CLOUDFLARE

PUBLICACIÓN DIGITAL

Guía de implementación de SASE para los CISO

Cómo evaluar plataformas de SASE para casos de uso prioritarios

La misión de consolidar la ciberresiliencia

El Instituto Nacional de Estándares y Tecnología (NIST) define la ciberresiliencia como la habilidad de anticipar, sobrellevar, superar y adaptarse a condiciones adversas, tensiones, ataques y peligros que ponen en riesgo a los sistemas que usan recursos cibernéticos o se basan en ellos.

Ahora bien, fortalecer la ciberresiliencia (y a la vez reducir los costos de la mitigación de filtraciones) supone muchos desafíos:

- **Los ciberdelincuentes desarrollan tácticas cada vez mejores:** a medida que los atacantes desarrollan herramientas, técnicas y procedimientos más sofisticados, a las organizaciones les cuesta cada vez más protegerse de ellos
- **Los entornos informáticos son cada vez más complejos:** debido a la gran cantidad de aplicaciones y dispositivos conectados a las distintas arquitecturas multinube, crear entornos seguros es un proceso complicado y costoso
- **Los equipos internos están sobrecargados:** a las organizaciones les cuesta administrar sus recursos debido a las limitaciones de presupuesto y las cargas de trabajo excesivas

Para superar estos desafíos, muchos CISO optan por implementar un modelo de perímetro de servicio de acceso seguro (SASE). A diferencia de alternativas anteriores, la arquitectura SASE unifica la seguridad y las redes en una plataforma en la nube que garantiza una constante visibilidad y control. En este esquema, los controles de red se ubican en el perímetro de la nube (y no en el centro de datos corporativo), y eso permite que las empresas brinden un acceso seguro y simple a cualquier usuario, aplicación, dispositivo o red, sin importar su ubicación.

En esta guía se cubren algunos de los casos de uso más comunes de SASE y se describen los principales pasos a seguir para implementar una arquitectura de este tipo con el objetivo de reforzar tu ciberresiliencia y conseguir beneficios instantáneos.

Caso de uso n.° 1:

Adopción del acceso a la red Zero Trust (ZTNA)

Cuando las empresas dependen de un sistema de seguridad basado en el perímetro tradicional para el trabajo híbrido, los entornos multinube y los dispositivos no administrados, experimentan problemas como una visibilidad limitada, configuraciones conflictivas y muchos riesgos. Una estrategia Zero Trust, con controles de acceso granulares que aseguran que ninguna entidad se tome por confiable de antemano, puede ayudarte a modernizar tu estrategia de seguridad de las siguientes maneras:

Reemplazo de los elementos de seguridad tradicionales basados en hardware

Los controles de perímetro de red tradicionales, como las redes privadas virtuales (VPN), son difíciles de escalar, afectan la visibilidad y hacen que sea más difícil para los equipos de seguridad detectar y mitigar ataques. Un modelo SASE es una alternativa segura porque implementa un acceso a la red Zero Trust (ZTNA), a la vez que se encarga del enrutamiento y el procesamiento del tráfico en una red global en la nube, lo que reduce la fricción del usuario final y el movimiento lateral.

Administración del acceso a los dispositivos

Dar acceso a terceros, como contratistas, agencias y proveedores, supone riesgos: de forma accidental, las organizaciones pueden dar más privilegios que los necesarios o garantizar acceso a dispositivos no administrados. La arquitectura SASE permite a las organizaciones establecer políticas Zero Trust sin clientes y así asegurar que los terceros solo tengan acceso a lo que necesitan.

Prevención de ataques de ransomware

Un ransomware puede propagarse rápidamente por toda una red y, en algunos casos, incluso por más de una o más allá de una organización. La arquitectura SASE evita la propagación de los ataques de ransomware, ya que impide el acceso a la red y las aplicaciones en cuanto se detecta una infección. Este enfoque, basado en el principio Zero Trust de "control de acceso con mínimos privilegios", dificulta que los atacantes escalen privilegios y se muevan lateralmente dentro de una red.

Reducción de la exposición de datos

La exposición y la exfiltración de datos suponen una grave amenaza para las organizaciones, ya que los usuarios cargan o distribuyen información confidencial a través de aplicaciones autorizadas y no autorizadas. Para prevenir la exposición de datos, las políticas Zero Trust y la arquitectura SASE limitan a qué aplicaciones tiene acceso cada usuario y escanean las suites SaaS más populares en busca de datos confidenciales y configuraciones erróneas.

CASO PRÁCTICO

Implementación de una estrategia Zero Trust

Un proveedor de telecomunicaciones incluido en la lista Fortune 500 usa la plataforma SASE de Cloudflare para proteger su entorno de trabajo híbrido con más de 100 000 empleados y cientos de aplicaciones alojadas en AWS, Azure y otros entornos en la nube. Gracias a una arquitectura de red Zero Trust basada en la identidad, una puerta de enlace web segura y controles de acceso unificados, logran proteger a los usuarios de amenazas sin necesidad de combinar múltiples interfaces de creación de políticas, VPN y servicios de filtrado de Internet.

Caso de uso n.º 2:

Protección de las superficies de ataques

La transformación digital y el teletrabajo ampliaron la superficie de ataques: hay más usuarios descentralizados y dispositivos no gestionados que necesitan acceder a recursos internos. Pero extender los firewalls locales a la nube y ampliar las redes mediante el uso de VPN puede dejar a las organizaciones más expuestas a las amenazas externas e internas, y a la vez reducir su visibilidad. Una arquitectura SASE permite a las organizaciones ampliar la visibilidad y los controles para contar con un modelo "sin perímetro" y una protección uniforme. Esto se logra de las siguientes maneras:

Mitigación del phishing multicanal

Los atacantes suelen usar el phishing en canales donde los usuarios tienden a tener la guardia baja a la hora de hacer clic, en especial en aquellas herramientas que no siempre están protegidas por los controles de seguridad del correo electrónico. Una plataforma SASE unificada ofrece una protección integral en todos los entornos a fin de mitigar el riesgo de robo de credenciales, apropiación de cuentas y exfiltración de datos.

Protección de los trabajadores remotos

El teletrabajo requiere que los usuarios se conecten desde distintas ubicaciones y dispositivos, a menudo fuera del alcance de las organizaciones que los emplean. Una arquitectura SASE permite a las organizaciones proteger el acceso de los empleados y terceros a entornos y datos esenciales. Esto ayuda a mejorar la seguridad y la productividad del teletrabajo.

Mejora de la experiencia del usuario

A la hora de filtrar el tráfico de las oficinas, los métodos tradicionales reenvían el tráfico a centros de datos corporativos centralizados, y eso genera latencia y perjudica la productividad. Pero la alternativa (dar a los usuarios acceso directo a Internet) implica riesgos de seguridad y afecta la experiencia del usuario. Una arquitectura SASE gestiona y optimiza de forma inteligente las conexiones directas a cualquier nube o destino de Internet, y aplica políticas y protecciones en los puntos más cercanos posibles a los usuarios finales.

Protección de las redes de área amplia (WAN)

Algunas WAN eluden la seguridad de la nube en el tráfico entre filiales, por lo que las garantías de integración entre los servicios de seguridad y las WAN definidas por software pueden no ser muy sólidas. Una arquitectura SASE permite a las organizaciones simplificar y proteger la forma en que se conectan a través de las WAN, ya que filtra e inspecciona el tráfico entre oficinas, centros de datos, nubes públicas y otras ubicaciones dentro y fuera de Internet en su conjunto.

CASO PRÁCTICO

Protección de las superficies de ataques en expansión

Durante su migración a la nube, Werner Enterprises implementó nuestros servicios SASE con eficacia; no hubo interrupciones operacionales ni en los servicios que brindan a los clientes. Luego de ese proceso, lograron reducir en más de un 50 % los correos electrónicos maliciosos, ahorrar varias horas de trabajo diarias de análisis manual de correos electrónicos y permitir que el equipo de seguridad se centrara en objetivos empresariales más estratégicos.

Caso de uso n.º 3:

Protección de los datos en todas partes

En la medida en que los datos se extienden por más entornos, a las organizaciones les resulta más difícil hacer un seguimiento de ellos. El uso no autorizado de la inteligencia artificial generativa y elementos de shadow IT puede dejar expuestos datos confidenciales, lo que podría dar lugar a vulnerabilidades o fugas costosas de contrarrestar. Una arquitectura SASE combina la visibilidad de datos y controles en entornos web, SaaS y de aplicaciones privadas, y eso ayuda a las organizaciones a lograr lo siguiente:

Simplificar el cumplimiento normativo en materia de privacidad de datos

El auge de los modelos lingüísticos de gran tamaño (LLM) y otras herramientas de IA requiere que la normativa se adapte para proteger los datos de los usuarios. Una arquitectura SASE garantiza la seguridad y la privacidad de los datos gracias a que unifica los respectivos controles y permite que los equipos de seguridad puedan bloquear las clases de datos regulados, reducir el riesgo de fugas y cumplir con los estrictos requisitos correspondientes de forma persistente.

Administrar elementos de shadow IT

Los elementos de Shadow IT (aplicaciones no autorizadas que no están administradas ni protegidas por las organizaciones que las utilizan) pueden plantear riesgos cuando alojan datos confidenciales o estos pasan por ellos. Una arquitectura SASE minimiza estos riesgos gracias al redireccionamiento del tráfico mediante proxy a través de agentes de seguridad de acceso a la nube (CASB) en línea que registran cada conexión y solicitud, detectan si hay aplicaciones no autorizadas y permiten a las organizaciones controlar cómo se accede a ellas y cómo se utilizan.

Usar la IA generativa de forma segura

A medida que más organizaciones implementan la IA, también aumenta el riesgo de exponer datos confidenciales. Gracias a una puerta de enlace web segura y un agente de seguridad de acceso a la nube en línea, un enfoque SASE permite a los equipos de seguridad detectar y aprobar el uso de aplicaciones de IA, analizar errores de configuración que supongan riesgos de fuga de datos o ejecutar aplicaciones de IA en navegadores web aislados para restringir la entrada y la salida de datos.

Proteger los datos confidenciales

Una arquitectura SASE permite a las organizaciones detectar y controlar cómo se mueven los datos confidenciales dentro, alrededor y fuera de sus entornos informáticos. Además, facilita el análisis de aplicaciones y la inspección del tráfico en busca de datos personales regulados y propiedad intelectual, el bloqueo de amenazas web como el phishing y el ransomware, y protecciones adicionales contra el robo de datos y las filtraciones inadvertidas.

CASO PRÁCTICO

Protección de datos en cualquier lugar

Applied Systems usa nuestros servicios de SASE para proteger el acceso de más de 2500 empleados a las aplicaciones autoalojadas y la infraestructura. Este nuevo enfoque le da a su equipo de seguridad la flexibilidad necesaria para aplicar controles rigurosos en función de las distintas necesidades de los usuarios y, a la vez, controlar cómo se comparten sus datos con las herramientas de IA.

Elegir una solución SASE:

Unificación mediante un proveedor único vs. numerosas soluciones específicas

Una solución SASE de proveedor único combina las funciones de red y seguridad en un único servicio que se presta en la nube. De esta manera, las empresas pueden unificar diferentes productos específicos, eliminar dispositivos y garantizar que sus políticas se apliquen de forma continua. Si bien implementar una solución SASE de múltiples proveedores puede dar resultados similares a los de un enfoque de proveedor único, a menudo la complejidad y los costos son mayores, y la visibilidad y la flexibilidad internas, menores.

Combinar estas funciones en una plataforma unificada te permite aprovechar la verdadera esencia de SASE: una infraestructura de red y seguridad sencilla y eficiente que reduce los costos totales de propiedad y se adapta con facilidad para responder a las cambiantes necesidades de tu empresa.

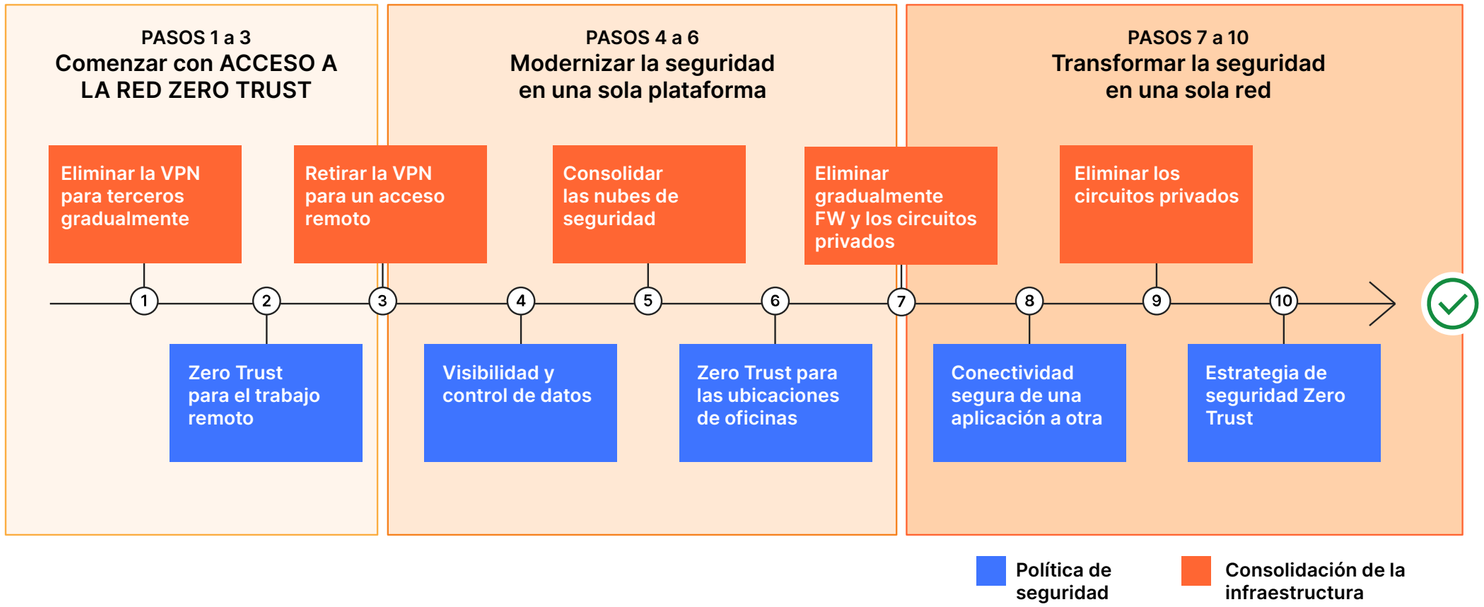
Cuando evalúes posibles proveedores de SASE, plantéate lo siguiente:

1. ¿Los motores de detección de amenazas y datos confidenciales pueden desencriptar e inspeccionar el tráfico de las aplicaciones en un único paso? ¿Hay limitaciones de implementación?
2. ¿Están protegidos todos los flujos de datos y las comunicaciones a través de las suites SaaS en todos los canales (actividad web y de correo electrónico en línea y fuera de banda)?
3. ¿Está habilitado el aislamiento remoto del navegador para cada usuario y aplicación? ¿Cómo afecta esto a la productividad? ¿Genera gastos adicionales?
4. ¿Se pasan por alto funciones de seguridad en algún acceso a la red?
5. ¿Es posible asegurarse de que el tráfico de los clientes permanezca aislado y privado en la arquitectura de nube multiinquilino?
6. ¿Qué funciones de localización de datos están disponibles? ¿Habilitarlas agrega latencia para los usuarios remotos que se conectan fuera de tu región localizada?
7. ¿Puedes integrar tus fuentes de información sobre amenazas en su arquitectura? ¿Cómo reduce la plataforma los falsos positivos de las fuentes de información sobre amenazas?
8. ¿Qué tipo de puntuación y análisis de riesgos de usuarios/dispositivos están disponibles? ¿Se puede aplicar la puntuación de manera uniforme en todas las aplicaciones?

Cómo Cloudflare ofrece SASE

Para recorrer el camino hacia una plataforma SASE unificada, muchas empresas confían en Cloudflare. Somos el único proveedor de SASE que empezó a ofrecer una arquitectura de red Zero Trust con una conectividad basada en la identidad y el contexto, integrada de forma sistemática en toda nuestra plataforma.

Tu hoja de ruta a largo plazo para implementar una arquitectura SASE completa debería seguir este procedimiento:



Con el respaldo de una red global que abarca más de 310 ciudades de todo el mundo, Cloudflare ayuda a los CISO a mejorar la seguridad, la resiliencia y el rendimiento de las empresas al máximo nivel. Nuestro panel de control único combina soluciones específicas en varios dominios de seguridad y está orientado a que las organizaciones puedan simplificar sus operaciones de seguridad y garantizar una protección constante contra las amenazas en constante evolución.

Visita nuestro sitio web para obtener más información sobre Cloudflare y su plataforma SASE.

Teléfono: +55 (11) 3230 4523
Correo electrónico: enterprise@cloudflare.com
Web: www.cloudflare.com/