10 COMPONENTES de los centros de datos de confianza cero

Los verdaderos centros de datos de confianza cero priorizan la experiencia de los usuarios finales.

Como resultado:

- *El acceso es rápido, confiable y escalable.*
- *Los usuarios y los dispositivos están protegidos.*
- *Las aplicaciones y las cargas de trabajo protegen los datos.*
- *La seguridad agiliza los negocios.*

10 ACCEDA A UNA VISIBILIDAD TOTAL

No se puede proteger lo que no se ve.

Es necesario contar con una vista integral de la red en diferentes entornos y de la protección de la que goza cada uno de sus segmentos, del cliente a la carga de trabajo.

9 APLIQUE LA SEGMENTACIÓN EN VARIOS PUNTOS

Analice cada detalle.

Desde los usuarios y los dispositivos hasta las aplicaciones y las cargas de trabajo, la segmentación y el control detallados pueden impedir el acceso no deseado y las fallas de seguridad.

8 ASIGNE IDENTIDADES A USUARIOS, DISPOSITIVOS Y CARGAS DE TRABAJO

La identidad no tiene por qué limitarse a los usuarios.

Si la aplica también a los dispositivos y las cargas de trabajo, los diversos factores de la identidad le serán de gran ayuda para detectar riesgos en la red en todo momento.

7 DISFRUTE DE POLÍTICAS EFICACES Y SIN LÍMITES FÍSICOS

Siga a los usuarios, dispositivos y aplicaciones adonde sea que vayan.

Los usuarios, las aplicaciones y las cargas de trabajo están siempre en movimiento, por lo que es necesario que las políticas de seguridad los sigan adonde vayan para evitar posibles vectores de ataque.

6 COMPRENDA LA INTENCIÓN DEL TRÁFICO DE RED

¿Cuál es el destino y el objetivo del tráfico?

Acceda a toda la información posible sobre el tráfico de la red y su destino, incluso aunque esté cifrado. Para ello, empiece por observar indicadores y comportamientos específicos del tráfico.

5 AUTOMATICE TODOS LOS PROCESOS POSIBLES

Saque el máximo provecho de la automatización.

La automatización facilita el trabajo, mejora la eficacia de los equipos, garantiza que los cambios implementados en una parte del centro de datos se apliquen a todas las demás y permite responder a los ataques incluso antes de que se conviertan en incidentes.

4 SUPERVISE Y UTILICE TODOS LOS PUNTOS DE CONEXIÓN

Lleve la seguridad a nuevas fronteras.

Use los enrutadores y los conmutadores para detectar amenazas y garantizar el cumplimiento de las normas a fin de proteger los entornos de los centros de datos.

3 DÉ POR SENTADO EL BLOQUEO DE AMENAZAS BÁSICAS

Huelga decir que, si una tecnología de seguridad no puede responder a las amenazas conocidas, no tiene sentido invertir en ella.

Los datos no mienten. Averigüe usted mismo qué proveedores de seguridad son los más eficaces en la detección de amenazas y en la contención de los ataques a la red.

2 OPTIMICE EL TIEMPO DE ACTIVIDAD DE LAS APLICACIONES

Las fallas no son nunca una opción viable.

El éxito de las empresas depende del funcionamiento de la red y de la conectividad de los recursos, así que no sería lógico sacrificar esos aspectos por implementar un buen sistema de seguridad. Cerciórese de que sus soluciones de seguridad sean confiables, ofrezcan una tolerancia a fallos sumamente rápida y brinden el nivel de transferencia de datos que su empresa necesita.

1 AVANCE A PASO FIRME

No se desvíe de este camino.

No se preocupe si aún no tiene todo resuelto. El hecho de que el marco de confianza cero despierte su interés ya es un buen punto de partida. Simplemente elija un elemento que quiera implementar y, más temprano que tarde, podrá disfrutar de un centro de datos de confianza cero. Dar un paso a la vez siempre es mejor que quedarse quieto.

Téngase confianza.

NO SE OLVIDE DEL BORDE

Los datos constituyen el eje de toda iniciativa de seguridad. El secreto para salvaguardar su centro de datos también yace en tener un sistema de seguridad eficaz que se extienda al borde para poder proteger el acceso a los datos. Proteja el acceso de los usuarios y dispositivos a las aplicaciones y los datos que residen en sus entornos de centros de datos y optimice la defensa de toda la red.

Juniper Networks

3050187-001-ES Agosto de 2023