

# Proteger y modernizar las redes del sector de la fabricación con SASE unificado



Las iniciativas de transformación digital que apuntan a mejorar la eficiencia, la productividad, la fiabilidad, la seguridad y la protección física dependen del acceso a los datos de los dispositivos de tecnología operativa (TO) e Internet industrial de las cosas (IIoT), así como a la información contextual como la ubicación y la identidad de las redes de tecnología de la información (TI). Además, la convergencia de TI y TO proporciona un mejor análisis de datos y mejores procesos de toma de decisiones, pero también supone importantes desafíos, especialmente en materia de seguridad.

Conectar y proteger dispositivos y aplicaciones dispares no es tarea fácil. Las empresas distribuidas de hoy en día tienen instalaciones, sitios remotos y personas distribuidas por todas partes. Las cargas de trabajo de las aplicaciones y los datos en tiempo real se pueden procesar localmente en la fábrica, en un centro de datos remoto, en una nube privada y/o en un proveedor de servicios en la nube. Para garantizar la productividad, estas empresas necesitan una arquitectura de red flexible que pueda adaptarse a las necesidades cambiantes con una gestión simplificada y una forma fácil de integrar nuevas ubicaciones y dispositivos en la red.

La seguridad se ha vuelto crucial en la fabricación para proteger la producción, los datos confidenciales, la propiedad intelectual y el IIoT contra las amenazas cibernéticas, pero también para demostrar el cumplimiento de los estándares y regulaciones del sector, como IEC 62443, GDPR e ISO 27000. Y proteger las comunicaciones en una empresa tan distribuida se ha vuelto un desafío con la expansión de la nube, la proliferación del trabajador remoto y la necesidad de una conectividad generalizada y permanente. En este escenario, el perímetro de la red tradicional no está tan definido como solía estar, lo que exige un conjunto de controles diferente o adicional a la arquitectura de protección absoluta de la fabricación.

Teniendo en cuenta los desafíos anteriores, veamos cómo la adopción de una solución SASE (Secure Access Service Edge) avanzada puede ayudar a los clientes industriales y de fabricación a hacer frente a estos desafíos.

# SASE unificado de HPE Aruba Networking para instalaciones de fabricación

SASE es un marco transformador que combina funciones de seguridad de red con capacidades WAN para dar soporte a las necesidades dinámicas impulsadas por la nube de los fabricantes modernos. Los dos componentes clave del SASE unificado de HPE Aruba Networking son HPE Aruba Networking EdgeConnect SD-WAN y HPE Aruba Networking SSE (Security Service Edge). Juntos, estos componentes crean un enfoque holístico de la seguridad y la red, en línea con la naturaleza descentralizada y móvil de las fábricas inteligentes de hoy en día. Además, un enfoque unificado permite una adopción más sencilla y una implementación más rápida, lo que reduce el tiempo de recuperación de la inversión.

Las soluciones EdgeConnect SD-WAN de HPE Aruba Networking están diseñadas para proporcionar acceso seguro y de alta disponibilidad al tráfico de TO, TI e IIoT a través de prácticamente cualquier combinación de enlaces, incluidos MPLS, internet, 4G/5G y comunicaciones vía satélite, lo que mejora el rendimiento de las aplicaciones y aporta flexibilidad para adaptarse a estos entornos dinámicos e incorporar fácilmente nuevas ubicaciones. EdgeConnect SD-WAN también admite redes multinube al direccionar de forma inteligente el tráfico a la nube, lo que elimina la necesidad de redirigir el tráfico de vuelta al centro de datos y optimiza el tráfico basado en la nube. Integra un cortafuegos de última generación para

proporcionar capacidades de seguridad avanzadas en sitios de fabricación, como IDS/IPS, defensa DDoS y segmentación basada en funciones, yendo más allá de la definición típica de SASE para incorporar seguridad de IoT.

HPE Aruba Networking SSE ofrece funcionalidades de seguridad en la nube clave como acceso de red de confianza cero (ZTNA), puerta de enlace web segura (SWG) y agente de seguridad para el acceso a la nube (CASB). ZTNA permite a los usuarios y terceros autorizados acceder a recursos, como trabajadores híbridos y contratistas que deben realizar tareas de mantenimiento remoto. Los empleados están protegidos contra las amenazas web que pueden irrumpir en su entorno de TO con la SWG y los datos confidenciales alojados en aplicaciones SaaS se supervisan de forma segura para evitar la filtración de datos (incluidas las recetas de productos, la documentación de diseño de productos y los datos PII) con un CASB.

La adopción de SASE unificado de HPE Aruba Networking ofrece beneficios tangibles, como una base común de confianza cero que los equipos de redes y seguridad pueden utilizar para impulsar el cumplimiento, la seguridad unificada, la defensa contra amenazas, la protección de datos, el rendimiento mejorado de las aplicaciones, la gestión centralizada y la facilidad de implementación.

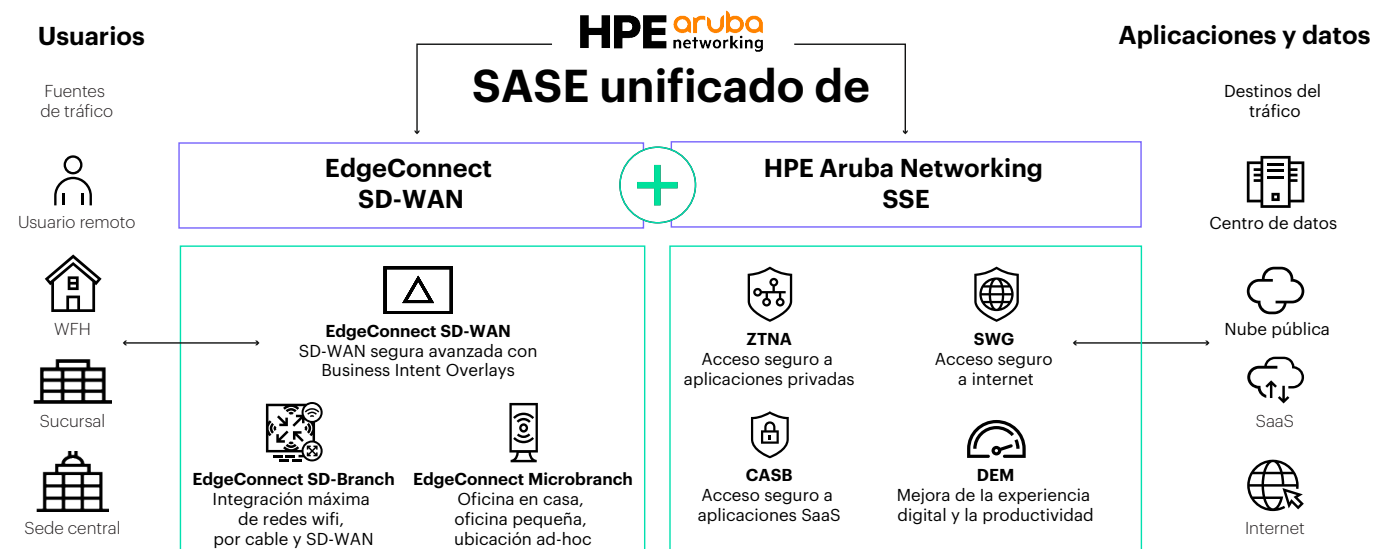


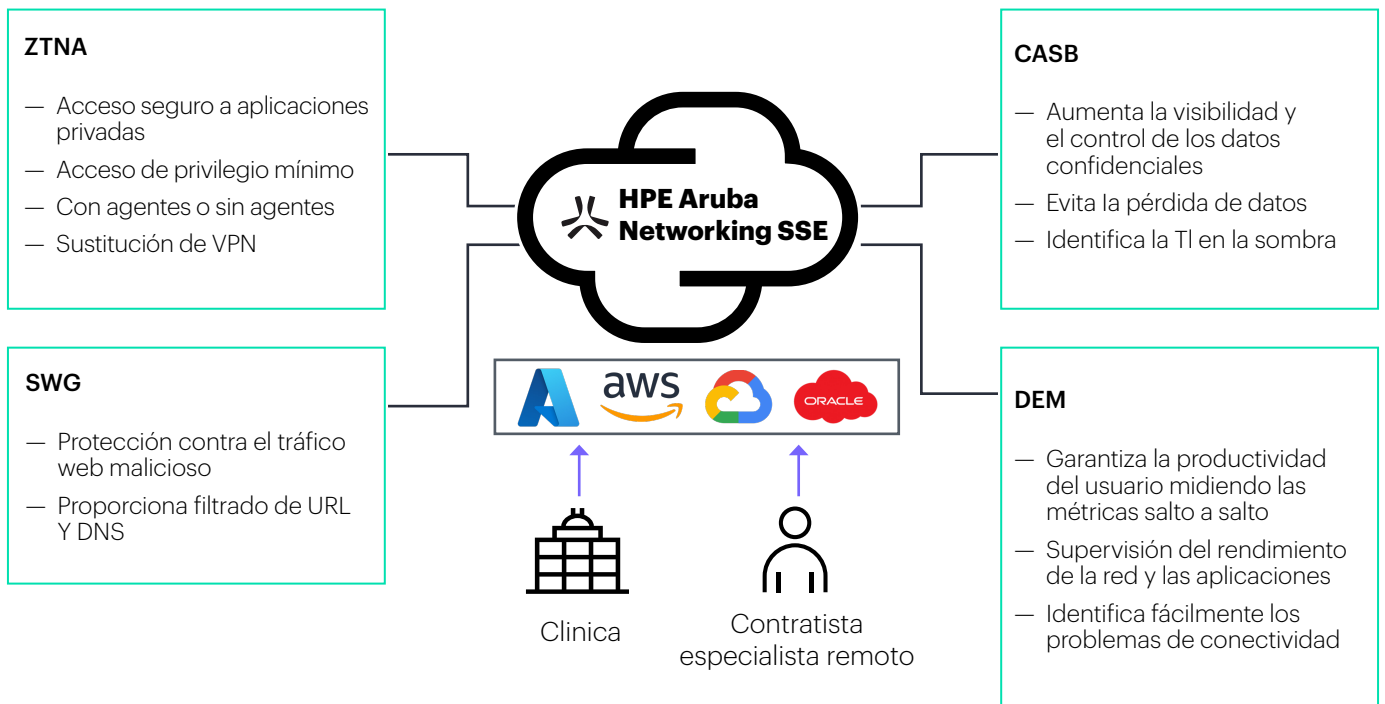
Figura 1. Implementa SASE unificado en la fabricación con HPE Aruba Networking



## Seguridad avanzada

A medida que las fábricas se mueven hacia una arquitectura centrada en la nube, donde muchas aplicaciones en los niveles 3 a 5 del modelo de Purdue se ubican en la nube y aumenta la demanda de un entorno de trabajo híbrido, la seguridad debe evolucionar en paralelo para evitar interrupciones en los servicios y la producción. HPE Aruba Networking SSE integra múltiples funcionalidades de seguridad como ZTNA, SWG y CASB para garantizar una postura de seguridad coherente.

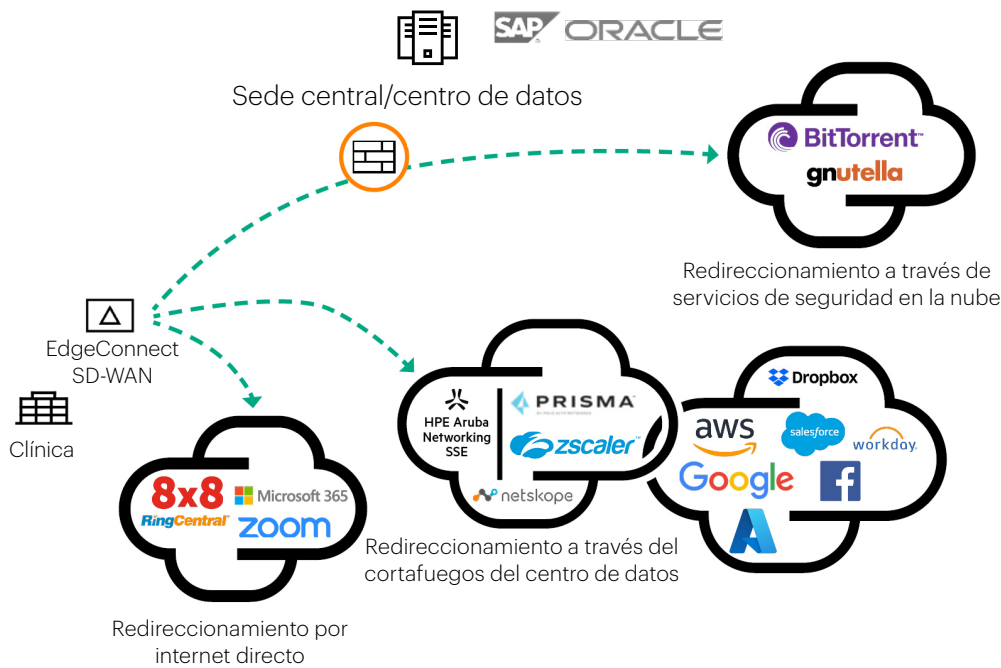
- **ZTNA (acceso a redes de confianza cero)** se basa en el principio de «nunca confiar, siempre verificar», de modo que un sujeto que se conecta a la red no es fiable de forma predeterminada. Permite a las empresas de fabricación reemplazar soluciones VPN heredadas que pueden ser propensas a vulnerabilidades conocidas. Además, las VPN no suelen ofrecer la experiencia que los fabricantes necesitan para realizar operaciones urgentes. Con ZTNA, el acceso de usuario está limitado únicamente a aplicaciones o microsegmentos específicos que hayan sido aprobados para el usuario, lo que impone un acceso con el mínimo privilegio. Con ZTNA, los trabajadores remotos pueden conectarse desde cualquier lugar. Los usuarios de terceros también pueden incorporarse fácilmente a la red con ZTNA sin agente.
- **La SWG (puerta de enlace web segura)** se sitúa entre un usuario y un sitio web para protegerlo contra amenazas maliciosas. Realiza varias inspecciones de seguridad, incluido el filtrado de URL, la detección de códigos maliciosos y el control de acceso a la web, y proporciona políticas que pueden limitar el acceso a sitios para adultos, sitios de apuestas o sitios peligrosos, entre otros. El sector de la fabricación se ha visto gravemente afectado por el ransomware en los últimos años y SWG juega un papel clave para mitigar este riesgo.
- **Un CASB (agente de seguridad para el acceso a la nube)** garantiza que los datos confidenciales alojados en aplicaciones SaaS como ERP y CRM permanezcan protegidos. Identifica y detecta datos confidenciales en aplicaciones en la nube y desvela la TI en la sombra. Supervisa las actividades de los usuarios en los servicios de nube, identifica posibles riesgos de seguridad e infracciones de políticas para evitar la pérdida de datos, y controla las cargas y descargas de aplicaciones SaaS.



**Figura 2.** Acceso seguro en la fabricación con HPE Aruba Networking SSE

Para mejorar la seguridad en los centros de fabricación, el cortafuegos integrado de última generación de EdgeConnect SD-WAN extiende la segmentación de confianza cero del extremo a la nube, protegiendo las aplicaciones, los usuarios y los dispositivos de TI, TO e IIoT. La segmentación es el control número uno para organizar el tráfico de TI y TO en un entorno de fabricación muy heterogéneo con activos de diversos orígenes, incluidos protocolos exclusivos heredados. Al segmentar la red en función del rol y la identidad, los usuarios y los dispositivos solo pueden conectarse a sus destinos y aplicaciones objetivo de acuerdo con la configuración de políticas.

Cuando se envía tráfico a través de internet, EdgeConnect First-packet iQ™ identifica y clasifica las aplicaciones en el primer paquete transmitido. Esta función de enrutamiento seguro de Internet automatiza la dirección del tráfico al destino correcto según las políticas de seguridad definidas. Por ejemplo, el tráfico de aplicaciones en la nube fiable, como UCaaS (videoconferencia), se puede enviar directamente a internet. Otro tráfico vinculado a internet (ERP, CRM, almacenamiento de datos e historiales) podría redirigirse a HPE Aruba Networking SSE u otra solución SSE de terceros. Las aplicaciones no fiables pueden ser enviadas de vuelta al centro de datos empresarial para realizar una inspección de seguridad más exhaustiva.



**Figura 3.** División segura del tráfico de Internet en función de la identificación del primer paquete con EdgeConnect SD-WAN

## Experiencia de red mejorada

El agrupamiento de túneles SD-WAN de EdgeConnect combina múltiples servicios de transporte WAN (incluidos MPLS, banda ancha de internet, comunicaciones vía satélite y 5G) para crear un único enlace lógico de mayor ancho de banda. El agrupamiento de túneles permite que la banda ancha de internet de bajo coste, donde su uso está permitido, ofrezca un rendimiento igual o mejor que el costoso y complejo MPLS. El desafío de los enlaces de internet y celulares es que son más propensos a la pérdida de paquetes, fluctuaciones y cortes que en un escenario normal podrían afectar a servicios que requieren un rendimiento más determinista en la pila de tecnología de la fabricación, como la transmisión de vídeo o la supervisión de procesos en tiempo real.

La función de corrección de errores de reenvío (FEC) de EdgeConnect SD-WAN reconstruye automáticamente los paquetes perdidos, mientras que la corrección del orden de los paquetes (POC) reordena los paquetes que llegan fuera de secuencia a su destino al equilibrar la carga del tráfico entre múltiples servicios de transporte WAN. Los enlaces lentos se solucionan mediante la opción Optimización de WAN, que aplica la aceleración del protocolo TCP, la deduplicación de datos y la compresión para acelerar el flujo de tráfico. AppExpress optimiza la experiencia del usuario a través de redes multinube para aplicaciones fundamentales para el negocio al explotar la diversidad de rutas SD-WAN y seleccionar automáticamente la mejor ruta para cada aplicación. La supervisión de la experiencia digital (DEM), parte de HPE Aruba Networking SSE, garantiza la productividad del usuario midiendo métricas y supervisando el rendimiento de aplicaciones, dispositivos y redes a través de internet.

## Implementaciones sencillas

La solución de SASE unificado de HPE Aruba Networking es fácil de implementar y acelera la adopción de SASE.

La plataforma ofrece una gestión centralizada para supervisar y controlar toda la infraestructura de red. Esto simplifica la aplicación de políticas, la supervisión y la resolución de problemas. La gestión centralizada incluye configuración y diagnóstico remotos, lo que elimina la necesidad de contar con personal de TI especializado local. Esto es especialmente relevante en el escenario actual de escasez de habilidades en el sector de la fabricación, donde muchas ubicaciones no cuentan con personal de TI dedicado (o solo con uno limitado).

HPE Aruba Networking SSE es una plataforma unificada donde ZTNA, SWG y CASB comparten una única base de código. Todas las políticas se administran desde una única interfaz de usuario, lo que facilita enormemente el control de acceso a los administradores de TI.

EdgeConnect SD-WAN integra en una sola puerta de enlace un optimizador de WAN, un enrutador y un cortafuegos, eliminando la necesidad de usar los tres dispositivos por separado.

## Resumen

La solución unificada SASE de HPE Aruba Networking permite a las fábricas reforzar sus defensas de ciberseguridad, optimizar las operaciones y adaptarse a las cambiantes demandas de la era digital. Ofrece acceso seguro de alta disponibilidad al tráfico de TO, TI e IIoT a través de prácticamente cualquier ruta WAN y permite un acceso remoto seguro. Se pueden integrar fácilmente nuevas ubicaciones y dispositivos sin comprometer la seguridad ni el rendimiento. Además, la gestión centralizada facilita las operaciones, aumenta la visibilidad y permite a los administradores de TI organizar de forma centralizada las políticas de red y seguridad. Con esta solución, las empresas de fabricación pueden mejorar el cumplimiento de las normas y los requisitos legales.

### Características y ventajas principales

#### Implementación del acceso de confianza cero, mejora de la seguridad y el cumplimiento

**Security Service Edge (SSE)** HPE Aruba Networking SSE proporciona componentes de seguridad clave, incluidos ZTNA (acceso a la red de confianza cero), SWG (puerta de enlace web segura) y CASB (agente de seguridad para el acceso a la nube).

**Apoyo para el trabajo remoto** Habilita un acceso seguro a las aplicaciones y los datos de fabricación desde ubicaciones remotas. Sustituye la lenta e insegura VPN heredada por ZTNA.

**Microsegmentación en dispositivos de TI, TO e IIoT** Segmenta el tráfico en función de las funciones y la identidad en subredes, lo que limita la propagación de ciberataques y malware en centros de fabricación, y reduce la superficie de ataque.

**Cortafuegos avanzado** El cortafuegos de última generación de EdgeConnect SD-WAN cuenta con inspección profunda de paquetes, detección y prevención de intrusiones (IDS/IPS) y defensa DDoS para controlar el tráfico entrante y supervisar, marcar y descartar el tráfico amenazante, lo que permite que los centros de fabricación reemplacen los cortafuegos heredados.

### Proporcionar una experiencia de conectividad avanzada

<b>Mayor rendimiento y reducción de costes</b>	EdgeConnect SD-WAN une simultáneamente enlaces MPLS, de internet, comunicaciones vía satélite o móviles para lograr un mayor rendimiento y menores costes operativos. Además, al consolidar las funciones de red y seguridad, SASE reduce potencialmente los costes de infraestructura.
<b>Optimización de red</b>	Supera los efectos de la latencia en la WAN comprimiendo y deduplicando los datos con la optimización de WAN. Mitiga los efectos de los enlaces inalámbricos y de internet que a menudo sufren pérdida de paquetes y fluctuaciones con la corrección de errores de reenvío (FEC).
<b>AppExpress</b>	Optimiza la experiencia de usuario aprovechando la diversidad de rutas SD-WAN y seleccionando automáticamente la mejor ruta para cada aplicación en la web.
<b>Redes multinube</b>	Proporciona una conectividad global con nubes públicas y privadas sin la necesidad de redirigir el tráfico de vuelta a un centro de datos.
<b>Supervisión de la experiencia digital (DEM)</b>	Proporciona visibilidad y análisis optimizados y en línea de las interacciones, la experiencia y el rendimiento de los dispositivos, las aplicaciones y las redes.

### Implementa fácilmente nuevas ubicaciones y supervisión de la actividad de la red

<b>Implementaciones más rápidas</b>	La gestión centralizada y el diagnóstico remoto aceleran las implementaciones sin necesidad de contar con personal de TI especializado. Integra nuevas ubicaciones y sitios remotos sin problemas, y sin comprometer la seguridad ni el rendimiento.
<b>Visibilidad total</b>	Los paneles avanzados proporcionan una vista agregada del estado de la red y la seguridad en función de los umbrales y alertas configurados.
<b>Aplicación de políticas</b>	HPE Aruba Networking SSE proporciona un único motor de políticas para configurar políticas ZTNA, SWG y CASB en una única interfaz. EdgeConnect SD-WAN organiza de forma centralizada las políticas de seguridad y conectividad de red, facilitando la implementación y la gestión de la solución.



## Recursos adicionales

[Diseño de instalaciones industriales hiperconscientes](#)

[HPE Aruba Networking ESP en la industria y la fabricación](#)

[Plataforma de SASE unificado de HPE Aruba Networking](#)

[HPE Aruba Networking Manufacturing](#)

Visit [HPE.com](https://www.hpe.com)

## [Chat con Ventas](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. La información aquí contenida está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo que aquí se indica 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.

El logotipo de Google es una marca registrada de Google LLC. Todas las marcas de terceros pertenecen a sus respectivos titulares..

a00119879ESE, Rev. 2

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

