LIBRO ELECTRÓNICO

Cómo lograr una seguridad uniforme para las cargas de trabajo en múltiples nubes

Índice

Introducción

Las empresas están migrando aplicaciones y cargas de trabajo a la nube pública a un ritmo sin precedentes, por todas las razones correctas.

La transformación a la nube aporta una amplia gama de ventajas, que van desde ahorros de costes hasta mayores eficiencias operativas, etc. La migración a la nube es una parte clave de la transformación digital, que permite a una organización volverse más ágil, satisfacer mejor las necesidades de clientes, proveedores y socios externos, y mejorar la experiencia del cliente.

A medida que un número cada vez mayor de organizaciones de todos los sectores adoptan estrategias de nube para seguir siendo competitivas con sus pares, la nube pública se ha convertido en el nuevo centro de datos empresarial. Al mismo tiempo, los entornos híbridos y multinube se han convertido en la norma. IDC Research predijo recientemente que, para fines de 2025, la mayoría de las empresas aprovecharán la nube pública para plataformas de inteligencia artificial generativa, herramientas para desarrolladores e infraestructura, y que el uso de la nube superará al de los sistemas locales.[1]

Los 3 principales proveedores de servicios en la nube poseen el 67 % de la participación de mercado

> Gartner predice que el 51 % del gasto en TI en software de aplicaciones, infraestructura y servicios de procesos de la organización se habrá trasladado a la nube pública para 2025, superando el gasto en TI tradicional.[4]

Si bien la transformación de la nube tiene un impulso enorme, y aunque se espera que los ingresos combinados de los proveedores de nube pública superen los 800 mil millones de dólares estadounidenses para fines de 2024,[2] el mercado está dominado por solo tres actores:[3]

- Amazon Web Services (AWS), con una cuota de mercado del 31 %
- Microsoft Azure, con una cuota de mercado del 25 %
- Google Cloud, con una cuota de mercado del 11 %

Estos proveedores de nube pública ofrecen a sus clientes nuevas oportunidades para aprovechar mayor velocidad, agilidad y elasticidad en el uso de recursos informáticos. Todos ellos permiten a los desarrolladores crear nuevos entornos en cuestión de segundos. Y todos ofrecen cientos de servicios diferentes, tanto autogestionados como gestionados por proveedores.

Sin embargo, estos factores también están contribuyendo al surgimiento de nuevos riesgos de seguridad, especialmente para las organizaciones que continúan confiando en arquitecturas de seguridad heredadas para proteger sus entornos de nube modernos. La disparidad fundamental entre los enfoques tradicionales para proteger las cargas de trabajo locales y lo que se necesita en los entornos de nube actuales a menudo hace que proteger las cargas de trabajo en la nube sea un proceso costoso, complejo y difícil.

1. IDC Research, IDC FutureScape: Predicciones de la nube a nivel mundial para 2024, 2023.
2. IDC Research, Seguimiento semestral mundial de servicios de nube pública.
3. Statista, Mercado de infraestructura en la nube, 2024.
4. Gartner, Gartner afirma que más de la mitad del gasto en TI empresarial en segmentos clave del mercado se trasladará a la nube en 2025.

Desafíos de seguridad de cargas de trabajo en la nube

Las organizaciones que migran cargas de trabajo a la nube sin modernizar al mismo tiempo su enfoque de seguridad se enfrentan a una serie de desafíos comunes.

La aplicación inconsistente o ineficaz de políticas deja las cargas de trabajo expuestas a ciberamenazas y ataques.

Confiar en enfoques tradicionales para proteger y conectar cargas de trabajo en la nube es inevitablemente complejo y costoso. Las arquitecturas de ciberseguridad basadas en cortafuegos y redes privadas virtuales (VPN) simplemente no fueron diseñadas para los ecosistemas de computación en la nube actuales.

Las cargas de trabajo expuestas pueden verse fácilmente comprometidas. Los ciberdelincuentes pueden tomar a las organizaciones como rehenes con devastadores ataques de ransomware. Recuperarse de ellos puede ser costoso y llevar mucho tiempo.

Las cargas de trabajo en la nube requieren comunicaciones extensas con otras cargas de trabajo e Internet. Los enfoques de seguridad tradicionales no son adecuados para esta conectividad siempre activa.

44%

experimentó una infracción de datos basada en la nube en 2024.[5]

49%

Informe de que la complejidad de la nube supone un importante desafío en materia de cumplimiento y seguridad.[6]

69%

experimentó sobrecostes presupuestarios en su gasto en la nube en 2023.[7]

5. Thales Group, Estudio de seguridad en la nube 2024.
6. Ibíd.
7. Gartner, Gasto en la nube 2024: TI equilibra los costes con la innovación GenAI.

Las aplicaciones de hoy están en movimiento. Zero trust debería acompañarlas.

A medida que el trabajo remoto e híbrido se ha convertido en algo común, las organizaciones de todas las industrias están adoptando zero trust para proteger a sus usuarios. En un enfoque zero trust, la confianza nunca se concede implícitamente. En cambio, se supone que cada solicitud de acceso es hostil o está comprometida, y la solicitud de acceso a la aplicación se concede si y solo si:

- Se puede verificar su identidad y contexto (el "quién, qué y dónde" de la solicitud)
- Los riesgos asociados a esa solicitud pueden evaluarse en profundidad.
- Las políticas se pueden aplicar por sesión

A medida que un número cada vez mayor de aplicaciones y cargas de trabajo se trasladan a la nube, es esencial que las organizaciones extiendan el mismo grado de protección que sus usuarios disfrutan actualmente cuando se trata del acceso a las aplicaciones de todos sus activos y servicios en la nube. Esto significa extender la seguridad basada en zero trust a cada una de sus cargas de trabajo en la nube.

Cuando las organizaciones migran sus aplicaciones monolíticas heredadas a la nube, a menudo optan por refactorizarlas utilizando un enfoque de microservicios. Esto permite aprovechar funcionalidades exclusivas de la nube, como bases de datos en la nube especializadas, funciones sin servidor y arquitecturas basadas en eventos. Esto genera una mayor eficiencia y puede reducir costes, pero también crea un entorno dinámico y altamente automatizado. En este entorno, las comunicaciones se intercambian constantemente entre cargas de trabajo.

Las cargas de trabajo en con frecuencia deben:

- Conectarse a Internet
- Comunicarse con otras cargas de trabajo

La gran cantidad de comunicaciones que deben enviarse entre cargas de trabajo es mucho mayor en este tipo de entorno que en el centro de datos tradicional.

¿Qué es una carga de trabajo?

Una carga de trabajo es el componente básico de una aplicación en la nube moderna. En los entornos locales tradicionales, la mayoría de las cargas de trabajo eran componentes dentro de grandes aplicaciones monolíticas. Este no es el caso en los entornos nativos de la nube actuales, donde las aplicaciones generalmente constan de muchos componentes modulares o microservicios. Cada servicio realiza una tarea específica y se comunica con otros servicios para ejecutar la lógica de la organización.

Algunos ejemplos de cargas de trabajo incluyen:

- Contenedores
- Máquinas virtuales (VM)
- Granjas de infraestructura de escritorio virtual (VDI)
- Funciones sin servidor

La seguridad de la red heredada no funciona para las empresas nativas de la nube

Demasiadas organizaciones se han embarcado en su viaje de transformación a la nube sin cambiar su estrategia de seguridad para seguir el ritmo. Pero las arquitecturas de seguridad de red heredadas se crearon para el centro de datos local, no para la nube. Cuando las organizaciones intentan trasladarlos a la nube, la arquitectura resultante es sumamente compleja e ineficaz.

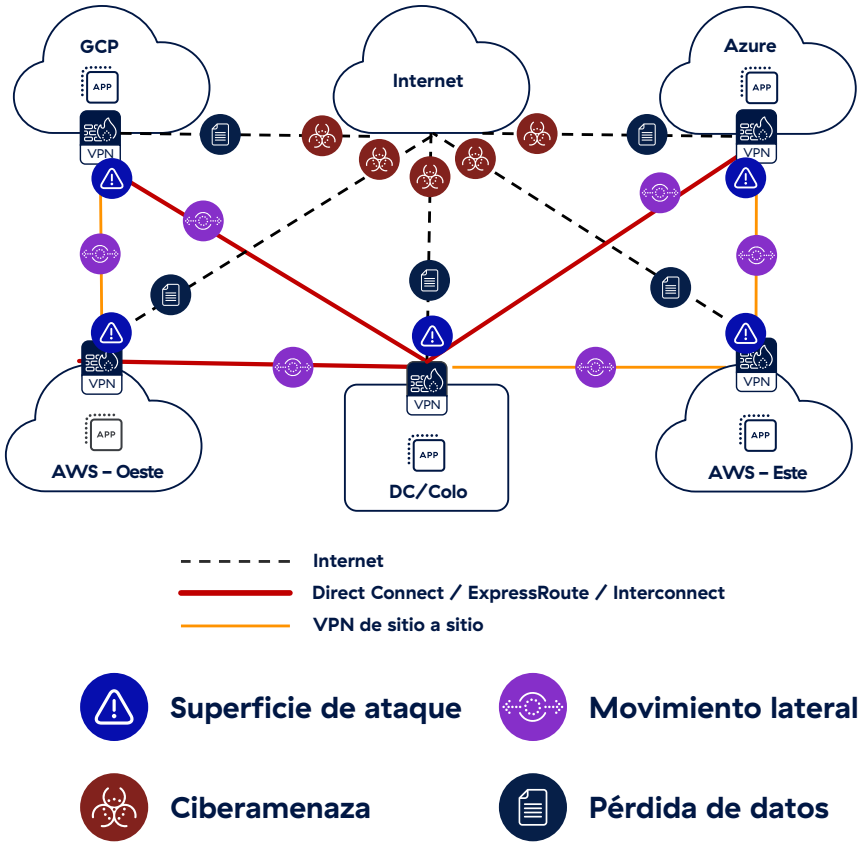
Las cargas de trabajo en la nube deben comunicarse de forma segura entre sí y con Internet. El enfoque tradicional para lograr esto implica construir redes enrutables entre infraestructuras en la nube mediante el uso de cortafuegos y VPN, extendiendo esencialmente la red de área amplia (WAN) de la organización hacia la nube.

En este modelo, las organizaciones deben instalar cortafuegos virtuales de próxima generación (vNGFW) en todos los lugares donde residan sus cargas de trabajo. En un mundo donde los entornos híbridos y multinube son omnipresentes, esto crea redes de malla completa, en las que cada nodo se conecta directamente a todos los demás. Esta arquitectura es enormemente compleja y difícil de gestionar.

Si las organizaciones desean implementar capacidades de seguridad adicionales, como prevención de pérdida de datos (DLP) o inspección TLS/SSL, necesitarán agregar dispositivos de seguridad virtuales adicionales, lo que creará aún más complejidad.

Incluso dentro del entorno de un solo proveedor de servicios en la nube, las organizaciones necesitarán configurar y administrar varios vNGFW adicionales para proteger el tráfico norte–sur y este–oeste entre las cargas de trabajo en la nube.

Las comunicaciones de carga de trabajo multiplican la complejidad y los desafíos de seguridad



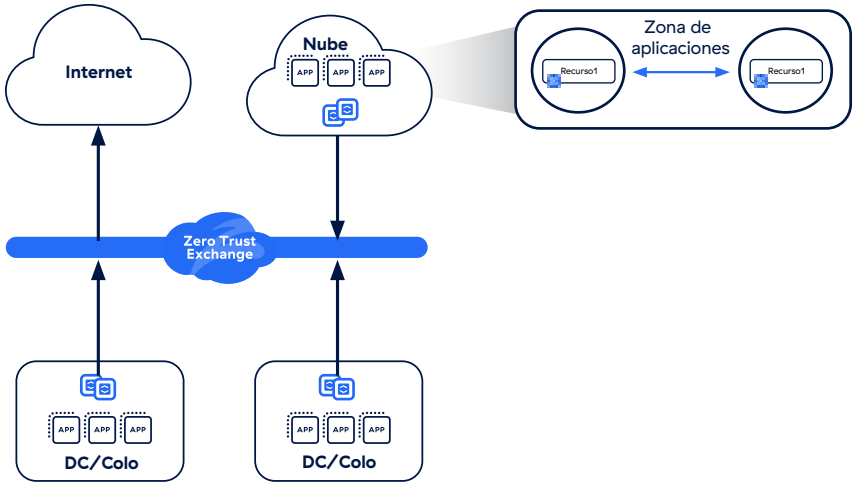
Ciberdefensa inadecuada para los ecosistemas informáticos actuales

Confiar en enfoques tradicionales para proteger y conectar cargas de trabajo en la nube conduce a:

- **Una superficie de ataque ampliada.** Cada vNGFW tiene una ubicación de red identificable y, por lo tanto, puede ser descubierto por los atacantes. Cuantos más cortafuegos se implementen, mayor será la superficie de ataque.
- **Compromiso de la carga de trabajo.** Una vez que los ciberdelincuentes descubren un punto de entrada al entorno y se afianzan allí, pueden comprometer las cargas de trabajo.
- **Movimiento lateral de amenazas.** Debido a que todas las cargas de trabajo están conectadas a través de una red en malla, una vez que una sola carga de trabajo se ve comprometida, los ciberdelincuentes pueden moverse lateralmente a través de la red para comprometer a otras.
- **No hay protección para los datos confidenciales.** A medida que se desplazan por la red, los atacantes podrán encontrar y extraer datos confidenciales, como información financiera de clientes y secretos comerciales.

Lo que se necesita: un nuevo enfoque para proteger las cargas de trabajo en la nube

Para proteger los ecosistemas informáticos empresariales actuales, que dependen en gran medida de la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) y el software como servicio (SaaS) de múltiples proveedores y vendedores de servicios en la nube, se requiere un enfoque diferente: uno que coloque las políticas de seguridad de la organización en el centro del diseño de su red. Esto significa permitir un acceso seguro y con el privilegio mínimo basado en la conectividad directa entre cargas de trabajo y entre cargas de trabajo e Internet. Este enfoque también facilita la creación y el mantenimiento de una arquitectura zero trust en todas las cargas de trabajo en la nube.



Con este nuevo y moderno enfoque:

- **Se elimina la superficie de ataque.** A diferencia de las soluciones tradicionales, las cargas de trabajo son prácticamente invisibles para los ciberdelincuentes, lo que elimina básicamente toda la superficie de ataque.
- **Las cargas de trabajo están protegidas.** La inspección completa de contenido en línea, junto con las capacidades de DLP, brindan una seguridad potente para los datos y las cargas de trabajo.
- **Se evita el movimiento lateral de amenazas.** Al proporcionar conectividad directa sin conexión a una red, el movimiento lateral es imposible.
- **Los datos están protegidos.** Agregar inspección TLS/SSL a escala de capacidades de DLP permite ofrecer protección de datos integral a escala.
- **Se reducen la complejidad y los costes.** La centralización de la gestión de la configuración de la nube junto con la seguridad (y la habilitación de la conectividad directa) permite reducir la complejidad y los costes.

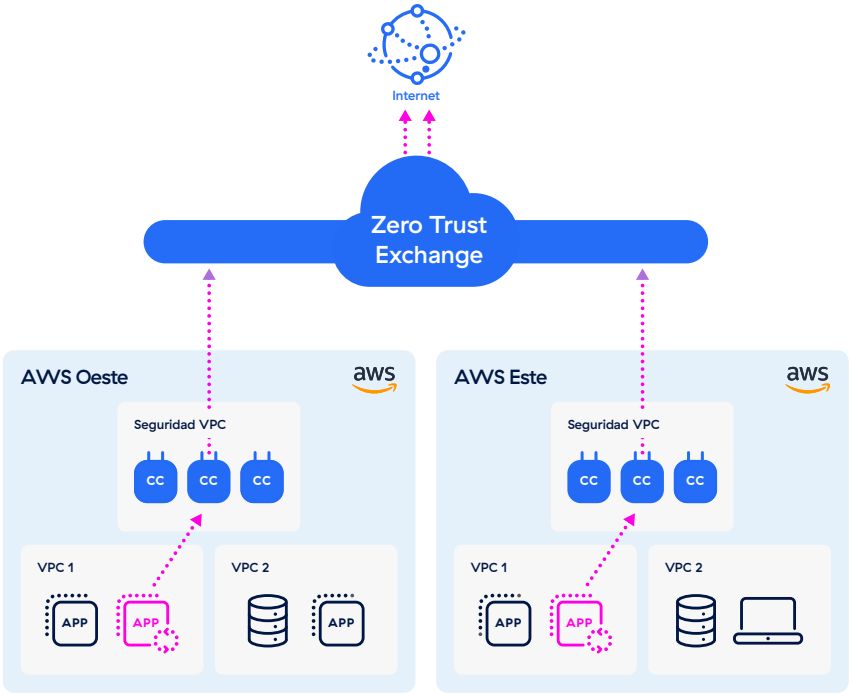
Simplifique y proteja las comunicaciones de la carga de trabajo a Internet

Dado que cada carga de trabajo en la nube depende de una comunicación casi constante a través de Internet pública, una solución zero trust para cargas de trabajo en la nube debe poder proteger toda la conectividad saliente. Dentro de una arquitectura simple de acceso directo a la nube, la solución debe brindar acceso seguro a Internet para todas las cargas de trabajo, independientemente de si están ubicadas en una nube pública o en el centro de datos empresarial.

Las capacidades clave necesarias para proteger las comunicaciones de la carga de trabajo a Internet incluyen:

- Inspección TLS/SSL completa basada en proxy
- Superficie de ataque cero
- Permiso de acceso únicamente a sitios aprobados
- Protección avanzada frente a malware para bloquear amenazas de día cero

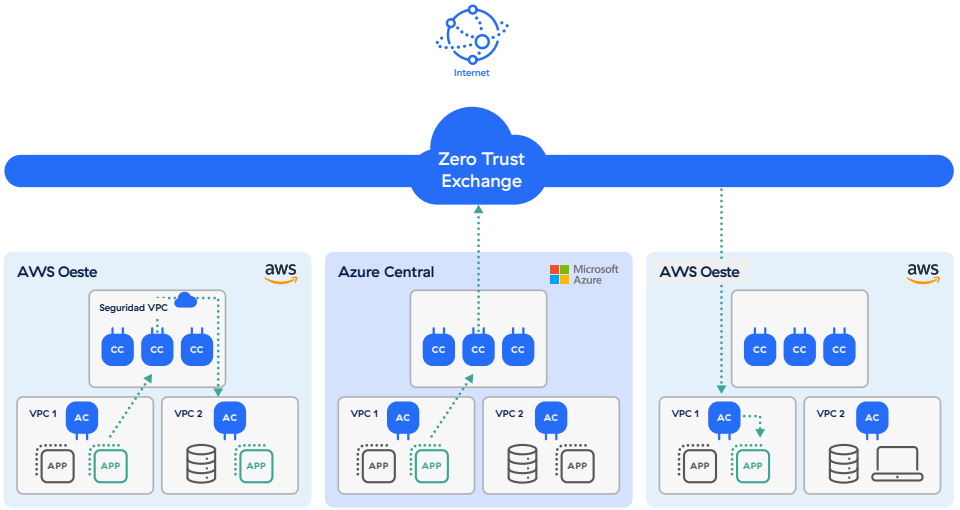
Por ejemplo, imaginemos que su organización tiene aplicaciones ubicadas en AWS West y AWS East, y ambas requieren una actualización. La solicitud deberá enviarse a una plataforma central donde se aplican y gestionan las políticas. Una solución ideal será capaz de aplicar políticas zero trust, y conectar fuentes y destinos de forma segura.



Simplifique y proteja las comunicaciones entre cargas de trabajo

La aplicación zero trust en las cargas de trabajo en la nube también requiere una conectividad segura entre cargas de trabajo. Es esencial que las cargas de trabajo puedan comunicarse, tanto a través de múltiples nubes como dentro de una única nube privada virtual (VPC). Estas comunicaciones deben fluir a través de la plataforma central de zero trust, donde se aplican las políticas de seguridad y donde se utilizan la identidad y el contexto para verificar la confianza antes de permitir la conexión.

En particular, debería existir un mecanismo para facilitar las comunicaciones dentro de la carga de trabajo. Para la conectividad de VPC a VPC, el tráfico podría enrutarse desde una VPC a un perímetro de servicio privado, desde donde luego se negociaría una conexión a la aplicación de destino (ubicada en una VPC diferente). Para la conectividad de nube a nube, el tráfico podría reenviarse a una plataforma central zero trust, donde se establecería una conexión con una aplicación de destino ubicada en una nube diferente.



Las capacidades clave necesarias para proteger las comunicaciones entre cargas de trabajo incluyen:

- Proteger la conectividad multinube y multirregional
- Proteger la conectividad inter-VPC/inter-VNET
- Eliminar la superficie de ataque de la red con acceso a la red zero trust (ZTNA)
- Bloqueo del movimiento lateral de amenazas

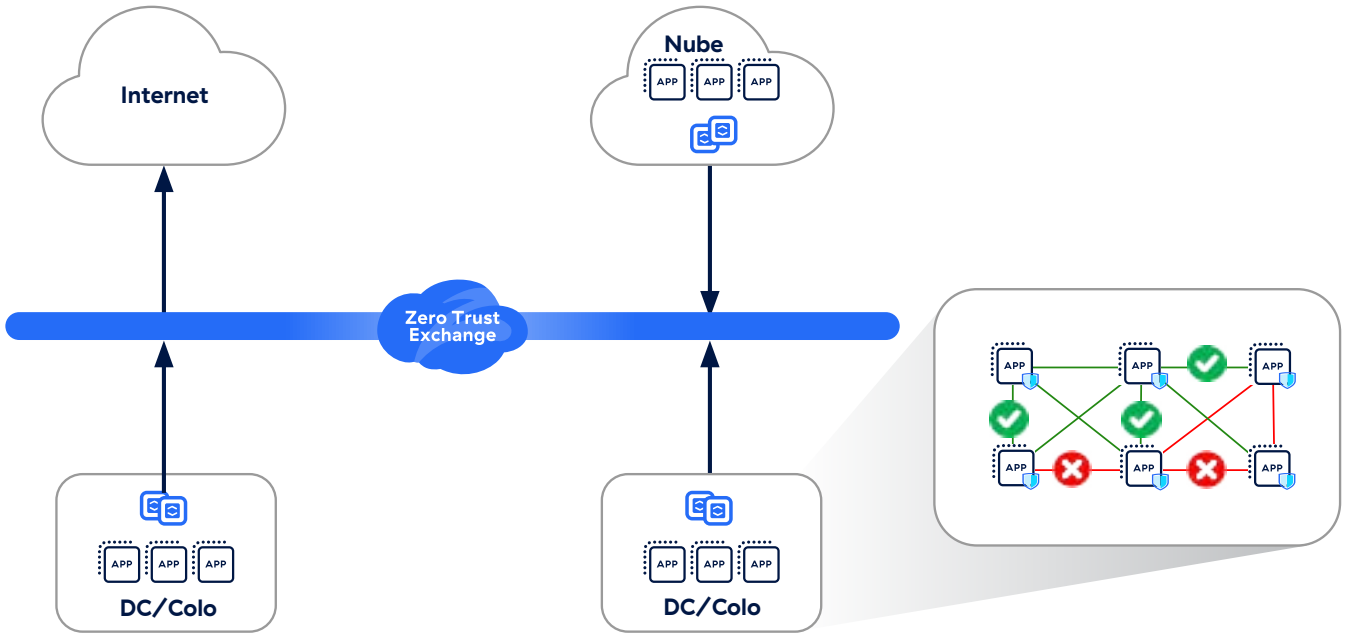
Consiga fácilmente una microsegmentación granular

La microsegmentación, un componente central de la seguridad zero trust, evita el movimiento lateral de amenazas al dividir grupos de aplicaciones o cargas de trabajo en pequeños segmentos según los requisitos de comunicación de las aplicaciones individuales. Las cargas de trabajo pueden comunicarse dentro de sus propios segmentos, pero no pueden intercambiar comunicaciones no autorizadas con cargas de trabajo fuera de ellas.

La microsegmentación permite aplicar políticas zero trust a un nivel granular en toda la red interna de la organización, no solo en su perímetro, extendiendo protecciones consistentes a las cargas de trabajo locales como a las que se ejecutan en la nube.

Las capacidades clave necesarias para la microsegmentación de la carga de trabajo incluyen:

- Detección de recursos en tiempo real impulsado por IA
- Segmentación basada en host y no basada en host
- Capacidad para segmentar cargas de trabajo dentro y entre VPCs/VNETs



Una solución de zero trust para cargas de trabajo en la nube debe tener varias características clave:

Nº 1: La capacidad de realizar inspección TLS/SSL a escala

Muchas de las amenazas más peligrosas de la actualidad se ocultan a simple vista en el tráfico cifrado. Para detectarlas, se necesita una plataforma integral que pueda realizar inspección TLS/SSL completa a escala, sin las limitaciones de rendimiento impuestas por las aplicaciones heredadas.

Busque una solución que pueda ofrecer:

- **Capacidad ilimitada** para inspeccionar todo el tráfico TLS/SSL de sus usuarios sin preocupaciones de rendimiento
- **Escalabilidad elástica** basada en las demandas del tráfico
- **Gestión optimizada de certificados**
- **Control de políticas granular** que simplifica el cumplimiento al excluir el tráfico de usuarios cifrados para categorías de sitios web como atención médica o banca

N° 2: Capacidades potentes de protección de datos

Un enfoque de defensa en profundidad para la protección de datos incluye la capacidad de aplicar políticas de prevención de pérdida de datos (DLP) a escala sin afectar el rendimiento. Esto proporciona una capa adicional de protección. Si alguna vez se ve comprometida una carga de trabajo en la nube, aún habrá un mecanismo para aplicar políticas y evitar la exfiltración de datos.

Busque una solución que pueda ofrecer:

- **Un panel de control optimizado** donde se puedan configurar y administrar las políticas de DLP
- **Técnicas avanzadas de gestión de datos,** como la gestión exacta de datos (EDM) y el reconocimiento óptico de caracteres (OCR)
- **Inspección de contenido fiable en línea a escala**

Nº 3: Capacidades avanzadas de protección frente a amenazas

Para bloquear las amenazas más peligrosas y sofisticadas de la actualidad, una plataforma de seguridad de carga de trabajo en la nube zero trust debe poder garantizar que cada paquete, de cada carga de trabajo, pueda inspeccionarse completamente de principio a fin. Esto requiere capacidades de inspección TLS/SSL integradas siempre activas, así como la capacidad de aplicar políticas detalladas para todo el tráfico.

Además, las capacidades clave que se deben buscar incluyen:

- **Tecnologías de engaño integradas** que utilizan señuelos, cebos y honeypots para proteger a sus activos más valiosos con alta fidelidad y bajas tasas de falsos positivos.
- **Sandbox en la nube** para poner en cuarentena e inspeccionar amenazas potenciales en lugar de permitirles pasar
- **Protección contra malware** que puede bloquear ransomware, spyware y malware conocidos, así como nuevas amenazas.

N° 4: Segmentación integral basada en host

La microsegmentación evita el movimiento lateral de amenazas para minimizar el radio de explosión y el daño que un incidente cibernético podría causar. La microsegmentación basada en host se basa en agentes instalados en dispositivos terminales para proporcionar un control y una visibilidad mucho más granulares, lo que facilita la gestión de la segmentación basada en identidad. El uso de un agente permite una segmentación basada en políticas dinámicas y comprensibles para los humanos, en lugar de reglas estáticas a nivel de red.

En particular, busque una solución que pueda proporcionar:

- **Detección de recursos en tiempo real** que aprovecha la IA para brindarle visibilidad granular en todos los dispositivos, servicios y activos dentro de su ecosistema empresarial
- **Recomendaciones de políticas zero trust** basadas en análisis de tráfico
- **Integración con una plataforma zero trust,** para que pueda proteger y segmentar su entorno en un solo lugar, sin necesidad de implementar múltiples productos puntuales

Los principales casos de uso para proteger la conectividad de la carga de trabajo

Una solución basada en zero trust para la conectividad de la carga de trabajo puede ayudar a las organizaciones a resolver varios desafíos clave. A continuación se enumeran cuatro de los más comunes:

Protección del tráfico a Internet

Cuando las aplicaciones se comunican con Internet o con aplicaciones SaaS, es necesario inspeccionar el tráfico de salida para detectar ciberataques y filtraciones de datos. Zscaler opera la mayor plataforma de seguridad en la nube en línea del mundo, que ofrece protección avanzada frente a amenazas a escala de la nube sin ningún impacto en el rendimiento ni degradación del servicio.

Segmentación de la carga de trabajo

Con la solución de comunicaciones de carga de trabajo adecuada, es posible adoptar un enfoque granular y metódico para la segmentación de la carga de trabajo. Esto simplifica la aplicación de políticas para controlar la conectividad de las cargas de trabajo en las VPC, las regiones, y las nubes públicas y privadas.

Migración a la nube

Este suele ser un proceso arduo y que requiere mucho tiempo para las organizaciones. Deben tener en cuenta muchos factores, incluida la estrategia de migración que deben seguir. ¿Tiene sentido hacer una migración simple o se deben refactorizar o reconstruir las aplicaciones? La solución de comunicaciones de carga de trabajo adecuada puede simplificar y facilitar la conexión segura de las aplicaciones en la nube recién migradas.

Fusiones y adquisiciones

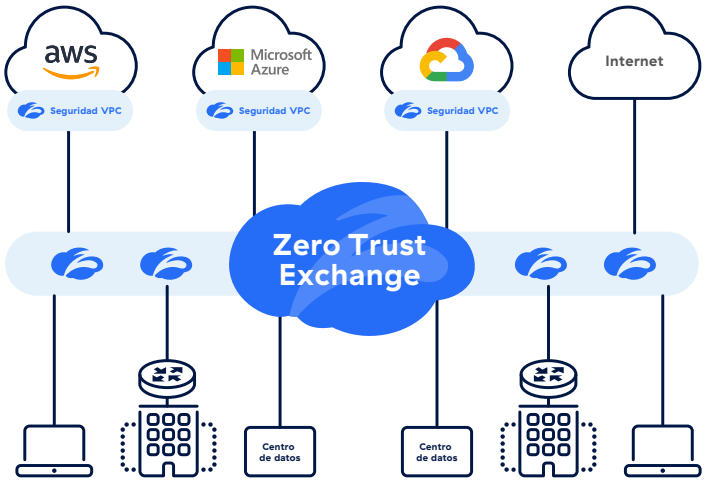
Con una solución de comunicaciones de carga de trabajo nativa de la nube, moderna y basada en zero trust, es posible brindar acceso seguro a aplicaciones entre redes, sin necesidad de rediseñar ni reconstruir las redes para conectarlas.

Zscaler Workload Communications es la respuesta

¿Busca una solución integral que pueda hacer todo esto y más? Zscaler Zero Trust Exchange™ ha hecho posible reinventar por completo las comunicaciones de carga de trabajo dentro de una arquitectura simple, probada y directa a la nube.

Al combinar Zscaler Internet Access™ (ZIA) para comunicaciones de carga de trabajo a Internet, Zscaler Private Access™ (ZPA) para comunicaciones de carga de trabajo a carga de trabajo y capacidades de microsegmentación zero trust de segmento de uno, Zscaler Workload Communications constituye un enfoque integral para proteger la conectividad de carga de trabajo en la nube y en las instalaciones. Al mismo tiempo, puede mantener el rendimiento para garantizar que sus usuarios tengan excelentes experiencias y la escalabilidad para seguir el ritmo de la evolución de su huella en la nube a medida que crecen sus operaciones.

Zscaler Workload Communications proporciona una seguridad en la nube basada en zero trust altamente efectiva que se puede ajustar según sus necesidades. Las capacidades de ajuste automático elástico le permiten gestionar aumentos de tráfico con facilidad. Zero Trust Exchange ya opera a hiperescala, con más de 150 centros de datos en todo el mundo. Zscaler maneja todas las actualizaciones automáticamente en su nombre, y la infraestructura está integrada de forma nativa con la infraestructura de seguridad de los proveedores de nube pública, aprovechando funcionalidades como puertas de tránsito y equilibradores de carga.



Además, Zscaler Workload Communications simplifica y centraliza la gestión de políticas. Todas las políticas se pueden crear y actualizar en una única consola central y fácil de usar. Se aplican dentro de Zero Trust Exchange, donde se pueden aprovechar las políticas ZIA o ZPA para proporcionar una inspección de contenido completa y un control basado en la identidad de las comunicaciones de la carga de trabajo. Desde allí, se pueden reenviar las comunicaciones a cualquier destino, ya sea a Internet o a otras aplicaciones privadas dentro de entornos de nube. Las políticas se pueden aplicar fácilmente a escala siempre que sea necesario implementar cargas de trabajo adicionales en la nube.

Si está interesado en obtener más información sobre las ventajas de usar Zscaler Workload Communications, póngase en contacto con nosotros hoy mismo. También puede obtener más información visitando la página web de Zscaler Zero Trust Cloud Connectivity.

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. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE 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