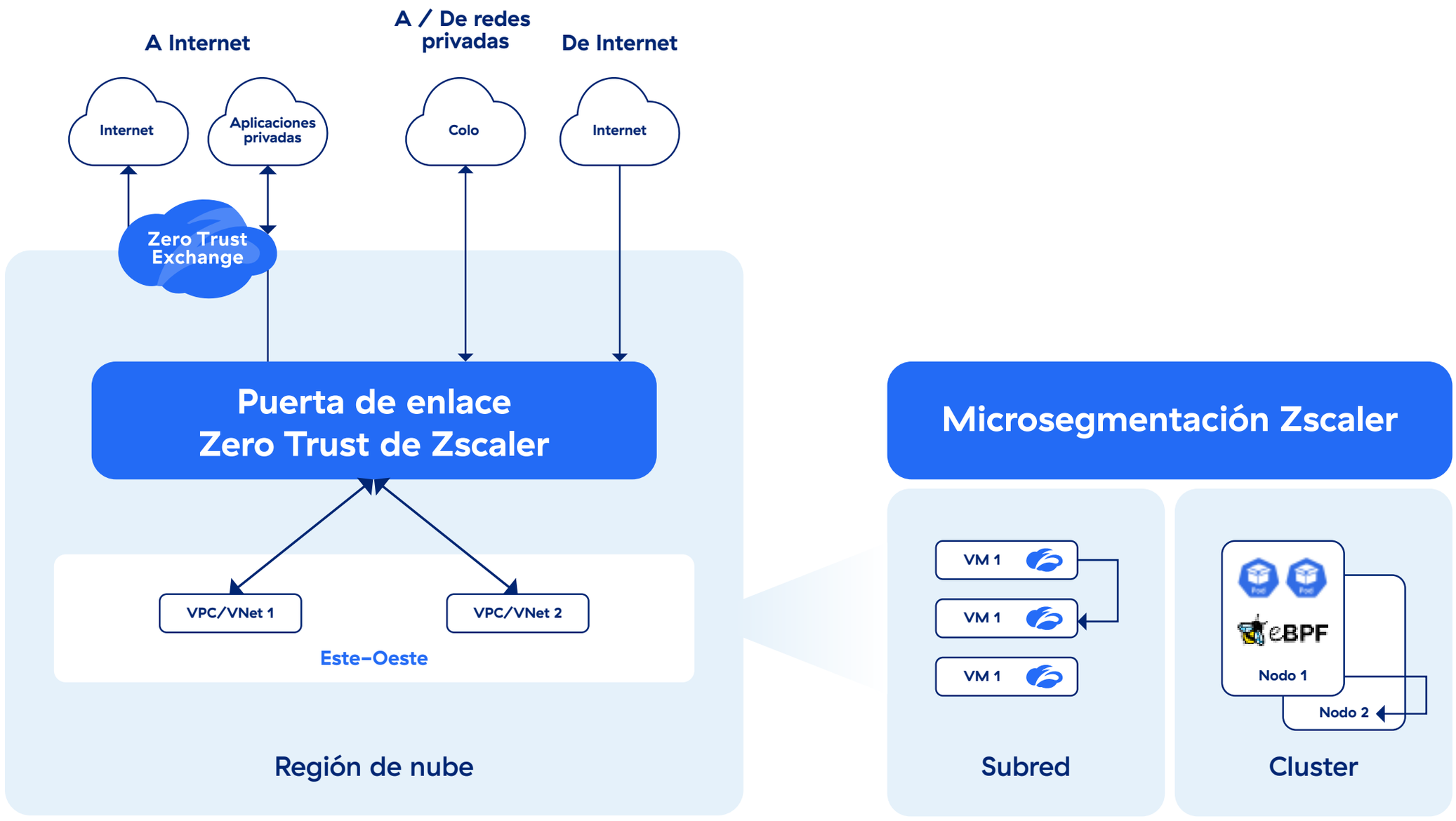
Zero Trust Cloud

La forma más sencilla de conectar y proteger todas las cargas de trabajo en cualquier nube.

FICHA DE DATOS

La era de la multinube, impulsada por la transformación digital, supone un auge de cargas de trabajo. Para que su empresa prospere, debe tener visibilidad de estos recursos clave y prevenir los ciberataques y la pérdida de datos.

Las soluciones de seguridad tradicionales, como los cortafuegos de red y las VPN IPSec, se basan en arquitecturas heredadas con fallos 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 inevitablemente aumenta la complejidad operativa y los costes.



Proteja todas las rutas de tráfico mediante conectores/puerta de enlace Zero Trust y microsegmentación Zscaler

La nube de zero trust hace extensiva la seguridad integral a su entorno multinube. Proporciona visibilidad en tiempo real con metadatos instantáneos e información a nivel de proceso, ofreciendo un inventario de activos preciso. Obtenga una protección de datos y frente a amenazas consistente en todas las rutas de tráfico y nubes, reduciendo los costos operativos con una sola plataforma. Para obtener la visibilidad y el control de los microflujos desde una máquina virtual o contenedor, la solución ofrece una microsegmentación inteligente basada en el host.

Haga extensiva la arquitectura de zero trust a un entorno multinube

Con Zero Trust Cloud, puede:

VISIBILIDAD DE LOS RECURSOS EN LA NUBE EN TIEMPO REAL

Obtenga visibilidad en tiempo real de sus recursos en la nube 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 de entornos de máquinas virtuales y contenedores.
- **Inventario de activos preciso:** proporciona un inventario detallado y preciso a nivel regional de VPC/VNet, subredes y VM/EC2 sin ninguna intervención manual.

OBTENGA UNA PROTECCIÓN DE DATOS Y FRENTE A AMENAZAS CONSISTENTE Y COMPLETA

Aplique políticas de seguridad uniformes en un entorno multinube

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

REDUZCA LA COMPLEJIDAD Y EL COSTE OPERATIVOS

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

- **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, incluidas las API de Zscaler, Hashicorp Terraform y AWS CloudFormation.
- **Soporte de nube a nube**, de nube a centro de datos, de región a región, de VPC/VNet a VPC/VNet, de subred a subred y entre hosts y nodos.

©2025 Zscaler, Inc. Todos los derechos reservados.

PROTEJA LAS APLICACIONES CRÍTICAS DE MISIÓN

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

- **Visibilidad a nivel de proceso:** obtenga información detallada sobre los recursos en la nube a nivel de proceso individual.
- **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 mínimo privilegio:** aplique reglas de seguridad granulares por segmento, otorgando solo el acceso esencial y limitando el movimiento lateral potencial.

Puerta de enlace Zero Trust/ Características del conector

EDICIÓN	DETALLES
Avanzado	• Inspección TLS/SSL • Cortafuegos en la nube (estándar) • Protección contra amenazas avanzadas • Registro de NSS (sin recuperación de registros) • Transmisión de nube a nube • Fundamentos del DNS • Control de archivos • Política dinámica de acceso y seguridad basada en riesgos • Seguridad SaaS (Estándar CASB) • Segmentación de carga de trabajo a carga de trabajo (ZPA) • Descubrimiento de aplicaciones (ZPA) • Protección de datos (modo monitor) • Anclaje de IP de origen de Zscaler
Avanzado Plus	• Todo lo disponible en la edición avanzada de Workloads • Protección de carga de trabajo a Internet • IPS, Protección de datos • Registro de NSS (con recuperación de registros) • DNS avanzado • Entorno de pruebas en la nube (avanzado) • Certificado raiz personalizado • Seguridad de SaaS • Cortafuegos en la nube (avanzado) • Protección de datos (en línea) • Coincidencia exacta de datos (EDM) • Coincidencia de documentos indexados (IDM) • Reconocimiento óptico de caracteres (OCR)

©2025 Zscaler, Inc. Todos los derechos reservados.

Características de microsegmentación de Zscaler

EDICIÓN	DETALLES
Avanzado	• Plataformas compatibles: Windows, Linux y Kubernetes (Amazon EKS) • Visibilidad de sus cargas de trabajo en la nube (AWS, Azure, GCP) • Visibilidad del flujo de tráfico, incluyendo detalles de la aplicación • Mapas de dependencias de aplicaciones • Aplicación de políticas • Zonas de aplicaciones para ámbitos de políticas avanzadas • Actualizaciones de agentes integradas mediante perfiles de versión • Análisis de flujo avanzado • Integración con SIEM mediante el servicio de transmisión de registros (LSS) • Servicio de detección de cargas de trabajo – Integración de conector/puerta de enlace Zero Trust para la visibilidad en tiempo real de los metadatos en múltiples nubes

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. 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 150 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