Zscaler y AWS

Proporcionando seguridad de confianza cero para usuarios, datos y cargas de trabajo

Available in AWS Marketplace

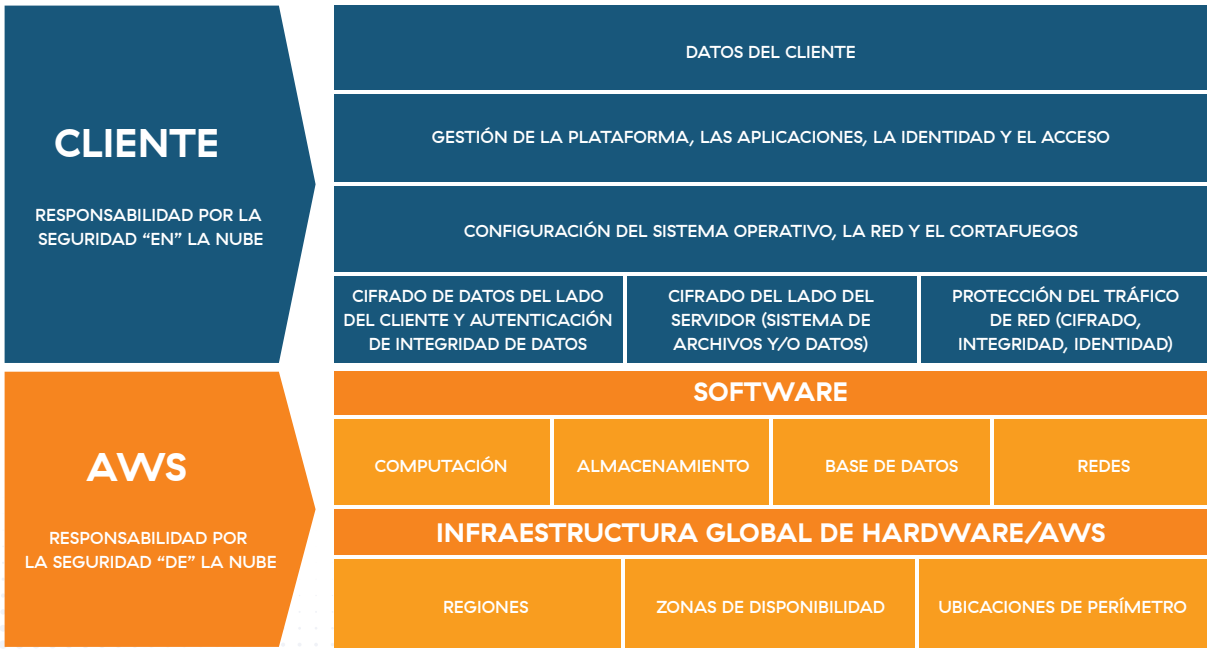
Introducción

La migración de cargas de trabajo a Amazon Web Services (AWS) es ya una realidad para muchas organizaciones y agencias del sector público. La pandemia global ha puesto de manifiesto la importancia de que las empresas aceleren la transformación digital e identifiquen estrategias para migrar aplicaciones críticas a AWS a fin de que puedan garantizar la continuidad y resiliencia del negocio, reducir gastos y obtener nuevas eficiencias. Los entornos de TI actuales han evolucionado de servidores físicos locales a una infraestructura virtualizada que admite aplicaciones y cargas de trabajo en múltiples regiones de AWS, lo que permite a los usuarios acceder a estas aplicaciones en cualquier lugar y en cualquier momento.

La seguridad basada en el perímetro no ha logrado satisfacer las necesidades de las empresas modernas

El modelo de seguridad predominante en la nube se basa en la responsabilidad compartida en la que AWS es responsable de la seguridad de la infraestructura de la nube subyacente, mientras que las empresas asumen la responsabilidad de proteger sus cargas de trabajo y aplicaciones en la nube.

Modelo de responsabilidad compartida de AWS



Fuente: https://aws.amazon.com/compliance/shared-responsibility-model/

Durante las últimas tres décadas, las organizaciones han estado construyendo y optimizando redes radiales complejas, de área amplia, conectando usuarios y sucursales al centro de datos a través de redes privadas. Estas redes radiales se protegían con pilas de dispositivos de seguridad, como VPN y cortafuegos, utilizando una arquitectura conocida como seguridad de castillo y foso. Este enfoque resultaba útil cuando la mayoría de los empleados trabajaban en oficinas corporativas y sus datos y aplicaciones residían en el centro de datos.

Hoy en día, los usuarios trabajan desde cualquier lugar y acceden con frecuencia a aplicaciones y datos que residen en la nube. Para una colaboración rápida y productiva, los usuarios necesitan acceso directo a las aplicaciones desde cualquier lugar y en cualquier momento. Ya no tiene sentido enrutar el tráfico de los usuarios de vuelta al centro de datos para obtener acceso y seguridad a fin de llegar a las aplicaciones alojadas en AWS.

A medida que los ataques cibernéticos se vuelven más sofisticados y los usuarios trabajan desde cualquier lugar, la seguridad del perímetro, que utiliza VPN y cortafuegos, brinda una seguridad incompleta e inconsistente, así como una experiencia de usuario deficiente por las siguientes razones:

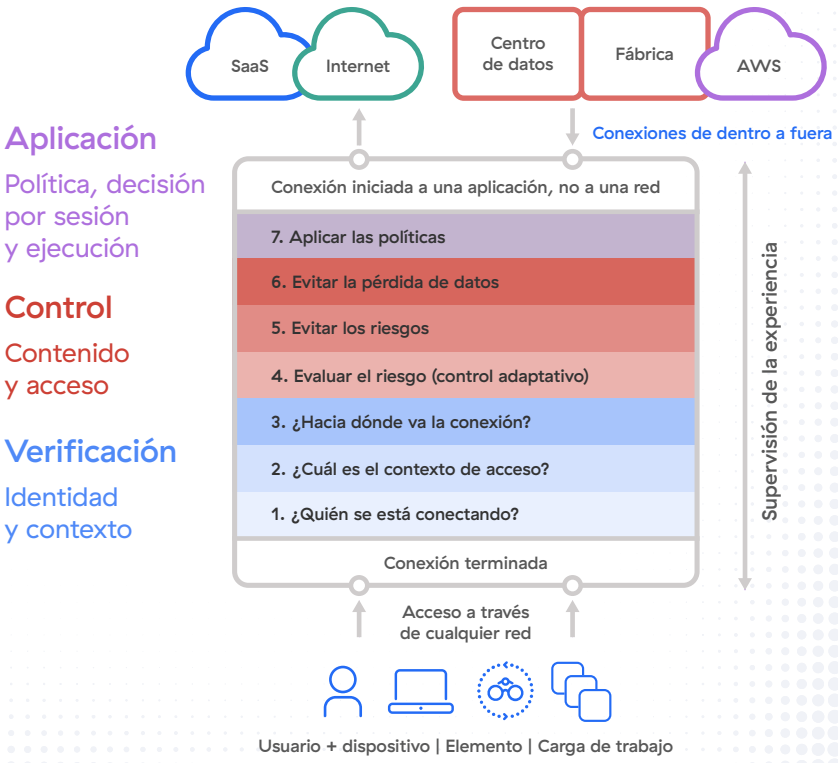
- Las VPN y los cortafuegos amplían la red corporativa, por lo que extienden la superficie de ataque y permiten que las amenazas se muevan lateralmente rápidamente, lo que genera brechas de seguridad.
- Un mosaico de productos puntuales de seguridad heredados presenta costes y complejidad, lo que resulta en ataques perdidos.
- El retorno del tráfico de usuarios remotos al centro de datos para obtener acceso y seguridad (bucles invertidos) da como resultado latencia, rendimiento lento y una experiencia de usuario deficiente.
- Los productos de múltiples proveedores brindan una seguridad inconsistente entre usuarios, dispositivos y ubicaciones, y dificultan la priorización de amenazas (múltiples paneles).
- Los adversarios eluden las defensas tradicionales con amenazas cada vez más sofisticadas entregadas a escala.
- A medida que las organizaciones se someten a la transformación de las aplicaciones (migrando aplicaciones a AWS o adoptando aplicaciones SaaS), deben alejarse de la seguridad de castillo y foso basada en cortafuegos y VPN e ir hacia una arquitectura moderna que asegure el acceso rápido y directo a las aplicaciones desde cualquier lugar y en cualquier momento.

Necesitan adoptar una arquitectura de confianza cero.

Zscaler Zero Trust Exchange

Zscaler, socio de software de nivel avanzado de AWS y un líder en seguridad de confianza cero durante una década, ha ayudado con éxito a miles de empresas a asegurar sus transformaciones digitales con Zscaler Zero Trust Exchange.

La arquitectura de confianza cero de Zscaler es una plataforma integrada que actúa como un panel de control inteligente para intermediar conexiones entre usuarios, dispositivos y aplicaciones en AWS. Cada solicitud se verifica utilizando la identidad y el contexto, como el tipo de dispositivo, la ubicación, la aplicación y el contenido. Una vez que se verifican la identidad y el contexto, la arquitectura de confianza cero evalúa el riesgo asociado con la solicitud de conexión, además de inspeccionar el tráfico en busca de ciberamenazas y datos confidenciales. Y, finalmente, se aplica la política antes de



establecer una conexión a las aplicaciones de AWS. Este enfoque moderno elimina los desafíos de seguridad, redes y retorno/rendimiento, lo que permite a las organizaciones acelerar sus migraciones de aplicaciones y cargas de trabajo a AWS al tiempo que brinda una seguridad superior y una experiencia de usuario positiva.

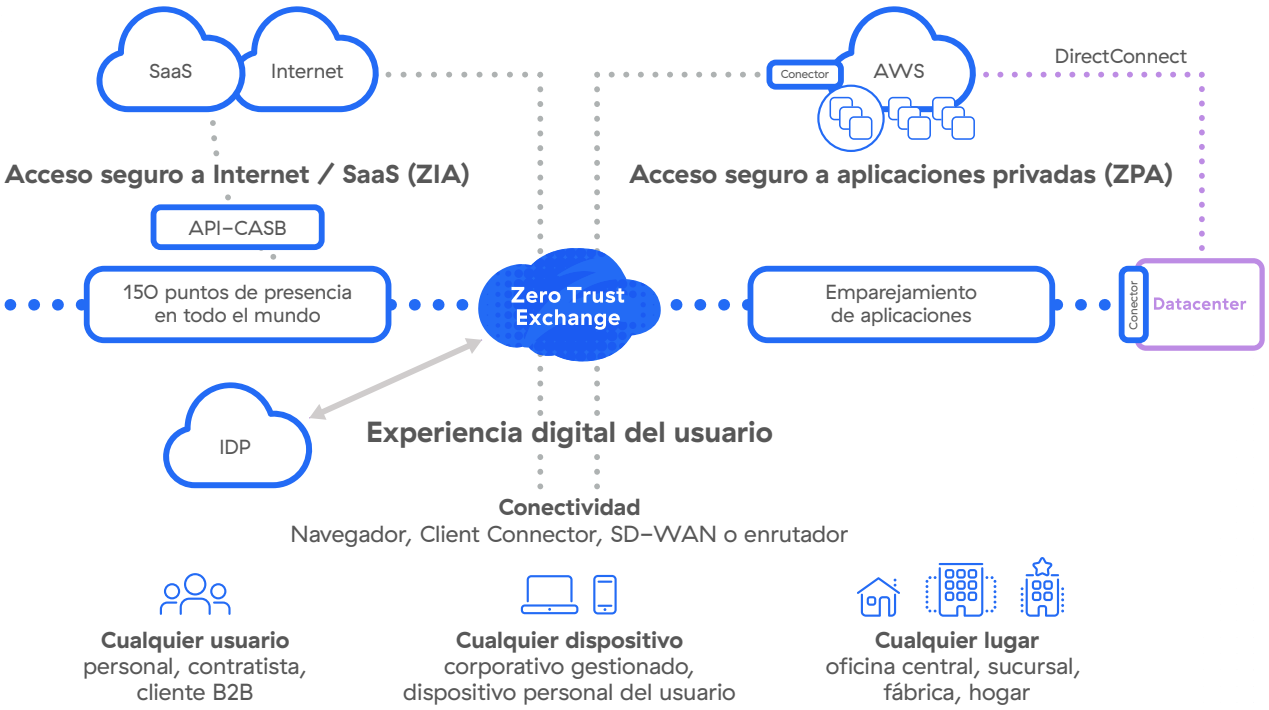
Zero Trust Exchange es la mayor nube de seguridad del mundo con más de 150 puntos de presencia (PoP) en todo el mundo y en la mayoría de las regiones de AWS a nivel mundial, incluidas GovCloud East y West. La arquitectura distribuida con centros de rendimiento garantiza que cualquier comunicación se pueda enviar directamente a AWS de manera eficiente y segura.

Cómo Zscaler y AWS impulsan la transformación digital segura

1. Protegiendo a los usuarios

Capacitar a un personal híbrido seguro y centrado en el usuario requiere flexibilidad para apoyar a empleados y terceros en cualquier ubicación y en cualquier dispositivo. Requiere una experiencia de usuario que ofrezca acceso rápido, seguro y confiable a datos, aplicaciones y cargas de trabajo dentro de AWS. Exige una solución que escale con la empresa y la proteja contra amenazas conocidas y desconocidas.

Zscaler protege a los usuarios de AWS:



- Conectando a los usuarios directamente a cargas de trabajo específicas de AWS y nunca a la red. Esto garantiza que las amenazas no puedan propagarse lateralmente para infectar a otros usuarios, dispositivos y aplicaciones.
- Haciendo que los usuarios y las aplicaciones se queden detrás del intercambio de confianza cero para hacerlos invisibles desde Internet.
  Los ciberdelincuentes no pueden atacar lo que no pueden ver. Como resultado, los usuarios no se ven afectados por el malware o amenazas cibernéticas como el ransomware y el phishing.

Esto permite a las organizaciones reducir significativamente el riesgo, mejorar la productividad y ofrecer una experiencia de usuario superior.

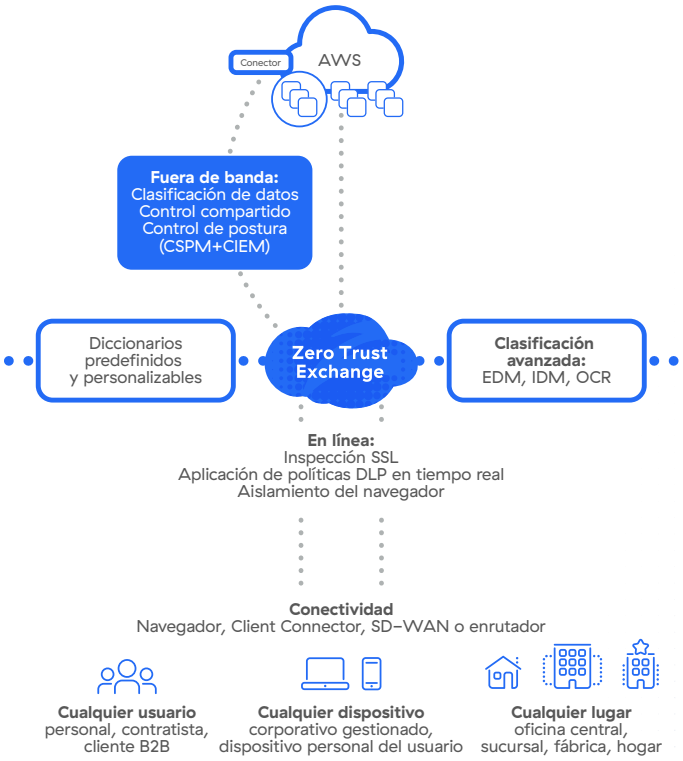
Zscaler es una solución nativa de la nube completa e integrada que reemplaza los productos puntuales heredados e inconexos, y cumple con la visión del perímetro del servicio de seguridad (SSE) al reunir varias tecnologías centrales para respaldar las cargas de trabajo de AWS. Entre ellas:

- Zscaler Internet Access (ZIA) para la puerta de enlace web segura en la nube (SWG), el agente de seguridad de acceso a la nube (CASB) o la prevención de pérdida de datos en la nube (DLP), entre otros
- Zscaler Private Access (ZPA) para el acceso a la red de confianza cero (ZTNA) de próxima generación
- Zscaler Digital Experience (ZDX) para la supervisión de la experiencia digital (DEM)

2. Protegiendo los datos

Los usuarios trabajan de forma remota desde diversos dispositivos, y acceden y cargan datos en ofertas de AWS como S3. Como resultado, los dispositivos de seguridad centrados en el perímetro no pueden proteger estos datos, y cambiar a un producto puntual diferente para cada nuevo caso de uso genera costes y complejidad.

Zscaler Data Protection sigue los datos dondequiera que vayan para hacer cumplir los principios de confianza cero. Los datos se analizan en línea para la clasificación en tiempo real y la aplicación de políticas. El aislamiento del navegador transmite datos como píxeles a dispositivos no administrados para detener la exfiltración.
Se analizan los datos en reposo en AWS en busca de información confidencial y se revoca automáticamente el uso compartido de riesgo. Posture Control corrige configuraciones incorrectas y permisos que exponen datos confidenciales; por ejemplo, depósitos de S3 públicos no deseados.



Zscaler Data Protection se distingue por:

- Ser parte de la plataforma de seguridad más unificada que satisface las necesidades de SSE y más
- Un motor de políticas unificado que protege los datos de manera consistente dondequiera que vayan
- Inspección SSL completa desde la mayor nube de seguridad y de mayor rendimiento del mundo
- Una plataforma comprobada implementada a escala en las organizaciones más grandes del mundo

3. Protegiendo las cargas de trabajo

A medida que las cargas de trabajo migran a la nube, las organizaciones tienen una necesidad urgente e imperiosa de modernizar sus redes y su seguridad para garantizar la competitividad empresarial. Las redes perimetrales que se diseñaron para entornos estáticos simplemente no pueden hacer frente a las necesidades de conectividad en la nube. Esto crea desafíos importantes para las organizaciones, como un área de superficie de ataque ampliada, riesgo de movimiento lateral de amenazas, productividad y colaboración reducidas, así como costes más altos y la complejidad de administrar arquitecturas de seguridad de red para proteger a un personal híbrido y las aplicaciones basadas en la nube.

Zscaler aborda estos desafíos para las organizaciones que utilizan AWS mediante la entrega de la solución integral Zscaler for Workloads, que protege las aplicaciones desde el momento de la compilación hasta la ejecución. Basada en una innovadora arquitectura de confianza cero, Zscaler for Workloads es una potente combinación de control de postura (CNAPP) y comunicaciones de carga de trabajo. Unifica la seguridad de las aplicaciones nativas de la nube y las basadas en máquinas virtuales que se ejecutan en AWS al reemplazar los productos puntuales de seguridad heredados con una solución completa diseñada para la confianza cero. Este enfoque consolidado no sólo elimina la necesidad de adquirir y administrar soluciones de productos puntuales que incrementan los costes y los gastos generales de administración, sino que también aumenta la colaboración multifuncional entre equipos y acelera la transformación digital.

Solución de seguridad en la nube para AWS

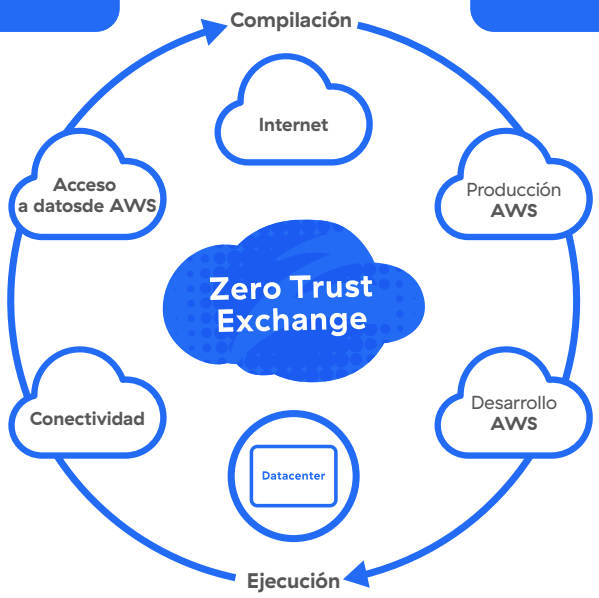
Control de postura (CNAPP)

Análisis de exposición (sin agente)

- Identifique los activos expuestos y la vulnerabilidad (superficie de ataque)
- Descubra datos confidenciales

Análisis de configuración

- Identifique y priorice las configuraciones incorrectas
- Identifique permisos excesivos para usuarios y cargas de trabajo



Workload Communications

Carga de trabajo a Internet

- Reducción de la superficie de ataque
- Prevención del compromiso del tiempo de ejecución y de la pérdida de datos sin cortafuegos/proxies virtuales

De carga de trabajo a carga de trabajo

- Cuentas de AWS
- De AWS al centro de datos

Segmentación

- Segmentación de usuario a aplicación, de aplicación a aplicación sin segmentación de red
- Microsegmentación basada en la identidad de la carga de trabajo de AWS

1. Posture Control (CNAPP)

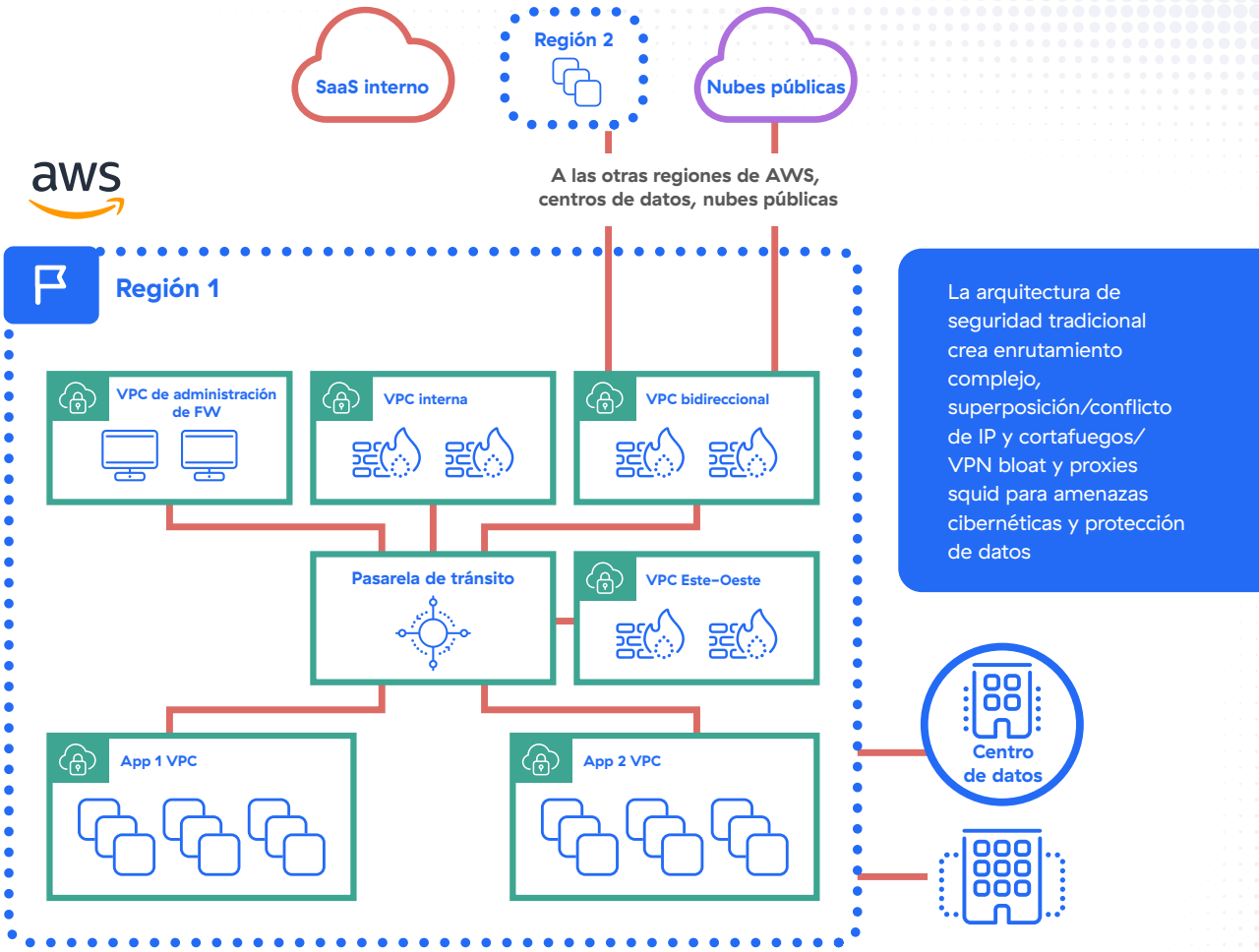
Posture Control, una plataforma de protección de aplicaciones nativas de la nube (CNAPP), reinventa la seguridad de las aplicaciones nativas de la nube como una solución 100 % sin agentes que utiliza el aprendizaje automático para correlacionar los riesgos ocultos causados por errores de configuración, amenazas y vulnerabilidades en las implementaciones de AWS. Capacita a los equipos de seguridad, desarrollo y DevOps para priorizar y remediar de manera eficiente los riesgos en aplicaciones nativas de la nube y basadas en máquinas virtuales lo antes posible en su ciclo de desarrollo.

Principales beneficios

- Reduce la complejidad y los costes de administrar múltiples soluciones puntuales para proteger los entornos en la nube y mantener el cumplimiento.
- Aplica políticas de seguridad uniformes en todos los servicios en la nube con un motor de políticas unificado.
- Previene configuraciones incorrectas y problemas de seguridad debidos a recursos y conjuntos de habilidades limitados.
- Aporta seguridad a los flujos de trabajo de los desarrolladores que prioriza y soluciona los riesgos críticos al tiempo que reduce la fatiga de las alertas.
- Aprovecha la potente capacidad de visualización y generación de informes para resaltar las vulnerabilidades de seguridad, las configuraciones incorrectas, los permisos y los datos expuestos.

2. Workload Communications

Con Workload Communications, Zscaler ha reinventado por completo la conectividad en la nube al permitir la confianza cero para las cargas de trabajo en la nube, lo que ofrece un acceso sencillo y seguro para las cargas de trabajo a Internet y las aplicaciones privadas. A diferencia de las soluciones de red heredadas, Workload Communications proporciona una arquitectura directa a AWS que utiliza la plataforma comprobada Zscaler Zero Trust Exchange para verificar la confianza en función de la identidad y el contexto para permitir una comunicación segura de carga de trabajo a Internet, una comunicación de carga de trabajo a carga de trabajo en múltiples regiones y zonas de disponibilidad de AWS, así como comunicaciones de carga a carga de trabajo dentro del entorno de AWS.

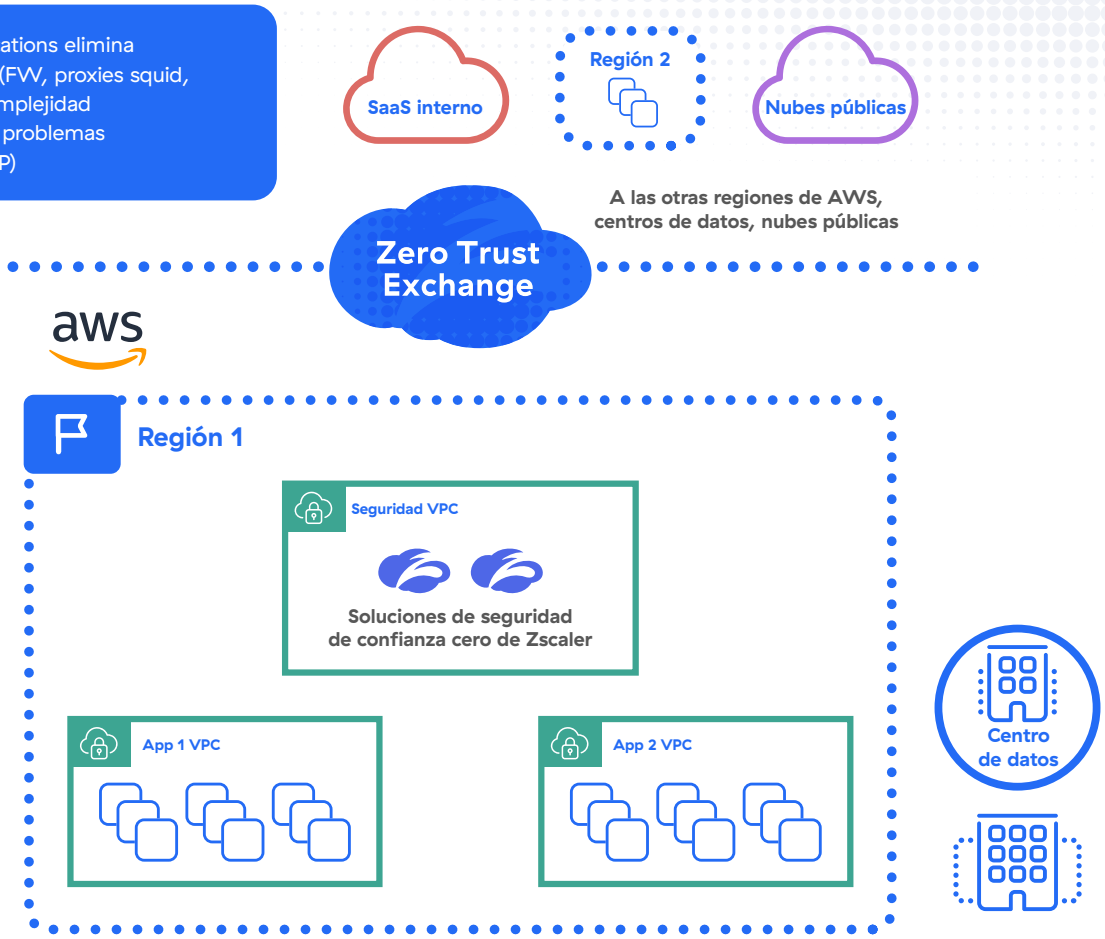


Principales beneficios

Workload Communications elimina la superficie de ataque de red al conectar directamente cargas de trabajo a Internet y a aplicaciones privadas mediante una arquitectura proxy completa. Esta arquitectura simplifica drásticamente la conectividad al eliminar el enrutamiento, las VPN, las puertas de enlace de tránsito, los centros de tránsito y los cortafuegos, al tiempo que permite el reenvío flexible y la administración de políticas de flexibilización mediante el uso del marco de políticas comprobado de ZIA y ZPA. Este enfoque único proporciona tres beneficios clave para los usuarios de AWS:

- Superficie de ataque cero y prevención de la pérdida de datos: al utilizar la arquitectura directa a la nube para sacar el tráfico de la red corporativa, las aplicaciones de los entornos AWS se vuelven invisibles para las ciberamenazas, lo que reduce el riesgo de pérdida de datos.
- Conectividad simplificada en la nube: la arquitectura de confianza cero también evita los cuellos de botella en el rendimiento, ya que se eliminan los problemas de solapamiento de IP, pues no se necesitan distribuciones de rutas y las cargas de trabajo se conectan directamente a otras aplicaciones.
- Rendimiento superior de la aplicación a escala: Zscaler se basa en una arquitectura verdaderamente distribuida en la que cada comunicación que llega al perímetro del servicio se procesa instantáneamente para determinar la identidad y el contexto. La relación de interconexión con AWS en la mayoría de las regiones del mundo, incluidas GovCloud East y West, garantiza la ruta más corta entre las aplicaciones sin importar dónde estén alojadas, lo que reduce la latencia y mejora el rendimiento de las aplicaciones.

Workload Communications elimina la sobrecarga de VM (FW, proxies squid, enrutamiento) y la complejidad del enrutamiento (sin problemas de superposición de IP)



Resumen

Juntos, Zscaler y AWS están ayudando a las organizaciones a impulsar sus viajes seguros de transformación digital, ofreciendo:

- Enrutamiento eficiente que reduce la latencia y acelera la migración de cargas de trabajo a AWS
- Simplificación de la arquitectura de red y seguridad mediante la eliminación de cortafuegos y VPN
- Acceso permanente que mejora la experiencia del usuario final
- Postura de seguridad más sólida y completa para eliminar las amenazas que tienen como objetivo las aplicaciones nativas de la nube
- Mayor agilidad empresarial para disfrutar de una ventaja competitiva
- Disminución de los costes para liberar fondos que estarían mejor destinados en otras áreas de la empresa

Las soluciones de seguridad de confianza cero de Zscaler están disponibles para su compra en AWS Marketplace. Tenemos todo lo que necesita para proteger a sus usuarios, datos y cargas de trabajo.

Más información sobre Zscaler para AWS

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

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