

# Zero Trust Cloud

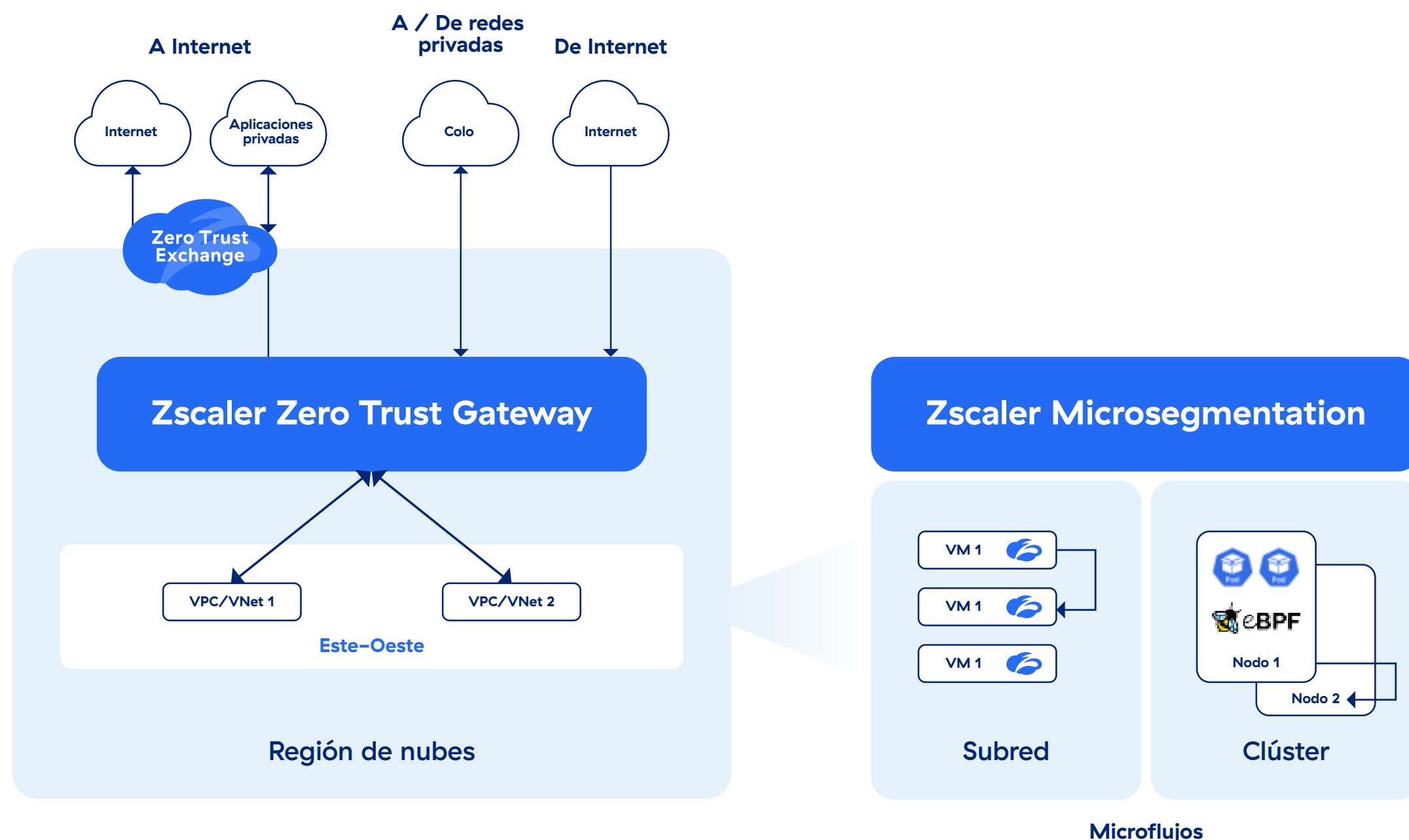


La manera más sencilla de conectar y proteger todas las cargas de trabajo en todas las nubes.

## FICHA DE DATOS

La era de la multinube, impulsada por la transformación digital, conlleva una explosión de cargas de trabajo. Para que su empresa prospere, debe tener visibilidad de estos recursos clave y evitar los ciberataques y la pérdida de datos.

Las soluciones de seguridad tradicionales, como los firewalls de red y las VPN IPSec, se basan en arquitecturas heredadas con deficiencias inherentes. Carecen de visibilidad de los activos en tiempo real, proporcionan una protección inconsistente, amplían la superficie de ataque y permiten el movimiento lateral. Esto aumenta inevitablemente la complejidad operativa y los costos.



Proteja todas las vías de tráfico mediante Zero Trust Gateway/Connectors y Zscaler Microsegmentation

La nube Zero Trust extiende la seguridad integral a su entorno multinube. Proporciona visibilidad en tiempo real con metadatos instantáneos e información detallada a nivel de proceso, y ofrece un inventario de activos preciso. Obtenga una protección de datos y contra amenazas uniforme en todas las vías de tráfico y nubes, lo que reduce los costos operativos con una sola plataforma. Para abordar la visibilidad y el control de los microflujos desde una máquina virtual o el contenedor, la solución ofrece una microsegmentación inteligente basada en el host.



# Extienda la arquitectura Zero Trust al entorno multicloud

Con Zero Trust Cloud, puede:



## VISIBILIDAD DE LOS RECURSOS EN LA NUBE EN TIEMPO REAL

Obtenga visibilidad de sus recursos en la nube en tiempo real con Zero Trust Cloud

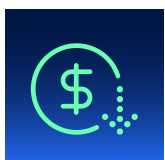
- **Captura instantánea de metadatos:** Se integra perfectamente con la infraestructura de la nube para recopilar automáticamente metadatos de la nube (etiquetas, rótulos, atributos) al crear, modificar o eliminar recursos.
- **Información detallada a nivel de proceso:** Los agentes de microsegmentación de Zscaler proporcionan metadatos granulares a nivel de proceso a partir de los entornos de máquinas virtuales y contenedores.
- **Inventario de activos preciso:** Proporciona un inventario detallado y preciso a nivel regional de VPCs/VNets, subredes y VMs/EC2s sin ninguna intervención manual.



## OBTENGA UNA PROTECCIÓN DE DATOS Y AMENAZAS UNIFORME Y COMPLETA

Aplique políticas de seguridad uniformes en un entorno multicloud

- **Asegure todas las vías de tráfico,** incluido el tráfico de entrada y salida, este-oeste, de red privada y los microflujos.
- **Evite ataques de día cero** con inspección TLS a escala de la nube y protección contra amenazas.
- **Detenga las fugas de datos** con protección de datos en línea.



## REDUCIR LOS COSTOS OPERATIVOS Y LA COMPLEJIDAD

Utilice una plataforma de seguridad para proteger todas las cargas de trabajo en sus nubes

- **Proteja las cargas de trabajo** en los principales proveedores de servicios en la nube, incluidos AWS, Azure y GCP, utilizando una plataforma unificada.
- **Automatice las implementaciones de seguridad** a través de interfaces programables que incluyen las API de Zscaler, Hashicorp Terraform y AWS CloudFormation.
- **Ofrezca compatibilidad nube a nube,** nube a centro de datos, región a región, VPC/VNet a VPC/VNet, subred a subred y entre hosts y nodos.



PROTEJA LAS APLICACIONES DE MISIÓN CRÍTICA

Cumpla con los requisitos normativos y regulatorios y refuerce la seguridad de las cargas de trabajo con microsegmentación basada en el host.

- **Visibilidad a nivel de proceso:** Obtenga información detallada sobre los recursos en la nube a nivel de los procesos individuales.
- **Agrupación automatizada de recursos:** Aproveche el aprendizaje automático para recomendar y definir automáticamente segmentos de recursos óptimos en función del análisis del flujo de tráfico.
- **Aplicación estricta del principio de privilegios mínimos:** Aplique reglas de seguridad granulares por segmento, y otorgue solo el acceso esencial para limitar el posible movimiento lateral.

Características de Zero Trust Gateway/Connector

EDICIÓN	DETALLES
Advanced	<ul style="list-style-type: none"><li>• Inspección TLS/SSL</li><li>• Firewall en la nube (Standard)</li><li>• Protección contra amenazas avanzadas</li><li>• Fuentes de registros de NSS (sin recuperación de registros)</li><li>• Streaming de nube a nube</li><li>• DNS Essentials</li><li>• Control de archivos</li><li>• Política de acceso y seguridad dinámica y basada en los riesgos</li><li>• Seguridad SaaS (CASB Standard)</li><li>• Segmentación entre cargas de trabajo (ZPA)</li><li>• Detección de aplicaciones (ZPA)</li><li>• Protección de datos (modo de supervisión)</li><li>• Anclaje de IP de origen de Zscaler</li></ul>
Avanzado Plus	<ul style="list-style-type: none"><li>• Todo lo disponible en la edición Workloads Advanced</li><li>• Protección de carga de trabajo a Internet</li><li>• Protección de datos, IPS</li><li>• Fuentes de registros de NSS (con recuperación de registros)</li><li>• DNS Advanced</li><li>• Sandbox en la nube (Advanced)</li><li>• Certificado raíz personalizado</li><li>• Seguridad de SaaS</li><li>• Firewall en la nube (Advanced)</li><li>• Protección de datos (en línea)</li><li>• Coincidencia exacta de datos (EDM)</li><li>• Coincidencia de documentos índice (IDM)</li><li>• Reconocimiento óptico de caracteres (OCR)</li></ul>

# Características de Zscaler Microsegmentation

EDICIÓN	DETALLES
Advanced	<ul style="list-style-type: none"><li>• Plataformas compatibles: Windows, Linux y Kubernetes (Amazon EKS)</li><li>• Visibilidad de sus cargas de trabajo en la nube (AWS, Azure, GCP)</li><li>• Visibilidad del flujo de tráfico, incluidos los detalles de aplicaciones.</li><li>• Mapas de dependencias de aplicaciones</li><li>• Aplicación de políticas</li><li>• Zonas de aplicaciones para ámbitos de políticas avanzadas</li><li>• Actualizaciones de agentes integradas mediante perfiles de versión</li><li>• Análisis de flujo avanzado</li><li>• Integración con SIEM mediante el servicio de streaming de registros (LSS)</li><li>• Servicio de detección de cargas de trabajo – Integración de Zero Trust Gateway/Connector para visibilidad en tiempo real de los metadatos en entornos multinube</li></ul>

## 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 ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 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](https://zscaler.com/mx) o síganos en Twitter [@zscaler](https://twitter.com/zscaler).

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en [zscaler.com/mx/legal/trademarks](https://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.



Zero Trust  
Everywhere