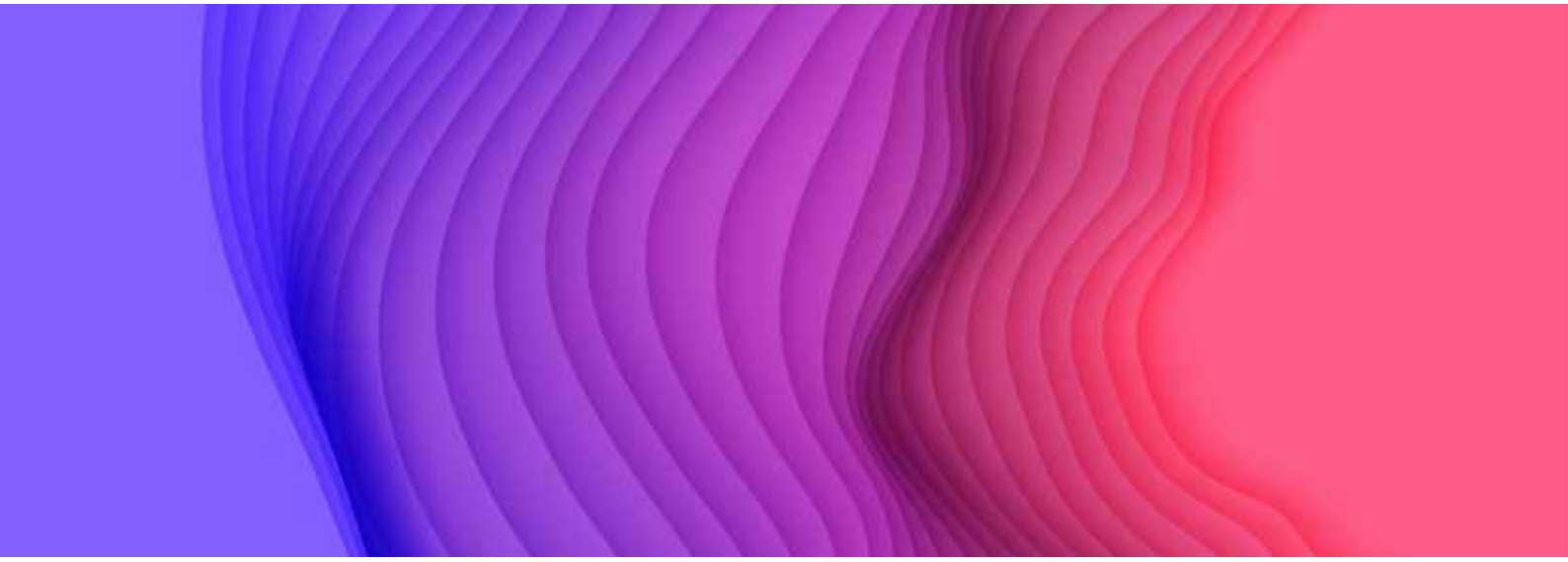
Folleto

Guía introductoria a SASE unificado

Para obtener SASE de forma más simple y económica

HPE aruba networking



48 %

"Para fines de 2023, el 48 % de los trabajadores del conocimiento trabajará de forma híbrida y completamente remota, frente al 27 % de 2019. De estos trabajadores, un 39 % lo hará de forma híbrida, frente al 12 % de 2020"[1], lo que aumenta la demanda de soluciones SASE.

46 %

"En los próximos 12 meses, el 46 % de las organizaciones habrá implementado una arquitectura de SASE".[2]

65 %

"Para 2025, el 65 % de las empresas habrá consolidado componentes SASE individuales en uno o dos proveedores SASE explícitamente asociados".[3]

[1] Forecast Analysis: Knowledge Employees, Hybrid, Fully Remote and On-Site Work Styles, Worldwide, Gartner, enero de 2023

[2] Informe de Ponemon Institute de 2023

[3] Gartner Market Guide for Single-Vendor SASE, Gartner, septiembre de 2022

El crecimiento de SASE unificado: un proceso más simple y económico para obtener SASE

Durante el último año, muchos líderes de TI adoptaron un marco de borde de servicio de acceso seguro (SASE) para permitir una conectividad más rápida y segura en todas sus organizaciones globales. SASE converge las funciones de soluciones de red y seguridad en un servicio único nativo en la nube que brinda conectividad consistente y seguridad desde cualquier lugar.

SASE no es solo una tendencia tecnológica. Es un imperativo estratégico para empresas modernas que buscan progresar en la era digital.

Sin embargo, no todas las soluciones SASE se crean de la misma forma. Algunos proveedores SASE ofrecen soluciones de múltiples puntos y poca integración, o requieren enrutamiento entre los diferentes puntos de presencia de proveedores, que pueden introducir latencia, problemas en el rendimiento y gastos generales de gestión.

Entonces, existen soluciones SASE que brindan todas las capacidades principales de SASE en una plataforma única y totalmente integrada, que mejora la seguridad, la eficacia del personal, las experiencias del usuario y el personal de administración, y el costo.

Esto es lo que llamamos SASE unificado. Y, para lograr una forma más simple y económica de obtener SASE, esta es la forma de hacerlo.

En esta guía, obtendrás todo lo que necesita saber sobre SASE unificado, incluido lo siguiente:

- ¿Qué es el SASE unificado?
- Los beneficios de SASE de proveedor único para empresas modernas
- Un potente SASE unificado con HPE Aruba Networking
- El inicio del proceso de SASE

Al final de esta guía, entenderás bien cómo SASE unificado puede ayudarlo a cumplir con tus objetivos de seguridad de manera más rápida y eficiente.

Las fuerzas impulsoras detrás de la adopción de SASE

Primero, lo primero: ¿por qué deberíamos adoptar SASE? Podemos resumir la respuesta en tres simples afirmaciones:

1. **La seguridad** que alguna vez fue efectiva ya no lo es.
2. **Las redes** que alguna vez pudieron gestionarse ya no se pueden.
3. **Las soluciones** que alguna vez funcionaron bien ya no lo hacen.

Las tradicionales arquitecturas de red y seguridad que dependían principalmente de conectividad segura basada en el perímetro ya no cumplen con las necesidades del entorno empresarial moderno. La rápida adopción de servicios de nube, dispositivos móviles, Internet de las cosas, OT y trabajo remoto/híbrido creó una fuerza de trabajo distribuida y dinámica que necesita acceso seguro y confiable a aplicaciones y datos desde cualquier lugar, en cualquier momento y con cualquier dispositivo.

Sin embargo, aunque las empresas necesitan evolucionar, la utilización de soluciones tradicionales de seguridad en la red expone a las organizaciones a nuevos desafíos y riesgos de conectividad, como los que se mencionan a continuación:

- **Mayor superficie y complejidad de los ataques:** con más usuarios, dispositivos, ubicaciones y servicios de nube que se deben proteger, la organización debe hacer frente a más posibles puntos de entrada para los atacantes y más herramientas de seguridad que se deben gestionar y actualizar. Por no hablar de que cada punto de entrada (es decir, usuario o dispositivo) tiene acceso directo a la red corporativa, lo que aumenta los riesgos.
- **Mala experiencia del usuario y menor productividad:** con más tráfico en backhaul a través de la VPN y la red corporativa, los usuarios experimentan un aumento de latencia, irregularidades, pérdida de paquetes y limitaciones de ancho de banda que afectan su rendimiento y productividad, por no hablar de la satisfacción.
- **Altos costos operativos e ineficiencias:** con la proliferación de soluciones, tanto de red como de seguridad, que se deben desplegar, mantener, actualizar y solucionar, la organización debe dedicar más recursos y tiempo a la gestión de la infraestructura y la solución de problemas.

Abordar estos desafíos y riesgos puede resultar abrumador. Sin embargo, al trabajar en conjunto, los líderes de redes y seguridad pueden erradicar estos problemas si utilizan un marco de SASE.

¿Qué es SASE?

El borde de servicio de acceso seguro, o SASE, es un concepto de ciberseguridad que se introdujo por primera vez en 2019. SASE es un marco de TI que combina funciones de redes y seguridad en una plataforma única que conecta, de forma segura, todos los usuarios, dispositivos y aplicaciones en la fuerza de trabajo globalmente distribuida.

SASE está compuesto por dos "conjuntos de tecnología", incluidos los servicios de borde de WAN (SD-WAN) y el borde de servicio de seguridad (ZTNA, SWG, CASB y DEM), que juntos posibilitan a equipos de red y seguridad similares permitir que cualquier usuario, dispositivo o servidor se conecte de forma segura desde cualquier lugar a través de cualquier método de transporte. Aprovechar una vasta estructura SD-WAN y SSE en la nube con una red global de puntos de presencia permite el rápido acceso desde el borde hasta la nube, lo que reduce la latencia y mejora el rendimiento.

Los elementos de SASE

Existen dos conjuntos básicos de tecnología que conforman la oferta de SASE unificado y de proveedor único:

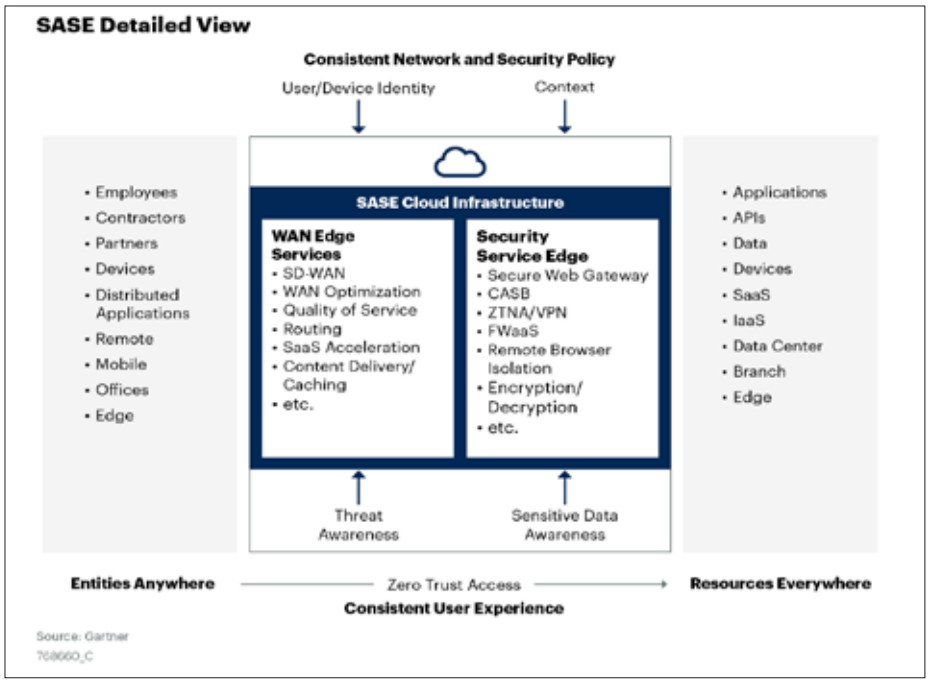


Figura 1. Borde de servicio de acceso seguro: vista detallada, Market Guide for Single-Vendor SASE[4]

WAN Edge Services (SD-WAN segura)

- **Seguridad**: las SD-WAN seguras incluyen capacidades de firewall de próxima generación, como IDS/IPS y segmentación granular, lo que permite a las organizaciones reemplazar firewalls de sucursales y proteger dispositivos de Internet de las Cosas. Además, todas las conexiones se encuentran cifradas en la estructura SD-WAN.
- **Redes multinube:** las instancias virtuales de las soluciones SD-WAN se pueden implementar en proveedores de servicios de nube como AWS, MS Azure y Google Cloud, lo que establece una conexión resistente desde la sucursal a la nube. SD-WAN también dirige de manera inteligente el tráfico de 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 ruta:** SD-WAN combina múltiples enlaces de transporte, como MPLS, Internet de banda ancha, 4G/5G o enlaces satelitales. Selecciona los mejores enlaces de manera dinámica en función de las condiciones de la red y el propósito comercial.
- **Condicionamiento de ruta:** las soluciones SD-WAN también utilizan técnicas como el condicionamiento de ruta para superar los efectos adversos de los paquetes de datos que se cortan o están desorganizados, y que son comunes con las conexiones de Internet de banda ancha y MPLS. Esto proporciona rendimiento similar al de una línea privada mediante enlaces de Internet, lo que permite a las organizaciones reducir la dependencia de MPLS y abrir nuevas sucursales con rapidez.
- **Control dinámico de ruta:** esta función acelera la transmisión de datos a través de la WAN, ya que aplica la aceleración del protocolo TCP, así como algoritmos de deduplicación y compresión de datos.
- **Organización centralizada:** las políticas comerciales y de seguridad se gestionan de forma centralizada desde una única interfaz. Esto simplifica las operaciones de red y la solución de problemas, ya que los administradores pueden realizar cambios y aplicar políticas desde una ubicación central.

[4] Gartner Market Guide for Single-Vendor SASE, Gartner, septiembre de 2022

Borde de servicio de seguridad (SSE)

Acceso a la red conforme a Zero Trust (ZTNA) | Acceso seguro a aplicaciones privadas

- La tecnología ZTNA brinda acceso Zero Trust granular y basado en la identidad a aplicaciones y recursos privados, independientemente de dónde estén alojados o dónde se encuentren los usuarios. Las soluciones modernas de ZTNA permiten que los equipos eliminen por completo las redes privadas virtuales (VPN) de acceso remoto para empleados y usuarios independientes, lo que reduce la superficie de ataque de manera significativa ya que permite el acceso a aplicaciones privadas autorizadas específicas sin ampliar el acceso a la red subyacente.

Gateway web segura (SWG) | Acceso seguro a Internet

- La SWG protege a las empresas distribuidas contra ataques avanzados gracias a capacidades tales como filtrado web, inspección de la seguridad de la capa de transporte (SSL), y detección y prevención de malware. La SWG garantiza que los usuarios autorizados obtengan acceso rápido y seguro a los recursos de Internet, al mismo tiempo que protege la empresa de cualquier daño.

Agente de seguridad de acceso a la nube (CASB) | Acceso seguro a aplicaciones SaaS

- El agente de seguridad de acceso a la nube permite que el departamento de TI identifique, gestione y controle el uso de servicios de nube. Un servicio de CASB media en las conexiones entre los usuarios y las aplicaciones SaaS basadas en la nube. Además, ayuda a regular el flujo de datos, previene la pérdida de datos y descubre TI en la sombra con el propósito de garantizar que los datos confidenciales permanezcan protegidos.

Monitoreo de experiencia digital (DEM) | Experiencia y productividad digital mejoradas

- El DEM brinda visibilidad y análisis en línea mejorados de las interacciones, la experiencia y el rendimiento de los dispositivos, las aplicaciones y las redes. También ayuda a los equipos de TI a utilizar mejor su tiempo, ya que acelera la solución de problemas y permite diagnosticar los problemas con precisión.

¿Qué es el SASE unificado?

SASE unificado combina los dos conjuntos de tecnología, SD-WAN y SSE, en una solución de proveedor único que permite a las empresas lograr mayor simplicidad, eficiencia operativa y ahorro de costos. Un enfoque unificado también permite lograr mayor agilidad y una implementación más rápida, lo que acelera la obtención de beneficios. Gartner predice que "para 2025, el 50 % de las nuevas compras de SD-WAN serán parte de una oferta SASE de proveedor único, frente al 10 % de 2022".[5]

Los beneficios de SASE de proveedor único para empresas modernas

SASE unificado ofrece a las organizaciones los muchos beneficios de SASE, al mismo tiempo que hace que la adopción sea más sencilla y rentable. Puede lograrlo al llevar a cabo lo siguiente:

- **Unificar y mejorar la postura de seguridad:** SASE unificado reduce la superficie de ataque, y mejora la detección de amenazas y los tiempos de respuesta mediante la aplicación de políticas de seguridad universales y controles de acceso centralizados en todo el tráfico y las ubicaciones.
- **Mejorar la eficiencia de los equipos de redes y seguridad:** contar con SASE de proveedor único no solo brinda consolidación, sino que también unifica las funciones de red y seguridad. Esto permite que se alivien los obstáculos entre los equipos. Además, minimiza las complejidades y el costo, mientras optimiza la colaboración e implementaciones multifuncional. Las operaciones de red y seguridad se optimizan al proporcionar un sistema de gestión centralizado para visibilidad, configuración, monitoreo y solución de problemas.

[5] Gartner Market Guide for Single-Vendor SASE, Gartner, septiembre de 2022

- **Ofrecer mejor experiencia de usuario y administrador:** SASE unificado permite que los equipos garanticen a los usuarios conectividad de baja latencia y alto rendimiento de las aplicaciones mediante el enrutamiento automático del tráfico a través de las rutas de acceso más rápidas y evitando el tráfico de retorno al centro de datos. Los usuarios finales obtienen una experiencia de acceso optimizada, mientras que los administradores obtienen controles de acceso simples, pero granulares aplicados a través de políticas universales de Zero Trust.
- **Menos costos y mayor flexibilidad:** SASE reduce los gastos de capital (CapEx) y los gastos operativos (OpEx) ya que no requiere soluciones de múltiples puntos y dispositivos de hardware. SASE unificado también es altamente escalable, se adapta rápidamente a las cambiantes necesidades comerciales y proporciona múltiples puntos de presencia para organizaciones distribuidas geográficamente.

Cómo comenzar a implementar SASE unificado

La implementación de una solución SASE de proveedor único puede parecer desalentadora, pero no tiene por qué serlo. Con el socio adecuado y un plan de acción claro, las organizaciones pueden hacer la transición a SASE sin problemas y de forma segura, sin interrumpir sus operaciones existentes ni comprometer su rendimiento.

Hay cinco pasos básicos que siguen las implementaciones de SASE más exitosas:

- **Paso 1: Define tus objetivos y requisitos de SASE.** Identifica tus objetivos comerciales, casos de uso y requisitos de SASE. Evalúa tu arquitectura actual de red y seguridad. Encuentra las brechas, los desafíos y los recursos existentes.
- **Paso 2: Elige un proveedor SASE de proveedor único.** Compara los diferentes proveedores en función de sus capacidades, cobertura, rendimiento, escalabilidad, confiabilidad, soporte y precios. Busca una solución SASE de proveedor único y bien diseñada que sea integrada, unificada, flexible y fácil de usar.
- **Paso 3: Diseña y desarrolla tu plan de juego de SASE.** Trabaja con tu proveedor para definir la topología de tu red, las políticas de seguridad, los grupos de usuarios, los perfiles de aplicación y las opciones de conectividad según 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: Comienza la implementación de SASE con un enfoque por etapas.** Implementa los componentes necesarios, como agentes, conectores, dispositivos SD-WAN o puntos de presencia privados mediante una consola de gestión centralizada. Migra usuarios, dispositivos, ubicaciones y aplicaciones a tu solución SASE en un enfoque por etapas o por lotes. SASE puede funcionar en conjunto con las soluciones existentes, lo que permite que la implementación sea rápida o lenta según las necesidades de tu equipo.
- **Paso 5: Aprovecha SASE al máximo.** A medida que continúe la implementación, usa las herramientas y los paneles de tu proveedor para obtener visibilidad, información y comentarios para optimizar aún más tu solución SASE. Aprovecha tu inversión al máximo, y descubre nuevos casos de uso y funcionalidad donde SASE puede beneficiar aún más a tu empresa.

Un potente SASE unificado con HPE Aruba Networking

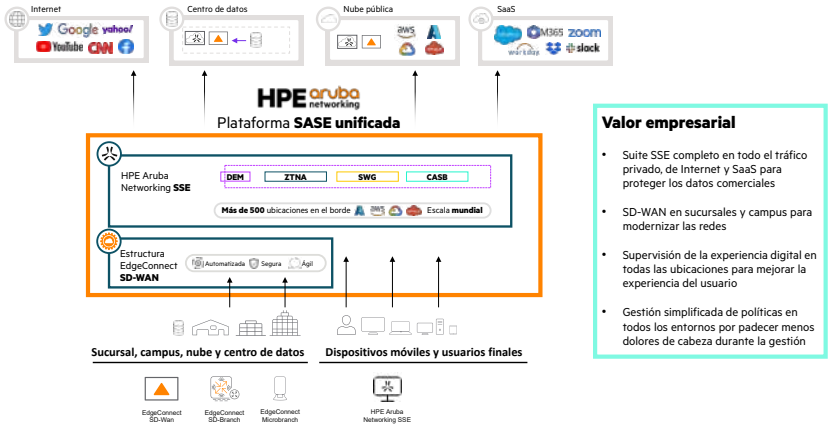


Figura 3. Plataforma de SASE unificado de HPE Aruba Networking

Si estás buscando una solución SASE potente de proveedor único que brinde acceso empresarial seguro y confiable desde cualquier lugar, HPE Aruba Networking SASE puede ser la respuesta que estabas buscando. Con su SD-WAN líder del sector y SSE galardonado, HPE Aruba Networking ofrece un enfoque integral y unificado de SASE que se diseñó para la empresa distribuida y dinámica de la actualidad.

Con las crecientes demandas de integración entre las soluciones de redes y seguridad, HPE Aruba Networking ayuda a los equipos de TI a consolidar, simplificar y proteger su conectividad empresarial. Con HPE Aruba Networking, los equipos de TI pueden ofrecer controles de seguridad de nube y WAN directamente a la aplicación en el borde de la red con HPE Aruba Networking EdgeConnect SD-WAN, en lugar de enrutar datos mediante el centro de datos, mientras que SSE garantiza que se puedan aplicar los controles de seguridad Zero Trust a todas las personas y todos los dispositivos, sin importar dónde se conecten: en el campus, la sucursal, el hogar o la carretera.

El inicio del proceso de SASE

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

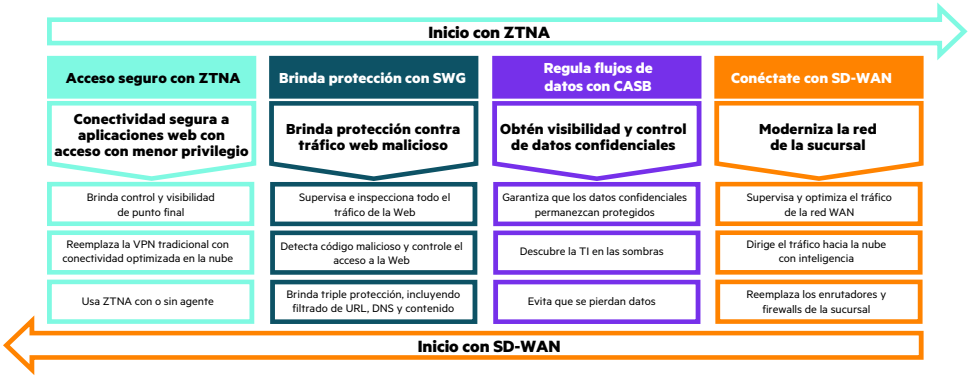
– Informe de Ponemon Institute de 2023[4]

SASE no es solo una tendencia tecnológica pasajera. Es un imperativo estratégico para empresas modernas que buscan progresar en la era digital. SASE puede ayudar a las organizaciones a superar los desafíos y riesgos de las arquitecturas de red y seguridad que se enfocan principalmente en el control de la red y lograr mejor postura de seguridad, experiencia de usuario, eficiencia operativa y ahorros de costos.

Y gracias a SASE unificado, que es brindado por un proveedor único, puedes cumplir tus objetivos y requisitos con mayor rapidez.

Si SASE unificado es una buena idea para tu organización, entonces queda una pregunta más por responder: ¿dónde quieres empezar tu implementación? Estas son las dos rutas más comunes que toman las organizaciones.

[4] Informe de Ponemon Institute de 2023



Ruta 1: Comienza con SSE (específicamente ZTNA)

El informe de adopción de SSE de 2023 determinó que el 67 % de las empresas tienen planificado comenzar su proceso de SASE con tecnología SSE. Si este es tu caso, considera reemplazar la VPN con HPE Aruba Networking ZTNA para brindar acceso Zero Trust a tus aplicaciones privadas, ya sea que se encuentren en el centro de datos, la nube o cualquier otro lugar.

Obtén más información sobre HPE Aruba Networking SSE.

Ruta 2: Comienza con SD-WAN

Empieza tu proceso de SASE mediante la incorporación de SD-WAN. Completa tu portafolio de borde seguro (oficina pequeña/oficina en el hogar, sucursal, campus o WAN) con una estructura SD-WAN simple impulsada por HPE Aruba Networking EdgeConnect.

Obtén más información sobre HPE Aruba Networking EdgeConnect.

Comunícate con una persona experta en www.arubanetworks.com/latam/empresa/contactese-con-nosotros/formulario-de-contacto/

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

Comunícate con nosotros

BR_UnifiedSASE_RVK_081023 a00133570spl