5 aspectos clave para seleccionar una solución de acceso a la red de confianza cero

netskope

5 aspectos clave para seleccionar una solución de acceso a la red de confianza cero

Las empresas están adoptando rápidamente Security Service Edge (SSE) para aprovechar de forma segura las ventajas de una arquitectura SASE. Una pieza fundamental de SSE es la solución de acceso a la red de confianza cero (ZTNA) que permite a los usuarios conectarse a una aplicación determinada en cualquier lugar. Security Service Edge ayuda a consolidar las funciones de seguridad, disminuye los costos totales de propiedad y mejora la eficiencia operativa a largo plazo, lo que se traduce en una mejor seguridad general.

netskope

La plataforma importa

Si está seleccionando e implementando ZTNA para un proyecto de trabajo remoto/híbrido, un proyecto inicial en un viaje de seguridad de confianza cero más grande, o si cuenta con una visión perfectamente planificada para SSE y SASE, es mejor trabajar con un proveedor que tenga una plataforma SSE completa: un solo agente, una sola consola y un solo motor de políticas, compatible con un entorno de diferentes nubes.

Gartner estima que «en 2025, el 70"% de las organizaciones que implementan el acceso a la red de confianza cero (ZTNA) basado en agentes seleccionará un proveedor de servicios de seguridad (SSE) para ZTNA, en lugar de una oferta independiente, en comparación con el 20"% que lo hacía en 2021*».

*Gartner, «Magic Quadrant for Security Service Edge» (Cuadrante mágico para SSE), John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, 15 de febrero de 2022

02

Facilite el trabajo híbrido en cualquier lugar

Para facilitar el trabajo híbrido desde cualquier lugar, es importante seleccionar un proveedor que tenga una presencia multinacional que se ajuste a su plan de expansión global y agilidad empresarial. Asegúrese de trabajar con un proveedor de ZTNA que cuente con centros de datos en las principales regiones desde donde se puedan conectar sus empleados. Para seleccionar su proveedor no solo debe basarse en los centros de datos, sino en escoger uno que cuente con una pila de seguridad completa disponible en cada región, con una capacidad completa en el perímetro, cerca de los usuarios, rampas de acceso de baja latencia y una amplia interconexíon (peering) para lograr la mejor experiencia para los usuarios y las aplicaciones.

Políticas fáciles de configurar

Además de un solo agente, únicamente debe existir un paso para configurar las políticas de acceso e identidad mediante una consola unificada. Podrá disfrutar de las ventajas de facilitar el acceso a la nube y aplicaciones privadas en solo días para respaldar fusiones y adquisiciones, u otras actividades con plazos definidos.

No se quede atrás con una aplicación VPN y reglas de *firewall* complejas que intentan suplantar a un verdadero ZTNA.

Proteja la información en cualquier lugar

Su solución ZTNA debe detectar el uso de datos, las actividades y las anomalías del comportamiento (UEBA, por sus siglas en inglés) de las personas que están conectadas a la red de la organización, hacer cumplir las reglas y políticas DLP avanzadas y aplicar políticas de acceso adaptables basadas en los riesgos del usuario.

ZTNA conecta de forma segura a usuarios con aplicaciones y recursos privados. Con frecuencia, dichos recursos son el activo más importante de la organización, que van desde el código hasta otras formas de datos patentados, como la información confidencial. Seleccione una solución que ofrezca diferentes opciones para que su organización sea capaz de proteger la información. Por ejemplo, una solución moderna de ZTNA debería ofrecer opciones para comprobar el tráfico y aplicar DLP para proteger los datos. Sin embargo, es posible que algunas organizaciones prefieran fijarse en análisis UEBA y en calificaciones de riesgo de los usuarios para obtener contexto en tiempo real, sin descifrar el tráfico o para minimizar el riego interno.

05

Integración eficaz de terceros

Con las integraciones e intercambios adecuados en entornos con varios proveedores, ZTNA puede ser una gran opción. Los mejores intercambios proporcionan puntuaciones fiables de usuarios y dispositivos que se normalizan en todo el entorno y pueden activar controles de acceso adaptables, configuraciones de grupos de usuarios y una emisión automática de tickets para investigaciones.

Conclusión

Recuerde que la confianza cero NO significa no confiar en nadie, ya que para permitir el desarrollo de la empresa es necesario ampliar el acceso (confianza). La clave para que su organización pueda sacar rendimiento a los principios de confianza, tanto de forma específica con ZTNA como de cualquier otra forma, es mediante la tecnología adecuada para tomar mejores decisiones sensibles al contexto sobre la confianza y el acceso para un usuario determinado, además de supervisar y adaptarse continuamente para reducir los riesgos. Este contexto se basa en varios factores, como el rol y la identidad del usuario, la identidad del dispositivo, la posición de seguridad, el tipo de aplicación, el riesgo de la aplicación y la instancia de la aplicación, además del nivel de confidencialidad de los datos. Las decisiones contextuales se traducen en políticas de acceso sólidas y optimizadas para el riesgo y se pueden aplicar de forma uniforme en la nube, la web y las aplicaciones privadas, mientras la empresa gana en agilidad y el usuario es más productivo.

Más información

Netskope, líder mundial en ciberseguridad, está redefiniendo la seguridad de la nube, los datos y la red con el objetivo de ayudar a las organizaciones a utilizar los principios de confianza cero para proteger sus datos. La solución Intelligent Security Service Edge (SSE) de Netskope es rápida y fácil de usar, y protege a las personas, los dispositivos y los datos en cualquier lugar.

Para conocer la forma en que Netskope ayuda a los clientes a prepararse para cualquier cosa durante su viaje SASE, **visite netskope.com.**