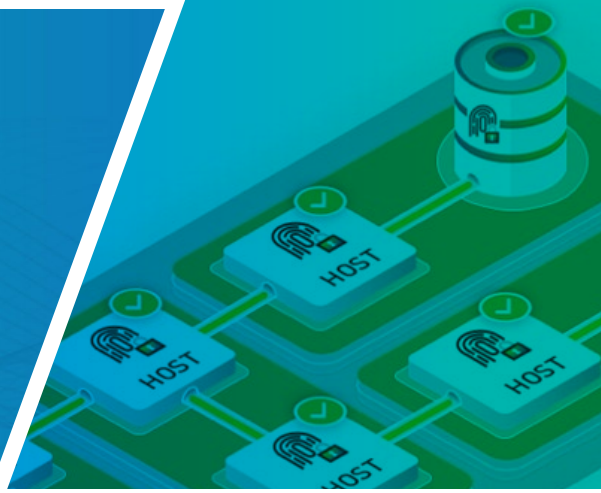
FICHA DE DATOS



ZSCALER™ WORKLOAD SEGMENTATION

Confianza Cero con un solo clic

Microsegmentación automatizada para nubes públicas y centros de datos

Microsegmentación increíblemente sencilla

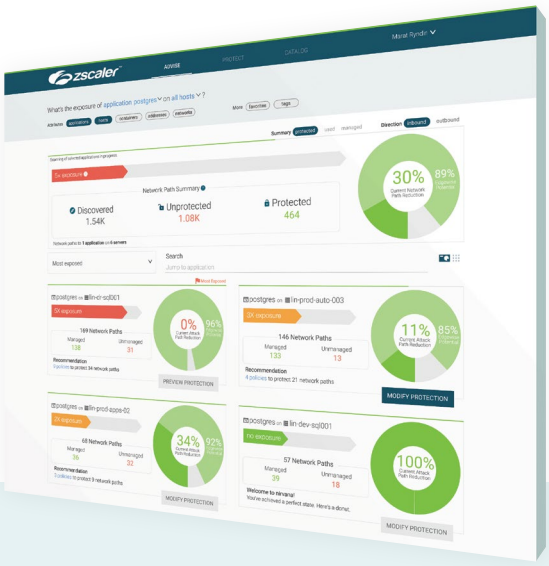
Las ciberamenazas necesitan vías de ataque para llegar a objetivos vulnerables. La forma más eficaz de reducir la superficie de ataque de la red es la segmentación y los expertos coinciden en que la microsegmentación es una estrategia básica de protección de las cargas de trabajo. Sin embargo, el tiempo requerido, la complejidad y el costo de implementar la segmentación han superado históricamente a su beneficio en materia de seguridad.

Ya no.

Zscaler Workload Segmentation es una nueva forma de microsegmentar su entorno. Es increíblemente sencillo y lo único que se necesita es un solo clic. Reduzca el riesgo y elimine el esfuerzo operativo permitiendo que Zscaler Workload Segmentation revele riesgos y le dé protección basada en identidad a sus cargas de trabajo, sin ningún cambio arquitectónico en sus redes y sin reiniciar. El modelo de software basado en identidad de Zscaler Workload Segmentation brinda protección sin fisuras con políticas que se adaptan automáticamente al entorno en el que se están ejecutando. La eliminación de la superficie de ataque de red nunca ha sido tan sencilla.

Valor de Zscaler Workload Segmentation

- Le da completa visibilidad de las comunicaciones de red este-oeste
- Políticas patentadas basadas en identidad que se adaptan a su entorno dinámico
- Protección basada en agentes para una seguridad y rendimiento máximos
- Optimiza sin esfuerzo las políticas para la reducción de riesgos y la facilidad operativa
- Rentabilidad previsible de su inversión en seguridad



> "...en algún momento, Zscaler Workload Segmentation podría implementarse en todas las empresas del mundo.
>
> goulston&storrs

Beneficios del control sensible a las aplicaciones

Las redes de nubes y centros de datos están llenas de datos atractivos para los ciberdelincuentes. A pesar de la solidez de sus controles de perímetro, los ciberdelincuentes pueden acceder a su red a través del phishing o cualquier otra forma de ingeniería social. Con una estrategia de seguridad tradicional basada en la red, una vez que los atacantes han robado credenciales o explotado una vulnerabilidad para obtener acceso a la red, están "a sus anchas": pueden introducir malware y moverse lateralmente dentro de las rutas de comunicación de la red de confianza para obtener acceso no autorizado a aplicaciones críticas. Pueden Tener una brecha en la red puede ser muy perturbador y causar daños financieros, de reputación y operacionales de gran alcance. A fin de evitar las comunicaciones no autorizadas entre este y oeste, las organizaciones necesitan controles de seguridad para centrarse en la *identidad verificada de las aplicaciones aprobadas.*

Zscaler Workload Segmentation permite a las empresas tomar conciencia de las aplicaciones y proteger cualquier red para no permitir que se comprometan las aplicaciones con controles de seguridad de confianza cero basados en la identidad criptográfica del software de comunicación.

Adoptar un enfoque de confianza cero

El enfoque de confianza cero y carga de trabajo basado en la identidad de Zscaler Workload Segmentation, abandona el modelo de seguridad tradicional de permitir la comunicación de las aplicaciones basada en direcciones IP, puertos y protocolos de confianza. Nuestro modelo de confianza cero trata las comunicaciones internas como si fuera Internet: potencialmente hostiles y llenas de amenazas. Solo las aplicaciones y los servicios verificados por su identidad criptográfica están autorizados a enviar y recibir comunicaciones, lo que redunda en una mayor seguridad que funciona dondequiera que lo hagan sus aplicaciones.

Autosegmentación patentada basada en identidad

La microsegmentación heredada implica varios pasos que pueden tomar meses. La microsegmentación de Zscaler Workload Segmentation se realiza en pocos minutos, con un solo clic. Desde el inventario de activos hasta el mapeo de los flujos de datos y la implementación de políticas para su aplicación, nuestra microsegmentación es rápida y sencilla.

La segmentación de Zscaler Workload Segmentation protege los datos y aplicaciones críticos en la nube híbrida a través de un plano de control fundamentalmente nuevo: la identidad del software. Todo el software de un entorno gestionado por Zscaler Workload Segmentation es sometido a un proceso de "toma de huellas dactilares" mediante una combinación de atributos de identidad criptográficos. La identidad del software es la base de cada decisión de control de acceso. Según nuestro modelo de confianza cero, si el software no puede ser verificado, no puede comunicarse, sin importar los permisos previos. Esto garantiza el mayor nivel de protección para sus cargas de trabajo, independientemente de los cambios en la red.

Protección de aplicaciones introducidas recientemente con la resegmentación automática

Si bien la segmentación automática es ideal para acelerar la implementación inicial de la microsegmentación, es igualmente importante asegurarse de que las aplicaciones recién introducidas también estén protegidas. Estas nuevas aplicaciones pueden tener vías de comunicación totalmente nuevas y también podrían interactuar con los servicios de aplicación existentes, todo lo cual debe ser protegido. Zscaler Workload Segmentation hace que la protección de estas nuevas aplicaciones sea increíblemente sencilla con la resegmentación automática, que se logra con un solo clic. Zscaler Workload Segmentation se basa en su segmentación existente y recomienda políticas nuevas o modificadas para abarcar las comunicaciones de la nueva aplicación, todo ello mediante un solo clic. Juntos, la autosegmentación y la resegmentación garantizan que su entorno dinámico esté siempre asegurado.

Esta nueva metodología significa que el control de seguridad se adapta a cualquier entorno, con menos políticas que administrar. La autosegmentación de confianza cero de Zscaler Workload Segmentation proporciona una protección más fuerte, simple y escalable para las nubes híbridas con seis atributos diferenciadores:

Las políticas se construyen automáticamente

El riesgo se reduce mediante la compresión de la política

Los resultados de seguridad son demostrables

Identidad del software verificada mediante atributos criptográficos

Los segmentos se adaptan para acomodar las actualizaciones y cambios de las aplicaciones

Las herramientas de supervisión de seguridad se enriquecen con datos de aplicaciones

Identidad de confianza cero

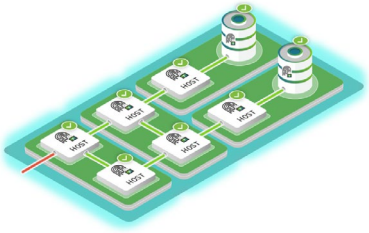
La tecnología que impulsa la microsegmentación automatizada de Zscaler Workload Segmentation se basa en la identidad de confianza cero (ZTID). Los atributos de identidad que comprenden la identidad de una carga de trabajo incluyen el hash SHA256, el hash difuso, la firma ejecutable, los valores de encabezamiento PE, el UID, los números de serie de la CPU, el nombre del host aprovisionado y más. Cada identidad única se informa al aprendizaje automático, que crea políticas recomendadas y es utilizado para tomar decisiones de control de acceso. Debido a que las políticas de Zscaler Workload Segmentation son de confianza cero, solo el software que puede ser verificado por su ZTID podrá comunicarse en sus redes, creando una red más segura pero operacionalmente eficiente.

Más sencillo para las operaciones

Microsegmente su entorno al instante, con un solo clic. Sus aplicaciones empresariales están protegidas y operativas automáticamente. No se requiere ningún cambio en la red. No hay necesidad de construir o actualizar manualmente una sola política. Y las largas jornadas de implementación son cosa del pasado.

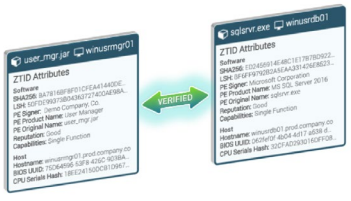
Más fuerte para la seguridad

Defina límites de microsegmentación en función de las interdependencias del software de comunicación, no de la dirección IP. Prevenga la propagación de malware y el abuso de las herramientas de administración verificando la identidad del software para autorizar las comunicaciones en su nube y centro de datos y asegúrese de que sólo las aplicaciones válidas de negocios se están comunicando.



Escalable para DevOps

A medida que se implementan sus cargas de trabajo, garantice que siempre tengan el acceso requerido para que las operaciones de negocio sean fluidas. A medida que su entorno se escala automáticamente, las políticas de Zscaler Workload Segmentation se adaptan automáticamente a los contenedores de VMs y Kubernetes, en las instalaciones o en la nube pública.



Administración centralizada para sus entornos de nube híbrida y de múltiples nubes

Zscaler Workload Segmentation proporciona el soporte más amplio en todos los entornos, así se trate de hardware en las instalaciones, una nube privada virtualizada, una nube pública o cualquier combinación de las mismas. Los entornos pueden ser estáticos o altamente dinámicos. Zscaler Workload Segmentation es compatible con 10 distribuciones de Linux (con más de 800 niveles de parches que datan desde la versión 2.6), Windows 7 y posteriores y cualquier sistema operativo Windows Server. Los entornos de contenedores soportados incluyen Kubernetes, Docker y AWS Elastic Container Service (ECS).

La plataforma y los productos continuamente en evolución de Zscaler Workload Segmentation están impulsados por APIs. Zscaler Workload Segmentation puede integrarse con las herramientas de seguridad y los procesos de DevOps existentes, permitiendo la autosegmentación con un solo clic.

Linux · Windows · Windows Server · kubernetes · docker · Amazon ECS · Azure · Google Cloud Platform · aws · vmware

Casos de uso de Zscaler Workload Segmentation

CONFIANZA CERO PARA LA PROTECCIÓN DE LA CARGADETRABAJO EN LA NUBE

Proteja sus aplicaciones críticas de negocio en entornos de nube desde una plataforma central.

MICROSEG-MENTACIÓN DE CONFIANZA CERO PARA EL CUMPLIMIENTO

Segmente las aplicacio-nes en "zonas seguras" para ver y detener las violaciones al cumpli-miento antes de que se produzcan.

MAPEO DEL FLUJO DE DATOS PARA LA VISIBILIDAD

Visualice la topología de su aplicación y vea cuándo se producen los cambios.

SEGURIDAD DE CONTENEDORES

Proteja las aplicaciones en entornos de producción efímeros sin interrumpir el flujo de trabajo de la IC/CD.

CORRELACIÓN DE EVENTOS Y SUPERVISIÓN DE SEGURIDAD

Introduzca los registros de comunicación de la aplicación en su SIEM, para poner en orden de prioridad las reparaciones.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, sólidos y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de los usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma alineada de seguridad en la nube del mundo.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com