

Mejorar la seguridad del centro de datos con la confianza cero



Cada vez existen más amenazas para la ciberseguridad. A medida que las organizaciones intentan proteger uno de sus tesoros más preciados, los datos, la confianza cero está rápidamente aventajando a los métodos tradicionales de seguridad de redes en el perímetro.

Seguridad de red en el perímetro

Se confía implícitamente en los sujetos de la red

El acceso se confiere según la ubicación física y la propiedad del dispositivo

La atención se centra en la protección de segmentos de red

Los ataques pueden propagarse fácilmente por toda la red (movimiento lateral)

Vs.

Seguridad de red de confianza cero

Se establece la confianza y se supervisa de forma continua

Se proporciona acceso con privilegios mínimos por sesión según la identidad, el rol y la necesidad

La atención se centra en la protección de los recursos

El acceso basado en roles puede reducir o prevenir el movimiento lateral de los ataques

Sin embargo, aunque numerosas soluciones de confianza cero se centran en proteger el extremo o el acceso a la red, corren el riesgo de pasar por alto una importante superficie de ataque: **el centro de datos**.

La importancia de la confianza cero en el centro de datos



Los adversarios están más motivados que nunca para penetrar en los centros de datos empresariales.



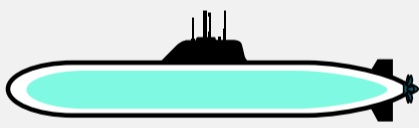
Dado que el centro de datos alberga la mayoría de las cargas de trabajo y aplicaciones físicas y virtualizadas que son fundamentales para el negocio de una organización, debe ser un componente central en el concepto y el diseño arquitectónico de la confianza cero.



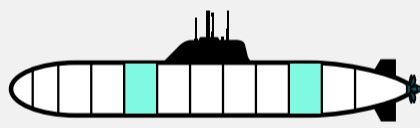
Confianza cero significa desconfiar de toda entidad de la red y de todo el tráfico dirigido al centro de datos, a menos que una política de seguridad explícita lo permita.

Microsegmentación: un requisito fundamental de la confianza cero

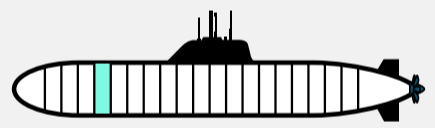
De la misma manera que los buques de guerra modernos están diseñados con cascos de acero compartimentados para limitar el impacto de un ataque, los centros de datos modernos deberían aprovechar la segmentación del diseño para limitar el alcance de los ataques a la seguridad.



Sin segmentación
Impacto operativo catastrófico



Con macrosegmentación
Impacto operativo significativo



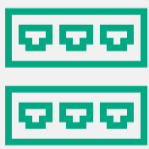
Con microsegmentación
Impacto operativo limitado

Impedir que los ciberdelincuentes se muevan por el submarino-centro de datos

Al inspeccionar todo el tráfico de este a oeste en el centro de datos y aplicar políticas a nivel micro a cargas de trabajo y aplicaciones individuales (independientemente de dónde se estén ejecutando), la confianza cero permite a las organizaciones detener el movimiento de los ciberdelincuentes por la red del centro de datos.

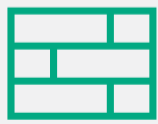
Limitaciones de las soluciones de segmentación tradicionales

Tradicionalmente, las organizaciones disponen de una cantidad limitada de soluciones para la microsegmentación en su centro de datos, y todas ellas presentan desventajas.



Lista de control de acceso sin información de estado de conmutador Ethernet

Seguridad insuficiente



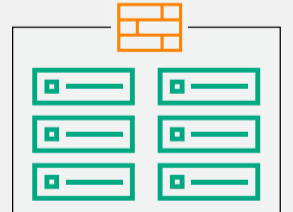
Dispositivo de cortafuegos de hardware

Caro y complejo



Dispositivo de cortafuegos virtualizado

Limitaciones de escalabilidad y rendimiento



Cortafuegos basado en agentes de software

Costoso, impuesto al servidor CPU

Pero ahora existe una nueva clase de soluciones que te ayudarán a superar las limitaciones de diseño, rendimiento y costes de las soluciones heredadas. Con ellas, podrás ampliar la segmentación de confianza cero al centro de datos de forma más exhaustiva, lo que mejorará la postura de seguridad.

Equípate con lo mejor para satisfacer las crecientes demandas empresariales con una arquitectura de confianza cero que escala y refuerza significativamente la seguridad de las cargas de trabajo para tareas cruciales.

Tu centro de datos necesita una red en la que se priorice la seguridad.

Más información en

[HPE.com/edge](https://www.hpe.com/edge)

Visita **HPE GreenLake** 



Chat con Ventas