidor con ajuste elástico y horizontal. Con Zero Trust Cloud, todo el tráfico de salida del servidor y de la carga de trabajo se reenvía a Zero Trust Exchange, donde se pueden aplicar control de acceso e inspección TLS/SSL completos.

Posteriormente, el tráfico de salida se reenvía a su destino previsto, ya sea Internet, aplicaciones SaaS u otras cargas de trabajo y servidores alojados en otras nubes públicas o centros de datos.

Con Zero Trust Cloud, puede:

Obtener una protección de datos y amenazas consistente y completa

Aplique políticas comunes en todos los entornos

- Evite ataques de día cero con inspección TLS a escala de la nube y protección contra amenazas
- Detenga las filtraciones de datos con la inspección de DNS y la protección de datos en línea
- Limitar los destinos a los que las cargas de trabajo y los servidores pueden acceder con controles estrictos

Eliminar la superficie de ataque y el movimiento lateral

Conecte aplicaciones, no redes: vuélvase invisible

- Aplique acceso con privilegios mínimos a las cargas de trabajo del segmento mediante IP, FQDN, VPC, VNet o etiquetas
- Conecte cargas de trabajo mediante Zero Trust Exchange, eliminando la superficie de ataque de la red
- Soporte de nube a nube, de nube a centro de datos, de región a región

Reduzca la complejidad y el coste operativos

Utilice una plataforma en la nube para proteger todas las cargas de trabajo

- Proteja las cargas de trabajo en todos los principales proveedores de servicios en la nube, incluidos AWS, Azure y GCP, mediante una plataforma unificada
- Automatice las implementaciones de seguridad a través de interfaces programables utilizando plantillas de infraestructura como código (IaC)
- Utilice integraciones de proveedores de servicios de nube pública, como el equilibrador de carga de puerta de enlace de AWS, las etiquetas definidas por el usuario de AWS y el escalado automático de AWS.

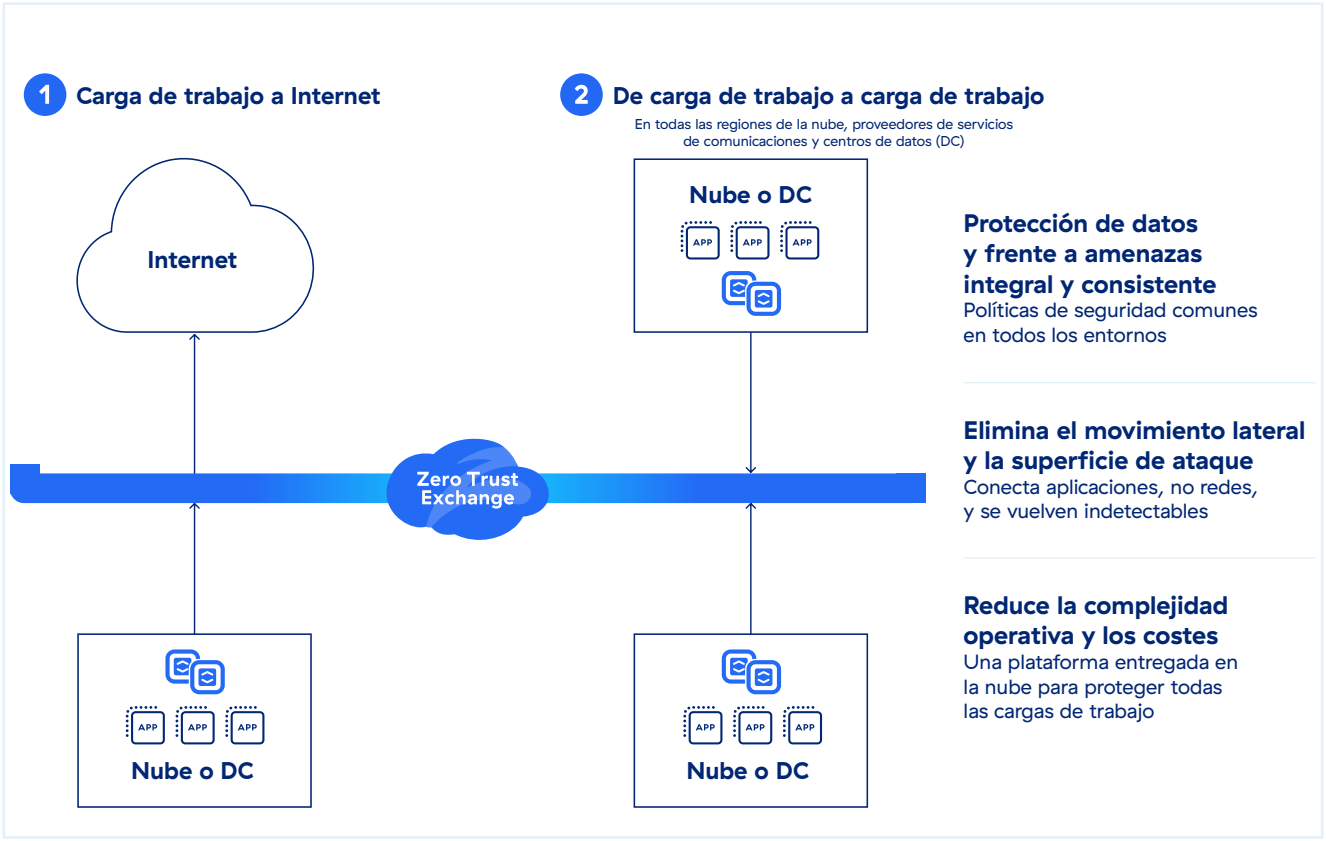


FIGURA Zscaler Zero Trust para cargas de trabajo

Capacidades de Zero Trust Cloud

Zero Trust Cloud se basa en Zscaler Zero Trust Exchange, que permite la conexión segura de usuarios, dispositivos y aplicaciones mediante políticas empresariales en cualquier red y en cualquier nube, a escala.

Arquitectura de proxy zero trust: nuestra arquitectura de proxy multiinquilino especialmente diseñada que se sitúa en línea para conectar de forma segura fuentes y destinos al tiempo que proporciona visibilidad completa del tráfico de salida.

Descifrado TLS a escala de la nube: la inspección de alto rendimiento se realiza mediante una arquitectura de acceso múltiple y análisis único diseñada para escalar.

Segmentación granular de aplicación a aplicación: el acceso con privilegios mínimos y de zero trust para todas las cargas de trabajo y servidores proporciona una gestión y aplicación de políticas comerciales simplificadas.

Inspección de amenazas bidireccional: la protección contra amenazas impulsada por IA (con 500 billones de señales diarias y 320 mil millones de transacciones diarias) ofrece protección hermética y permanente frente a ransomware, prevención de amenazas de día cero y prevención de malware desconocido.

Protección de datos en línea: inspección DLP escalable y de alto rendimiento en todos los canales y ubicaciones

Plataforma común, compatible con múltiples nubes: una plataforma unificada ofrece administración de políticas, supervisión del tráfico y seguimiento de registros. Las políticas estandarizadas se aplican en AWS, Azure, GCP y centros de datos locales.

Características de Zero Trust Cloud

PLATAFORMA ZSCALER ZERO TRUST CLOUD	
CARACTERÍSTICA	**DETALLES**
Nube pública y cobertura local	Compatible con la protección de cargas de trabajo en las regiones de AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure China y AWS GovCloud con soporte adicional para servidores de centros de datos locales. Certificado por FedRamp para AWS GovCloud.
Inspección TLS/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.
Transmisión de registros	Consolide registros de todas las cargas de trabajo y servidores, a nivel global, en un depósito central determinado por su organización, con Zscaler Nanolog Streaming Service. Los administradores pueden ver y extraer datos de transacciones mediante cargas de trabajo en la nube en tiempo real.
Infraestructura como código	Zscaler proporciona plantillas y proveedores de Terraform que automatizan el aprovisionamiento y la implementación de políticas de seguridad y máquinas virtuales de conectores en la nube.
Soporte de conectividad	Aproveche IPsec, GRE o Cloud Connectors para dirigir el tráfico de salida de la carga de trabajo al Zero Trust Exchange. IPsec y GRE protegerán el tráfico de la carga de trabajo a Internet. Cloud Connectors se utilizan para proteger el tráfico de Internet y de carga de trabajo.

ACCESO A INTERNET DE ZSCALER PARA CARGA DE TRABAJO A INTERNET	
CARACTERÍSTICA	**DETALLES**
Comunicación de carga de trabajo a Internet Protección	Evite las amenazas cibernéticas y la pérdida de datos en las comunicaciones de carga de trabajo a Internet. Incluye inspección SSL, IPS, filtrado de URL y protección de datos para todas las comunicaciones.
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.
Amenaza avanzada Protección	Detenga los ciberataques avanzados, como el malware, el ransomware, los ataques a la cadena de suministro y otros, con una protección específica frente a amenazas avanzadas. Establezca políticas granulares basadas en la tolerancia al riesgo de su organización.
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.
Prevención de intrusiones	Obtenga una protección completa frente a amenazas de botnets, amenazas avanzadas y día cero, junto con información contextual sobre las cargas de trabajo. El IPS web y en la nube funciona a la perfección en cortafuegos, sandbox y DLP.
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.
Filtrado DNS	Controle y bloquee las solicitudes DNS frente a destinos conocidos y maliciosos.
Control de archivos	Bloquee o permita la carga/descarga de archivos a aplicaciones basadas en la identidad de la carga de trabajo o la aplicación.
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.
Política dinámica de acceso y seguridad basada en riesgos	Adapte automáticamente la política de seguridad y acceso a las cargas de trabajo, servidores, destinos de Internet y riesgos de contenido.
Amenaza correlacionada Insights	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.
Filtrado de contenidos y reglas con estado	Filtre por política en 6 clases, 101 categorías y 29 supercategorías. Aproveche la clasificación de contenido dinámico para URL desconocidas y la búsqueda segura. Aplique políticas granulares por dirección IP, grupos e identidades alojadas.

ACCESO PRIVADO A ZSCALER PARA CARGAS DE TRABAJO A CARGAS DE TRABAJO	
CARACTERÍSTICA	**DETALLES**
Segmentación de carga de trabajo a carga de trabajo	Proteja la conectividad y la comunicación entre cargas de trabajo en entornos híbridos y multinube.
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.
Impulsada por IA Segmentación de aplicaciones	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.
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.

PROTECCIÓN DE DATOS	
CARACTERÍSTICA	**DETALLES**
Protección de datos en línea (datos en movimiento)	Para carga de trabajo a Internet y carga de trabajo a carga de trabajo, 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 o no gestionada, sin requerir registros de dispositivos de red.
Coincidencia exacta de datos (EDM)	Huella digital y datos seguros personalizados de la empresa.
Coincidencia de documentos indexados (IDM)	Digitalización de huella y protección de documentos y formularios personalizados.
Reconocimiento óptico de caracteres (OCR)	Encuentre y evite la pérdida de datos en imágenes y capturas de pantalla.

(Las capacidades enumeradas no son exhaustivas en su conjunto. Es posible que algunas funciones y capacidades específicas sólo estén disponibles con diferentes ediciones de Zscaler)

EDICIONES DE ZSCALER ZERO TRUST CLOUD	
NOMBRE DE LA EDICIÓN	**CAPACIDADES**
Zero Trust for Workloads Standard	• Suscripción anual a 1 GB de tráfico mensual para Zero Trust for Workloads Standard: • Incluye filtrado de estado y conector de nube
Zero Trust for Workloads Advanced	• Todo lo disponible en la edición Workloads Standard • Acceso a Internet para cargas de trabajo: inspección SSL/TLS, protección avanzada contra amenazas, Cloud NSS, anclaje de IP de origen • Acceso privado para cargas de trabajo: segmentos de aplicaciones, ubicación secundaria, registro y generación de informes del estándar LSS • Protección de datos para cargas de trabajo: web en línea (sólo en modo de monitor) • Protección cibernética para cargas de trabajo: cortafuegos estándar, control de DNS
Zero Trust for Workloads Advanced Plus	• Todo lo disponible en la edición avanzada de Workloads • Protección de datos para cargas de trabajo: protección de datos en línea y clasificación avanzada • Protección cibernética para cargas de trabajo: cortafuegos avanzado para cargas de trabajo, Sandbox avanzado para cargas de trabajo

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.com/es** o síganos en Twitter **@zscaler**.

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