

# Introducción guiada al SASE unificado

Para un proceso de adopción de SASE más sencillo  
y rentable

# 48 %

“A finales del año 2023, el 48 % de los trabajadores cualificados trabajarán de forma híbrida y enteramente a distancia, frente a un 27 % en 2019, con el 39 % de ellos trabajando de forma híbrida, frente a un 12 % en 2020<sup>1</sup>, lo que aumentará la demanda de soluciones SASE.

# 46 %

“En los próximos 12 meses, el 46 % de las organizaciones habrá implementado una arquitectura SASE”<sup>2</sup>

# 65 %

“En 2025, el 65 % de las empresas habrá consolidado componentes de SASE individuales en uno o dos proveedores de SASE con los que se habrá asociado explícitamente”<sup>3</sup>

## El auge del SASE unificado: una ruta hacia el SASE más sencilla y rentable

A lo largo del último año, muchos líderes de TI han adoptado el marco de extremo para servicios de acceso seguro (SASE, Secure Access Service Edge) a fin de permitir una conectividad más rápida y segura en sus organizaciones globales. SASE hace converger las funciones de soluciones de red y seguridad en un único servicio nativo de la nube que ofrece constancia de conectividad y seguridad desde cualquier lugar.

SASE no es solo una tendencia tecnológica; es un imperativo estratégico para las empresas modernas que desean prosperar en la era digital.

No obstante, no todas las soluciones SASE son iguales. Algunos proveedores de SASE ofrecen soluciones multipunto vagamente integradas o que requieren enrutamiento entre PoP de distintos proveedores, lo que puede implicar latencia, problemas de rendimiento y sobrecarga de gestión.

Por otro lado, existen soluciones SASE que ofrecen todas las funciones fundamentales de SASE desde una única plataforma estrechamente integrada, lo que mejora el nivel de seguridad, la eficacia del personal, la experiencia de administradores y usuarios y la rentabilidad.

### A esto lo llamamos SASE unificado. Y para llegar al SASE de forma más sencilla y rentable, este es el camino a seguir.

En esta guía aprenderás todo lo que necesitas saber sobre el SASE unificado, incluyendo:

- ¿Qué es SASE unificado?
- Las ventajas del SASE de proveedor único para la empresa actual
- Un potente SASE unificado con HPE Aruba Networking
- Inicio del proceso de adopción de SASE

Al final de esta guía, tendrás una noción clara de cómo SASE unificado puede ayudarte a alcanzar tus objetivos de seguridad de forma más rápida y eficaz.

<sup>1</sup> Análisis de previsión: Empleados cualificados, estilos de trabajo híbrido, enteramente a distancia y presencial, a nivel mundial, Gartner, enero de 2023

<sup>2</sup> Informe de Ponemon Institute, 2023

<sup>3</sup> Guía de mercado del SASE de proveedor único, Gartner, septiembre de 2022





## Las fuerzas motrices de la adopción del SASE

Lo primero es lo primero: ¿por qué adoptar el SASE? La respuesta puede resumirse en 3 simples enunciados:

1. **La seguridad** que solía ser efectiva ya no lo es.
2. **Redes** que solían ser gestionables, ya no lo son.
3. **Soluciones** que solían funcionar bien, ya no funcionan.

Las arquitecturas de redes y seguridad tradicionales que se basaban principalmente en una conectividad perimetral segura ya no cubren las necesidades del entorno empresarial actual. La rápida adopción de servicios en la nube, dispositivos móviles, IoT, OT y trabajo a distancia/híbrido ha creado una fuerza de trabajo distribuida y dinámica que necesita un acceso seguro y fiable a aplicaciones y datos en cualquier lugar, en cualquier momento y en cualquier dispositivo.

No obstante, aunque las necesidades empresariales han evolucionado, el aprovechamiento de soluciones de seguridad de red tradicionales expone a las organizaciones a nuevos retos y riesgos de conectividad, como:

- **Mayor superficie de ataque y complejidad:** ahora que cada vez hay más usuarios, dispositivos, ubicaciones y servicios de nube que proteger, la organización se encuentra con más vías de entrada potenciales para los cibercriminales y con muchas más herramientas de seguridad que administrar y actualizar. Eso sin mencionar que cada vía de entrada (por ejemplo, un usuario o un dispositivo) tiene acceso directo a la red informática de la empresa, lo que aumenta aún más el riesgo.
- **Una experiencia de usuario deficiente y una productividad baja:** con cada vez más tráfico redireccionado a través de VPN y la red corporativa, los usuarios experimentan aumento de la latencia, fluctuaciones, pérdida de paquetes y limitaciones del ancho de banda que afectan a su rendimiento y productividad, eso sin mencionar su satisfacción.
- **Altos costes operativos e ineficiencias:** con la proliferación de soluciones de red y seguridad para implementar, mantener, actualizar y solucionar problemas, la organización se ve obligada a gastar más recursos y tiempo en la gestión de la infraestructura y la resolución de incidencias.

Afrontar estos retos y riesgos puede parecer abrumador. No obstante, trabajando juntos, los responsables de redes y seguridad pueden desterrar estos problemas recurriendo a un marco SASE.

### ¿Qué es SASE?

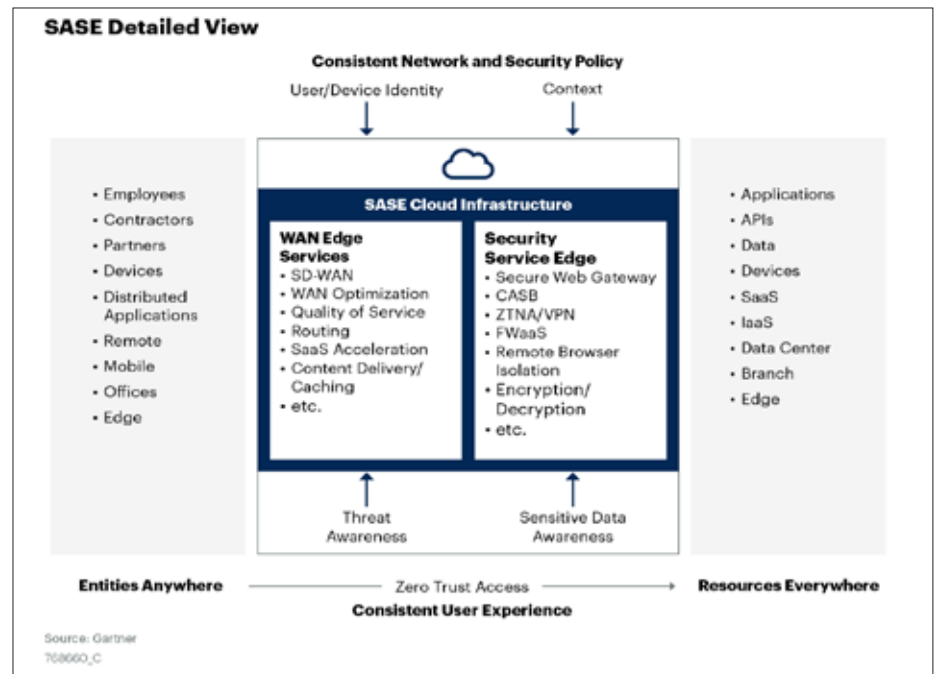
El extremo para servicios de acceso seguro, o SASE por sus siglas en inglés, es un concepto del ámbito de la ciberseguridad que se introdujo por primera vez en 2019. SASE es un marco informático que combina funciones de red y seguridad en una única plataforma que conecta de forma segura a todos los usuarios, dispositivos y aplicaciones de una plantilla distribuida por todo el mundo.

SASE se compone de dos “paquetes de tecnologías” que incluyen servicios de extremo WAN (SD-WAN) y Security Service Edge (ZTNA, SWG, CASB y DEM) que, en conjunto, permiten que los equipos de redes y seguridad por igual hagan posible que cualquier usuario, dispositivo o servidor se conecte de forma segura desde cualquier lugar a través de cualquier método de transferencia. Aprovechar una amplia estructura SD-WAN y SSE en la nube con una red global de PoP permite un acceso rápido del extremo a la nube, lo que reduce la latencia y mejora el rendimiento.



## Los elementos del SASE

Hay dos paquetes de tecnologías centrales que conforman una oferta de SASE unificado de proveedor único:



**Figura 1.** Extremo para servicios de acceso seguro: vista detallada, guía de mercado del SASE de proveedor único<sup>4</sup>

## Servicios de extremo WAN (SD-WAN seguro)

- **Seguridad:** las SD-WAN seguras incluyen funcionalidades de cortafuegos de nueva generación (ngfw), como IDS/IPS y segmentación granular, lo que permite a las organizaciones sustituir los cortafuegos de sucursal y proteger los dispositivos IoT. Además, todas las conexiones están cifradas a través de la estructura SD-WAN.
- **Conectividad de red multinube:** las instancias virtuales de las soluciones SD-WAN pueden desplegarse en proveedores de servicios en la nube como AWS, MS Azure y Google Cloud, lo que establece una conexión resiliente de la sucursal a la nube. SD-WAN también dirige de forma inteligente el tráfico de las aplicaciones a la nube para evitar el tráfico de retorno al centro de datos, y se adapta dinámicamente a los cambios en los patrones de tráfico.
- **Control dinámico de rutas:** SD-WAN combina múltiples enlaces de tráfico, como MPLS, Internet de banda ancha, 4G/5G o enlaces por satélite. Selecciona dinámicamente los mejores enlaces en función de las condiciones de la red y el propósito empresarial.
- **Acondicionamiento de rutas:** las soluciones SD-WAN también utilizan técnicas como el acondicionamiento de rutas para superar los efectos adversos de paquetes caídos y fuera de servicio, habituales en las conexiones a Internet de banda ancha y MPLS. Esto proporciona un rendimiento similar al de una línea privada a través de enlaces de Internet, lo que permite a las organizaciones reducir la dependencia de MPLS y poner en marcha rápidamente nuevas sucursales.
- **Control dinámico de rutas:** esta función acelera la transmisión de datos a través de la WAN, aplicando la aceleración del protocolo TCP así como algoritmos de deduplicación y compresión de datos.
- **Organización centralizada:** las políticas empresariales y de seguridad se gestionan de forma centralizada desde una única interfaz. Esto simplifica las operaciones de red y la resolución de problemas, ya que los administradores pueden realizar cambios y aplicar políticas desde una ubicación central.

<sup>4</sup> Guía de mercado del SASE de proveedor único, Gartner, septiembre de 2022

## Security Service Edge (SSE)

### **Acceso de red de confianza cero (ZTNA, por sus siglas en inglés) | Acceso seguro a aplicaciones privadas**

- La tecnología ZTNA proporciona acceso granular de confianza cero basado en la identidad a aplicaciones y recursos privados, sin importar dónde estén alojados o dónde se encuentren los usuarios. Las soluciones ZTNA actuales permiten a los equipos eliminar por completo las VPN de acceso remoto para empleados y terceros usuarios, lo que reduce significativamente la superficie de ataque al permitir el acceso a aplicaciones privadas específicas con autorización sin ampliar el acceso a la red subyacente.

### **Puerta de enlace web segura (SWG, por sus siglas en inglés) | Acceso seguro a Internet**

- SWG protege la empresa distribuida contra ataques sofisticados, con funciones como el filtrado web, la inspección SSL y la detección y prevención de malware. SWG garantiza a los usuarios autorizados un acceso rápido y seguro a los recursos de Internet, al tiempo que protege a la empresa de posibles daños.

### **Agente de seguridad de acceso a la nube (CASB, por sus siglas en inglés) | Acceso seguro a aplicaciones SaaS**

- CASB facilita la identificación, gestión y control informáticos del uso de los servicios de nube. Un servicio CASB media en las conexiones entre los usuarios y las aplicaciones SaaS basadas en la nube y ayuda a regular el flujo de datos, evita la pérdida y descubre la TI en la sombra para garantizar que los datos confidenciales permanezcan protegidos.

### **Supervisión de la experiencia digital (DEM, por sus siglas en inglés) | Mejora de la experiencia digital y la productividad**

- DEM proporciona visibilidad y análisis optimizados y en línea de las interacciones, la experiencia y el rendimiento de los dispositivos, las aplicaciones y las redes. DEM ayuda al personal de TI a aprovechar mejor su tiempo acelerando la resolución de problemas, lo que permite diagnosticar con precisión los problemas de su experiencia.

## ¿Qué es SASE unificado?

El SASE unificado combina los dos paquetes tecnológicos (SD-WAN y SSE) en una solución de proveedor único que permite a las empresas alcanzar una simplicidad, eficiencia operativa y ahorros de costes aún mayores. Un enfoque unificado también permite una mayor agilidad y una implantación más rápida, lo que mejora el tiempo de obtención de beneficios. Gartner predice que “en 2025, el 50 % de las nuevas adquisiciones de SD-WAN formarán parte de una oferta de SASE de proveedor único, frente al 10 % en 2022.”<sup>5</sup>

## Las ventajas del SASE de proveedor único para la empresa actual

El SASE unificado ofrece a las organizaciones las numerosas ventajas del SASE, al tiempo que simplifica y rentabiliza su adopción. Lo consigue de la siguiente manera:

- **Unificación y mejora de la estrategia de seguridad:** el SASE unificado reduce la superficie de ataque y mejora la detección de amenazas y los tiempos de respuesta aplicando políticas de seguridad universales y controles de acceso centralizados en todo el tráfico y todas las ubicaciones.
- **Mejora de la eficiencia de los equipos de redes y seguridad:** disponer de un SASE de proveedor único no solo mejora la consolidación, sino que también unifica las funciones de red y seguridad. Esto reduce los obstáculos entre los diferentes equipos y minimiza las complejidades y los costes, al tiempo que optimiza la colaboración y la implementación interfuncional. Las operaciones de red y seguridad se agilizan proporcionando un sistema de gestión centralizado que facilita la visibilidad, la configuración, la supervisión y la solución de problemas.

<sup>5</sup> Guía de mercado del SASE de proveedor único, Gartner, septiembre de 2022



- **Ofrecer una mejor experiencia al usuario y al administrador:** el SASE unificado permite a los equipos garantizar una conectividad de alto rendimiento y baja latencia para los usuarios de las aplicaciones mediante el enrutamiento automático del tráfico a través de las rutas de acceso más rápidas y evitando el retorno del tráfico al centro de datos. Los usuarios finales disfrutan de una experiencia de acceso optimizada, mientras que los administradores obtienen controles de acceso sencillos pero granulares aplicados a través de políticas universales de confianza cero.
- **Reducción de costes y aumento de la flexibilidad:** con SASE se reduce el desembolso de capital (CAPEX) y los gastos operativos (OpEx) al eliminar la necesidad de múltiples soluciones puntuales y dispositivos de hardware. El SASE unificado también tiene una alta capacidad de escalado, al adaptarse rápidamente a las cambiantes necesidades empresariales, y proporciona múltiples puntos de presencia para organizaciones con gran distribución geográfica.

## Cómo empezar a desplegar el SASE unificado

La implantación de una solución SASE de proveedor único puede parecer desalentadora, pero no tiene por qué serlo. Con el socio adecuado y una hoja de ruta clara, las organizaciones pueden hacer la transición a SASE sin problemas y de forma segura, sin interrumpir sus operaciones actuales ni comprometer su rendimiento.

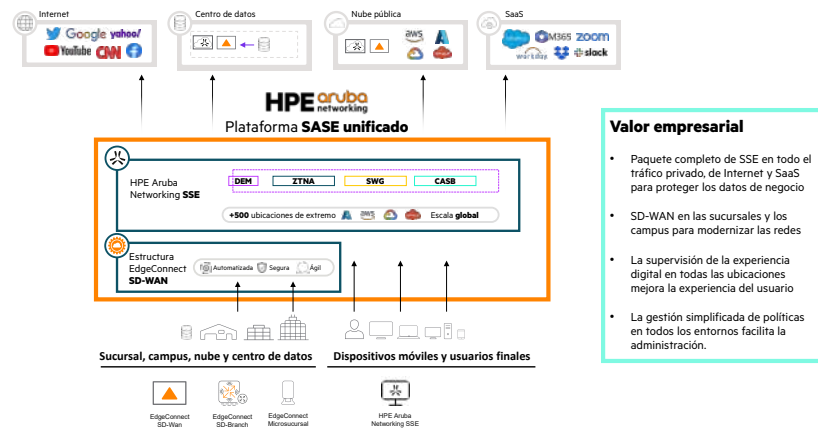
Hay cinco pasos básicos que se siguen en la mayoría de las implantaciones de SASE satisfactorias:

- **Paso 1: define tus objetivos y requisitos de SASE.** Identifica tus objetivos empresariales, casos de uso y requisitos de SASE. Evalúa tus redes y arquitectura de seguridad actuales. Detecta las lagunas, los retos y los recursos existentes.
- **Paso 2: elige un proveedor único de SASE.** Compara diferentes proveedores en función de sus capacidades, cobertura, rendimiento, escalabilidad, fiabilidad, asistencia y precios. Busca una solución SASE de proveedor único bien diseñada, integrada, unificada, flexible y fácil de usar.
- **Paso 3: diseña y desarrolla tu plan de juego SASE.** Trabaja con tu proveedor para definir la topología de tu red, las políticas de seguridad, los grupos de usuarios, los perfiles de las aplicaciones y las opciones de conectividad con base en las mejores prácticas. Este debe ser un proceso de colaboración con tu proveedor de SASE para garantizar el mayor éxito para tu empresa.
- **Paso 4: inicia el despliegue de SASE con un enfoque gradual.** Implementa los componentes necesarios, como agentes, conectores, dispositivos SD-WAN o PoP privados a través de una consola de gestión centralizada. Migra tus usuarios, dispositivos, ubicaciones y aplicaciones a tu solución SASE de forma gradual o por lotes. SASE puede trabajar en tándem con las soluciones existentes, permitiendo que el despliegue sea tan rápido o lento como tu equipo necesite.
- **Paso 5: sácale el máximo partido a SASE.** A medida que continúa el despliegue, utiliza las herramientas y los paneles de control de tu proveedor para obtener visibilidad, información y comentarios que te permitan optimizar aún más tu solución SASE. Aprovecha al máximo tu inversión y descubre nuevos casos de uso y funcionalidades en los que SASE puede aportar más beneficios a tu negocio.





## Un potente SASE unificado con HPE Aruba Networking



**Figura 3.** Plataforma SASE unificada de HPE Aruba Networking

Si buscas una solución SASE de proveedor único potente que ofrezca acceso empresarial seguro y fiable desde cualquier lugar, HPE Aruba Networking SASE puede ser tu respuesta. Con su SD-WAN líder del sector y su galardonado SSE, HPE Aruba Networking ofrece un enfoque integral y unificado de SASE diseñado para la empresa distribuida y dinámica de hoy en día.

Con las crecientes demandas de integración entre las soluciones de red y las de seguridad, HPE Aruba Networking ayuda al personal de TI a consolidar, simplificar y proteger la conectividad de tu empresa. Con HPE Aruba Networking, el personal de TI puede proporcionar controles de seguridad de WAN y de la nube directamente a la aplicación en el extremo de la red con HPE Aruba Networking EdgeConnect SD-WAN, en lugar de enrutar los datos a través del centro de datos, mientras que SSE garantiza que los controles de seguridad de confianza cero se puedan aplicar a todas las personas y dispositivos, sin importar dónde se conecten: en el campus, en la sucursal, en casa o de viaje.

### Inicio del proceso de adopción de SASE

**“En los próximos 12 meses, el 46 % de las organizaciones habrá implementado una arquitectura SASE”.**

- Informe de Ponemon Institute, 2023<sup>4</sup>

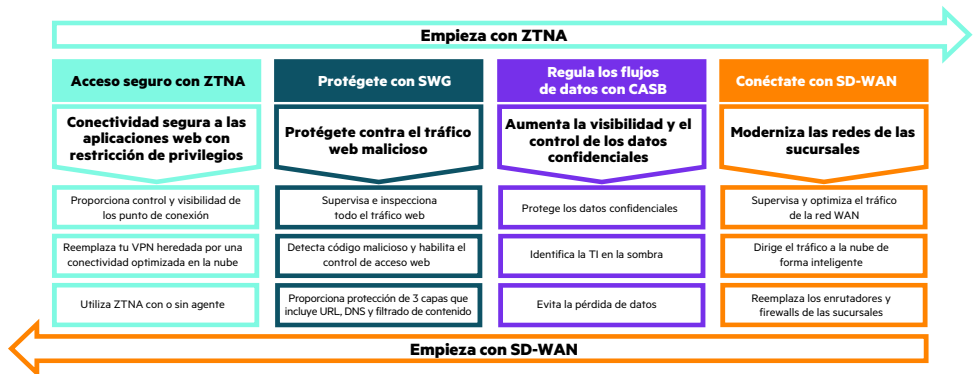
SASE no es solo una moda tecnológica pasajera; es un imperativo estratégico para las empresas modernas que quieren prosperar en la era digital. SASE puede ayudar a las organizaciones a superar los retos y riesgos de las arquitecturas de red y seguridad que se centran principalmente en el control de la red, y lograr una mejor posición de seguridad, experiencia de usuario, eficiencia operativa y ahorro de costes.

Y con SASE unificado, suministrado por un único proveedor de SASE que cumpla tus objetivos y requisitos, puedes conseguirlo aún más rápido.

Si el SASE unificado te parece adecuado para tu organización, solo te queda una pregunta: ¿por dónde quieres empezar tu implementación? Estas son las dos vías más comunes que siguen las organizaciones.

<sup>4</sup> Informe de Ponemon Institute, 2023





### Opción 1: empezar con SSE (específicamente ZTNA)

El informe de adopción de SSE de 2023 desveló que el 67 % de las empresas tiene pensando empezar a adoptar SASE con la tecnología SSE. Si este es el caso de tu organización, considera la opción de reemplazar tu VPN por HPE Aruba Networking ZTNA para proporcionar acceso de confianza cero a tus aplicaciones privadas, ya sea en el centro de datos, en la nube o en cualquier ubicación intermedia.

[Más información sobre HPE Aruba Networking SSE](#)

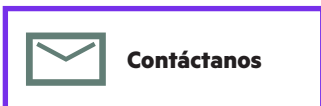
### Opción 2: empezar con SD-WAN

Empieza tu proceso de adopción de SASE por SD-WAN. Completa tu portfolio del extremo seguro (oficina pequeña/oficina doméstica, sucursal, campus o WAN) con una única estructura SD-WAN con tecnología HPE Aruba Networking EdgeConnect.

[Más información sobre HPE Aruba Networking EdgeConnect](#)

Chatea con un experto en [www.arubanetworks.com/es/compania/pongase-en-contacto-con-nosotros/formulario-de-contacto/](http://www.arubanetworks.com/es/compania/pongase-en-contacto-con-nosotros/formulario-de-contacto/)

Toma la decisión de compra correcta. Contacta con nuestros especialistas en preventa.



© Copyright 2023 Hewlett Packard Enterprise Development LP. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise quedan establecidas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. Ninguna de las declaraciones anteriores debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabilizará de los errores u omisiones técnicos o editoriales que pudiera contener el presente documento.

GARTNER es una marca comercial registrada y marca de servicio de Gartner, Inc. y/o sus afiliados en EE. UU. y a nivel internacional, y se utiliza en este documento con su permiso. Todos los derechos reservados.

BR\_UnifiedSASE\_RVK\_081023 a00133570ese