

**Entregar SASE y
confianza cero
universal del
extremo a la nube**

A medida que las organizaciones avanzan hacia una arquitectura centrada en la nube, donde la mayoría de las aplicaciones residen en la nube y aumenta la demanda de trabajo híbrido, la seguridad debe evolucionar en paralelo. Las arquitecturas tradicionales se basan en defensas perimetrales, mientras que los datos corporativos ahora están alojados en aplicaciones SaaS y los trabajadores remotos acceden a los recursos corporativos desde cualquier lugar y cualquier dispositivo. Los directores de información (CIO) y otros encargados de la toma de decisiones se están centrando más en las soluciones de seguridad de confianza cero, pero se enfrentan a desafíos a la hora de implementar soluciones de confianza cero maduras para usuarios y cosas que acceden a los recursos desde cualquier lugar. Además, a medida que las amenazas a la seguridad se vuelven más complejas y frecuentes, los equipos de TI tienen dificultades para detectar y responder a las amenazas cambiantes en tiempo real. Las herramientas de supervisión tradicionales generan un gran volumen de alertas, mientras que la intervención manual para identificar y resolver problemas consume mucho tiempo.

Estas son las razones clave por las que una plataforma de extremo de servicio de acceso seguro (SASE) de un solo proveedor con confianza cero universal del extremo a la nube es fundamental para las empresas digitales modernas:

- los modelos de seguridad tradicionales no ofrecen un acceso uniforme y seguro a todos los usuarios y cosas en diferentes entornos, incluidos los locales, los basados en la nube y el teletrabajo, así como en distintos tipos de dispositivos.
- Las redes virtuales privadas (VPN) heredadas suelen ofrecer una experiencia de usuario deficiente. Además, el uso de VPN sin controles granulares puede otorgar niveles demasiado amplios de privilegios de red, lo que concede a los usuarios acceso a más recursos de los necesarios y aumenta los riesgos de seguridad.

- Las arquitecturas de red tradicionales dirigen el tráfico de las aplicaciones al centro de datos para su inspección de seguridad, lo que ya no resulta práctico y afecta al rendimiento de las aplicaciones porque la mayoría de ellas ahora residen en la nube.
- Dado que los datos corporativos se alojan cada vez más en aplicaciones SaaS, las organizaciones necesitan tomar medidas adicionales para proteger sus datos. Los datos corporativos pueden almacenarse tanto en aplicaciones en la nube (o TI en la sombra) aprobadas como no aprobadas y pueden circular por enlaces no seguros, lo que supone un riesgo potencial de pérdida de datos.
- Los empleados son vulnerables a amenazas basadas en la web, como ataques de phishing y ransomware, cuando navegan por internet o simplemente acceden a correos electrónicos.

En 2023, organizaciones de todo el mundo detectaron 317,59 millones de intentos de ransomware² y se detectaron casi nueve millones de ataques de phishing en todo el mundo. Solo en el primer trimestre de 2024, hubo casi un millón de sitios de phishing únicos en todo el mundo.³

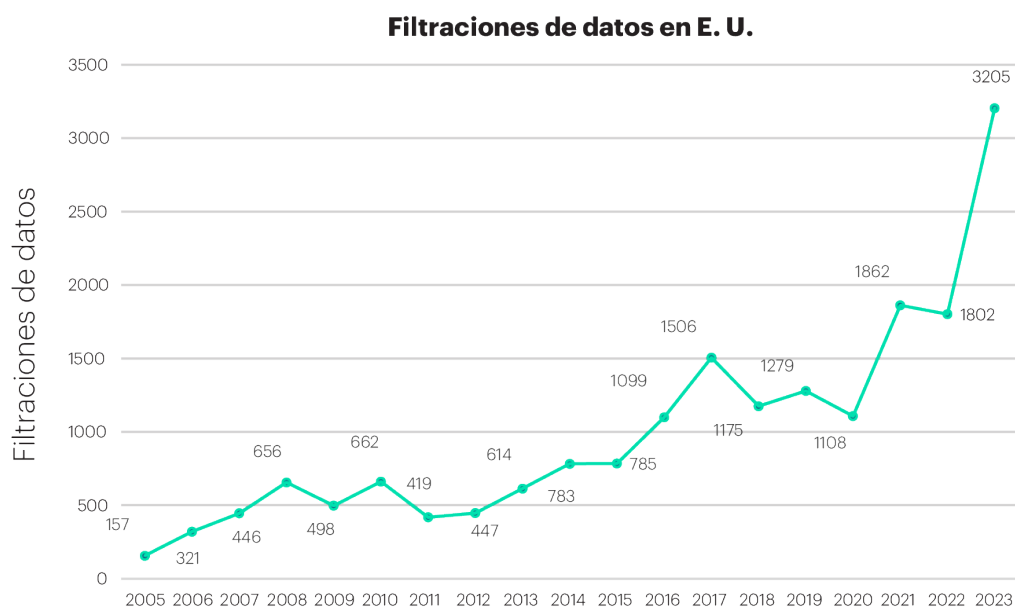


Figura 1. Filtraciones de datos en EE. UU. de 2005 a 2023¹

¹ "Annual number of data compromises and individuals impacted in the United States from 2005 to 2023," Statista, December 10, 2024

² "Annual number of ransomware attempts worldwide from 2017 to 2023," Statista, April 23, 2024

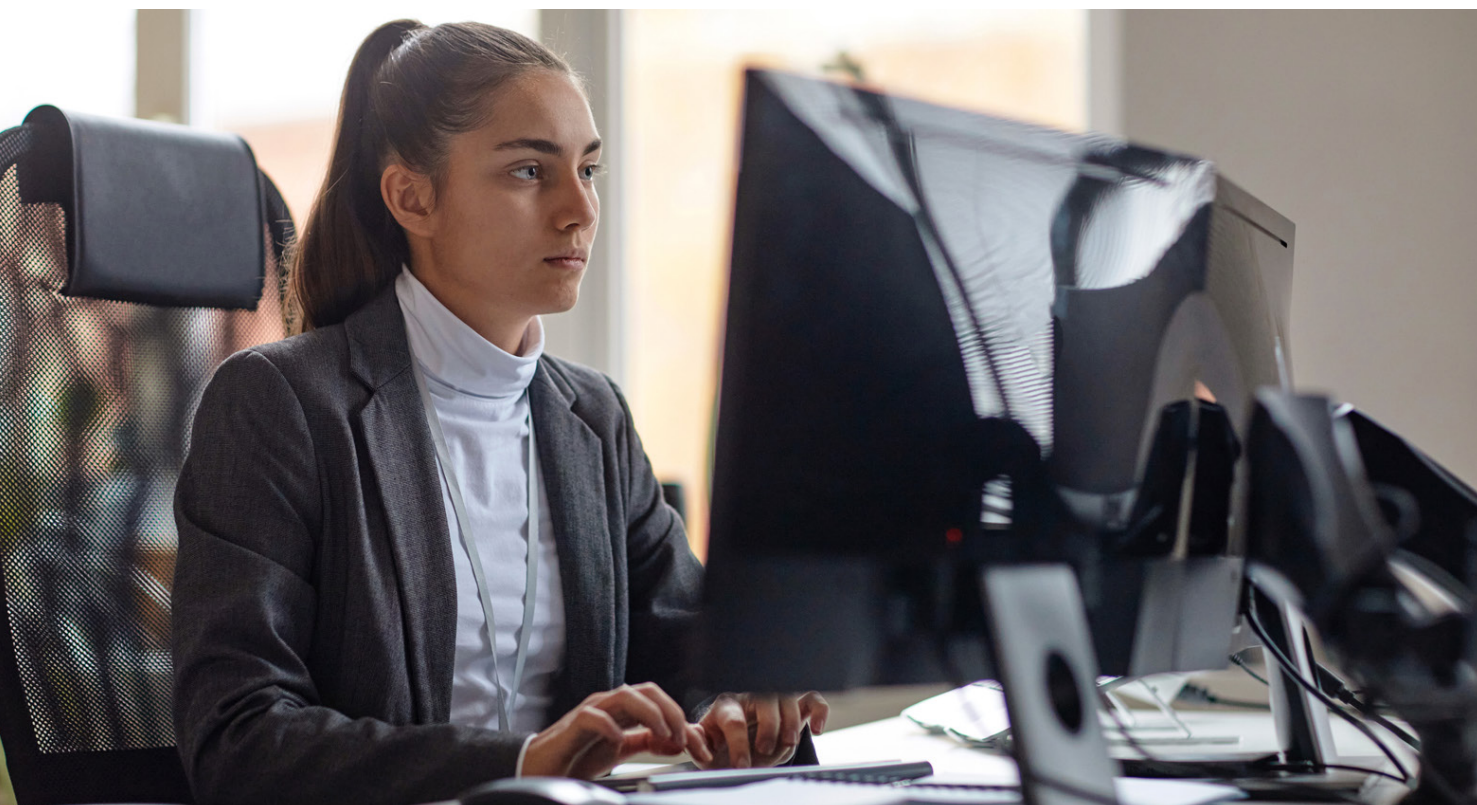
³ "Phishing - Statistics & Facts," Statista, September 24, 2024

- La proliferación de dispositivos y las políticas BYOD (traiga su propio dispositivo) dificultan la protección de los distintos dispositivos que acceden a la red corporativa, de forma local o remota. La explosión de dispositivos de Internet de las cosas (IoT) en los últimos años, la mayoría de los cuales no son propiedad ni están gestionados por el equipo de TI, ha aumentado significativamente la superficie de ataque. Sin embargo, los dispositivos IoT suelen construirse con un diseño sencillo y carecen de mecanismos de seguridad sofisticados.
- Con la evolución de las amenazas cibernéticas, los equipos de TI necesitan automatizar la supervisión de la infraestructura de red y seguridad y analizar continuamente una gran cantidad de datos en tiempo real. También necesitan capacidades de resolución de problemas eficientes para identificar con rapidez la causa raíz de los problemas de red.
- Las organizaciones deben cumplir mandatos regulatorios como NIST, HIPAA, NIS2 y RGPD, pero a menudo carecen de las herramientas esenciales y los informes completos necesarios para demostrar el cumplimiento.

Para abordar estos desafíos, las organizaciones pueden elegir entre un enfoque SASE de un solo proveedor y un enfoque SASE de múltiples proveedores. Aunque un enfoque multiproveedor permite a las organizaciones integrar nuevas características SASE en un ecosistema de seguridad existente, una estrecha integración del servicio de seguridad en el extremo (SSE) y una WAN definida por software (SD-WAN) en una plataforma SASE de un solo proveedor ofrece a las organizaciones numerosos beneficios, entre ellos una implementación más rápida, una gestión centralizada, políticas de seguridad homogéneas y la capacidad de adaptarse con fluidez al cambiante panorama de amenazas.

De hecho, Gartner predice que:

«Para 2027, el 65 % de las nuevas compras de SD-WAN formarán parte de una oferta SASE de proveedor único, un aumento del 20 % con respecto a 2024».⁴



⁴ 2024 Magic Quadrant for single-vendor SASE, Gartner, July 2024

Haz converger la red y la seguridad con una solución SASE de un solo proveedor impulsada por IA

Una solución SASE de un solo proveedor impulsada por IA ofrece un enfoque integral y unificado para la red y la seguridad. La integración de varios servicios de seguridad como SD-WAN, puerta de enlace web segura (SWG), agente de seguridad para el acceso a la nube (CASB), acceso a la red de confianza cero (ZTNA) y capacidades de IA en una plataforma cohesiva optimiza la complejidad asociada con la gestión de múltiples componentes de seguridad

y proporciona acceso de confianza cero del extremo a la nube. Esta arquitectura integrada no solo simplifica la implementación, sino que también garantiza unas políticas de seguridad unificadas, una gestión centralizada y un acceso de confianza cero uniforme, además de información generada por IA, visibilidad integral y resolución proactiva de problemas.

Qué esperar de una solución SASE de un solo proveedor

1. Arquitectura nativa de la nube y escalabilidad

Una plataforma SASE de un solo proveedor se diseña con una arquitectura nativa de la nube, de modo que aprovecha la escalabilidad y la agilidad de la computación en la nube. Esta arquitectura permite a las organizaciones asignar recursos dinámicamente en función de la demanda de tráfico, lo que facilita una red más eficiente y con capacidad de adaptación.

2. Presencia de red global

Una plataforma SASE de un solo proveedor proporciona una presencia de red global a través de puntos de presencia (PoP) distribuidos geográficamente para garantizar un rendimiento constante y una baja latencia, con independencia de la ubicación del usuario. Simplifica la gestión de los PoP, ya que las organizaciones solo tienen que administrar los PoP de un proveedor, a diferencia de un enfoque de múltiples proveedores, que requiere múltiples puntos de presencia de diferentes proveedores.

3. Gestión de políticas global

Una solución SASE de un solo proveedor gestiona las políticas de seguridad de forma centralizada y las implementa automáticamente a nivel global en toda la red. Este enfoque agiliza las operaciones, reduce la complejidad y ayuda a las organizaciones a implementar y aplicar políticas uniformes de manera eficaz.

4. Interfaz de usuario centralizada y paneles completos

Una solución SASE de un solo proveedor proporciona a los equipos de TI la capacidad de gestionar todas las operaciones de red y seguridad en una interfaz de usuario centralizada. Ofrece una mejor visibilidad del tráfico de red, los eventos de seguridad y la aplicación de políticas, lo que mejora la detección de amenazas y la respuesta a incidencias. Además, mejora las capacidades de elaboración de informes, y proporciona a las organizaciones los medios para demostrar el cumplimiento de los requisitos reglamentarios y los estándares del sector.

5. Acceso de confianza cero, protección de datos y defensa contra amenazas

Una plataforma SASE de un solo proveedor hace converger sin problemas capacidades de seguridad como ZTNA, SWG y CASB en una plataforma unificada:

- ZTNA sigue el principio de «no confiar nunca, verificar siempre». A diferencia de las VPN que garantizan un amplio acceso a la red corporativa, el ZTNA limita el acceso de los usuarios a aplicaciones o microsegmentos específicos previamente autorizados para cada usuario. También mejora la experiencia del usuario al proporcionar múltiples PoP en lugar de unos pocos concentradores VPN que implican prolongados redireccionamientos del tráfico. Esta forma de actuar refuerza el principio del acceso con privilegios mínimos. Permite que los teletrabajadores, así como los usuarios de terceras partes con ZTNA sin agente, se conecten de forma segura desde cualquier lugar. El ZTNA universal extiende los principios de confianza cero a las ubicaciones locales para cualquier usuario y dispositivo, incluido el IoT.
- CASB identifica y protege todos los datos en las aplicaciones SaaS, detecta TI en la sombra y previene la pérdida de datos con políticas que controlan a qué puede acceder un usuario y qué puede descargar, subir o compartir. En el modo en línea, toda la comunicación entre el usuario y la aplicación SaaS se envía mediante proxy a los PoP más cercanos para descifrarlos mediante SSL y analizar los datos en movimiento. El modo fuera de banda utiliza integraciones basadas en la interfaz de programa de la aplicación (API) para permitir el escaneo automático de los datos en reposo en las aplicaciones SaaS.
- SWG protege contra ransomware, malware y phishing al inspeccionar, escanear y filtrar todo el tráfico. Esta función lleva a cabo varias inspecciones de seguridad, incluido el filtrado de URL, el filtrado de contenido y el control de acceso web. Además, la SWG dispone de políticas para restringir el acceso a ciertas categorías de sitios web, como los de contenido para adultos, apuestas o sitios peligrosos.

- El cortafuegos como servicio (FWaaS) permite a las organizaciones aplicar políticas de seguridad e inspeccionar el tráfico independientemente de la ubicación, lo que permite una protección de cortafuegos escalable y flexible. Las SD-WAN seguras, parte de la solución SASE, ofrecen capacidades de seguridad avanzadas que incluyen cortafuegos de última generación, sistemas de detección y prevención de intrusiones (IDS/IPS), defensa contra denegación de servicio distribuido (DDoS) y segmentación basada en roles, lo que permite a las organizaciones reemplazar sin problemas los cortafuegos heredados en las sucursales.

6. Capacidades SASE combinadas

Con una solución SASE de un solo proveedor, las organizaciones pueden combinar fácilmente varias capacidades SASE para mejorar su postura de seguridad e inspeccionar el tráfico de una sola pasada. La inspección SSL se realiza solo una vez, lo que mejora el rendimiento y reduce la complejidad. Además, al combinar SWG y CASB con la prevención de la pérdida de datos (DLP), las organizaciones pueden supervisar mejor las actividades de los usuarios para proteger los datos confidenciales y evitar filtraciones, además de implementar controles aún más granulares sobre el acceso web.

7. Calidad de experiencia mejorada (QoE)

La supervisión de la experiencia digital (DEM) garantiza la productividad del usuario al medir métricas y supervisar el rendimiento de aplicaciones, dispositivos y redes a través de internet. Las SD-WAN avanzadas también optimizan la experiencia del usuario a través de redes multinube para aplicaciones fundamentales para el negocio aprovechando la diversidad de rutas SD-WAN y seleccionando automáticamente la mejor ruta para cada aplicación. Direccionan 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. Incluyen optimización de WAN para superar los efectos de latencia de la WAN, mediante la compresión y la deduplicación de los datos, y para mitigar los efectos de internet y los enlaces inalámbricos, que a menudo sufren pérdida de paquetes y fluctuaciones, con corrección de errores de reenvío (FEC).

8. Inteligencia artificial

Una solución SASE de un solo proveedor incluye capacidades de inteligencia artificial, como AIOps e IA generativa (GenAI), para mejorar la visibilidad de los usuarios y dispositivos conectados, además de permitir el control de acceso adaptativo. La IA también proporciona a las organizaciones información sobre el tráfico y la seguridad de la red para solucionar problemas y diagnosticar problemas de red de forma proactiva. La solución también proporciona análisis predictivo y sugiere cambios en las políticas de red y seguridad para anticipar amenazas y problemas futuros.

Implementación de la confianza cero universal desde el extremo hasta la nube

El acceso de confianza cero universal representa un cambio fundamental en el enfoque de la seguridad de red. Proporciona acceso uniforme y seguro a aplicaciones y recursos desde cualquier ubicación (remota o local) y habilita los principios de la confianza cero en todas partes, mientras que las soluciones ZTNA se centran solo en los usuarios remotos para reemplazar las soluciones de VPN heredadas.

En este enfoque, el principio de acceso con privilegios mínimos es un elemento central, que garantiza que los usuarios y los dispositivos accedan únicamente a los recursos esenciales para sus tareas. Esto se puede lograr segmentando la red en función de la identidad y el rol, reduciendo la superficie de ataque y también con otros mecanismos que incluyen visibilidad, autenticación multifactor (MFA), controles de acceso y ajuste continuo del acceso a la red en función del contexto del usuario/dispositivo.

Las organizaciones suelen tener dificultades para resolver estos desafíos clave relacionados con la confianza cero:

- los modelos de seguridad tradicionales no ofrecen un acceso uniforme y seguro a todos los entornos, como el entorno local, el basado en la nube y el teletrabajo, así como a distintos tipos de dispositivos.
- Como las organizaciones suelen operar en varias plataformas y gestionan diversas infraestructuras, cada entorno puede tener su propio conjunto de herramientas de seguridad, políticas y controles de acceso, lo que genera controles de seguridad incoherentes en toda la organización.
- Las organizaciones no disponen de una visibilidad completa de los dispositivos, las actividades y los comportamientos dentro de la red. La proliferación de dispositivos IoT y las políticas BYOD dificultan la protección de los distintos dispositivos que acceden a la red corporativa, de forma local o remota. Las organizaciones suelen tener dificultades para identificar, autenticar y autorizar estos dispositivos.

Las soluciones SASE avanzadas de un solo proveedor proporcionan un enfoque integral de confianza cero, desde el extremo hasta la nube, que protege el acceso a los usuarios y dispositivos ubicados fuera o dentro del perímetro de seguridad de la empresa. Este enfoque se puede resumir en cuatro pasos:

En 2024, más del 30 % de los encuestados informaron que ya habían implementado una estrategia de confianza cero, mientras que el 27 % planeaba implementarla en los seis meses siguientes.⁵

⁵ ["Organizations' plans for adopting zero trust strategy worldwide 2024,"](#) Statista, October 8, 2024

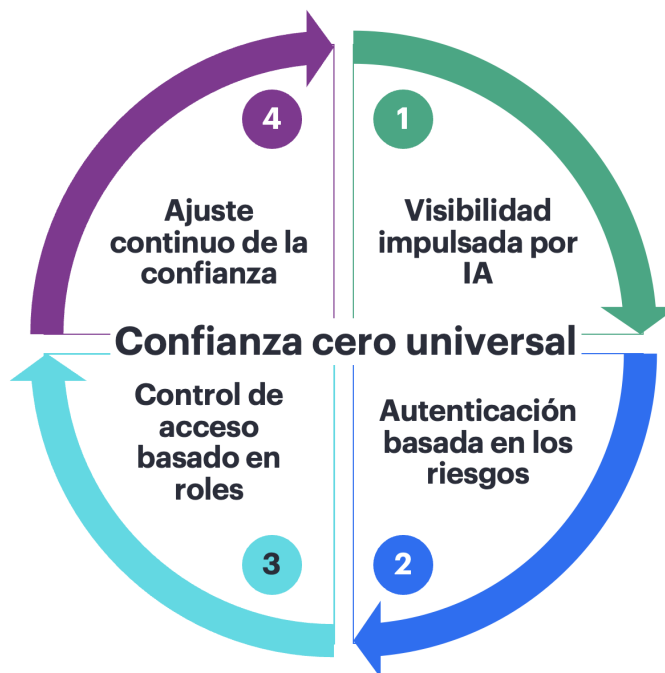


Figura 2. Adopta la confianza cero, del extremo a la nube

- 1. Visibilidad impulsada por IA:** Con la adopción creciente de políticas de IoT y BYOD, las soluciones universales de confianza cero incluyen visibilidad y creación de perfiles impulsados por IA para identificar de manera rápida y precisa cualquier tipo de dispositivo con modelos de clasificación basados en aprendizaje automático (ML).
- 2. Autenticación basada en el riesgo:** Este paso permite a los equipos de TI autenticar y autorizar cada dispositivo que se conecta a la red en función del nivel de riesgo y confianza. Esto se logra mediante MFA y otras técnicas de verificación de la identidad. Se evalúan los roles de usuario, el estado del dispositivo y factores contextuales como la ubicación y la hora de acceso para determinar la autorización. Las soluciones de confianza cero universal utilizan estándares como 802.1X para la autenticación segura o se integran con soluciones de gestión de la identidad y el acceso (IAM) como Okta o Microsoft Entra ID.™
- 3. Control del acceso basado en roles:** En este paso, los equipos de TI gestionan el control de acceso basado en roles a través de un único motor de políticas para usuarios remotos, así como para entornos de sucursales y campus. La información de la política de seguridad y cualquier actualización relacionada con el usuario, el tipo de dispositivo, el rol y la postura de seguridad se propagan a toda la red. Unas políticas sencillas de confianza cero evitan que los usuarios entren en la red corporativa, lo que garantiza la microsegmentación al nivel de las aplicaciones, mientras se enmascaran los recursos privados para los usuarios de internet.
- 4. Ajuste de confianza continuo:** En un enfoque de confianza cero universal, resulta esencial adaptar las políticas y el control de acceso en tiempo real en función de cambios en el contexto, como el tipo de dispositivo, la ubicación de acceso y el estado del dispositivo. Las soluciones avanzadas de confianza cero utilizan una confianza adaptativa para reevaluar continuamente los derechos de acceso, lo que garantiza el acceso con el mínimo privilegio por sesión, sin intervención manual. La defensa contra IDS/IPS y DDoS proporciona una capa adicional de seguridad. El registro de amenazas se puede enviar a una solución de gestión de eventos e información de seguridad (SIEM) para supervisar las amenazas en tiempo real a través de paneles avanzados.

Dispositivos IoT seguros con la confianza cero universal

La proliferación de dispositivos IoT se ha convertido en otra preocupación principal para las organizaciones, ya que esto aumenta de forma significativa la superficie de ataque. El diseño simple de estos dispositivos les impide alojar un agente de seguridad y, por tanto, no pueden protegerse fácilmente.

Las soluciones de confianza cero universal proporcionan una profunda capacidad de observación de la red para identificar y supervisar con precisión el comportamiento del dispositivo. Se centran en autenticar y autorizar dispositivos en función de su identidad, lo que garantiza que solo los dispositivos IoT fiables y autenticados puedan conectarse a la red. Las organizaciones también pueden definir políticas de acceso contextual basadas en factores como el tipo de dispositivo, la ubicación y el comportamiento para ayudar a aplicar medidas de seguridad adaptadas a los requisitos específicos de los dispositivos IoT.

Además, con la gestión de políticas centralizada y la segmentación basada en roles, la confianza cero universal utiliza varios puntos de aplicación, como conmutadores o SD-WAN seguras, para segmentar dinámicamente la red y evitar movimientos laterales. Esto garantiza que el tráfico del IoT permanece aislado de las aplicaciones para tareas cruciales, de tal forma que los usuarios y los dispositivos IoT solo se comunican con destinos coherentes con su rol según la identidad, los derechos de acceso y la postura de seguridad.

La confianza cero universal también verifica de manera continua la identidad y la postura de seguridad de los dispositivos IoT antes de conceder acceso, evitando el acceso no autorizado y garantizando que solo los dispositivos que cumplen los requisitos puedan entrar en la red. También supervisa las actividades y los comportamientos de los dispositivos IoT para detectar de manera proactiva las amenazas de seguridad asociadas con ellos y activar acciones de respuesta apropiadas.

La integración de las capacidades de SWG en SD-WAN es otra medida que ayuda a las organizaciones a proteger los dispositivos IoT contra amenazas basadas en la web. Los dispositivos IoT pueden ser vulnerables a las amenazas basadas en la web, ya que generan tráfico web cuando se comunican con servicios de nube para actualizaciones, telemetría u otros fines. Al incorporar capacidades SWG en SD-WAN, las organizaciones pueden implementar mecanismos completos de filtrado web y detección de amenazas directamente en el nivel de red para todos los dispositivos. Esto garantiza que los dispositivos IoT estén protegidos de sitios web maliciosos, ataques de phishing y otras amenazas basadas en la web, sin necesidad de contar con agentes de seguridad individuales.

Plataforma de confianza cero desde el extremo hasta la nube HPE Aruba Networking

HPE Aruba Networking establece un nuevo estándar en ciberseguridad al ofrecer una plataforma unificada e integral que trasciende las limitaciones de las soluciones de confianza cero tradicionales, que a menudo solo abordan aspectos aislados de la protección, como el acceso de usuarios remotos o el control de acceso a la red (NAC).

Nuestra plataforma de confianza cero desde el extremo hasta la nube integra una solución SASE de un solo proveedor con capacidades NAC basadas en aprendizaje automático avanzado, lo que permite a las organizaciones aplicar principios ZTNA universales en todos los dispositivos, ya sean remotos o locales.

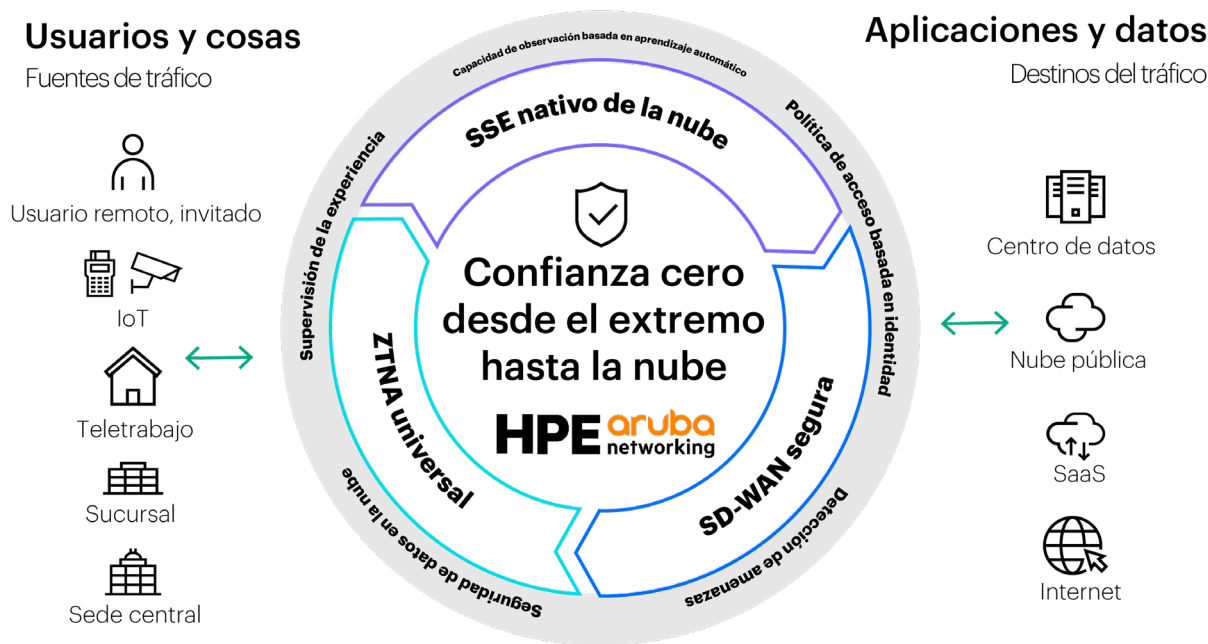


Figura 3. Plataforma de confianza cero desde el extremo hasta la nube HPE Aruba Networking

A partir de usuarios remotos, la plataforma proporciona acceso seguro y sin fisuras a recursos privados al reemplazar las VPN heredadas con ZTNA moderno. Su capacidad sin agente permite a los usuarios de terceros conectarse de forma segura, mitigando los riesgos de terceros al tiempo que simplifica la implementación y la gestión. Sobre esta base, la plataforma incorpora la funcionalidad SWG para proteger los puntos de conexión de las amenazas basadas en la web, junto con capacidades CASB y DLP que salvaguardan el acceso a las aplicaciones SaaS y protegen los datos confidenciales contra filtraciones.

Para las ubicaciones de campus y sucursales, HPE Aruba Networking amplía la seguridad de confianza cero con el extremo privado ZTNA, que ayuda a garantizar que el tráfico local permanezca local, lo que ayuda a eliminar el enrutamiento innecesario a la nube. Al mismo tiempo, aplica las mismas políticas de control de acceso granular que se aplican a los usuarios remotos, creando una postura de seguridad coherente en toda la organización.

La visibilidad impulsada por el aprendizaje automático de la plataforma se extiende a todos los dispositivos conectados, incluido el IoT, para lograr una precisión de elaboración de perfiles de hasta el 99 % que garantiza la detección y eliminación total de las amenazas.

Los administradores pueden definir y aplicar de manera centralizada una política global de confianza cero a través de HPE Aruba Networking Central, mediante cortafuegos incorporados en los conmutadores HPE Aruba Networking CX, puntos de acceso y las soluciones HPE Aruba Networking EdgeConnect SD-WAN para proteger cada punto de conexión. Para los entornos de centros de datos, HPE Aruba Networking CX 10000 Switch Series presenta la segmentación de confianza cero avanzada y un cortafuegos este-oeste, lo que mitiga la ineficacia del enrutamiento a dispositivos de hardware externos y proporciona una protección fiable de las cargas de trabajo críticas.

Pero la seguridad no termina ahí. La plataforma supervisa de manera continua la red para ajustar la confianza dinámicamente en tiempo real. Los IDS/IPS integrados funcionan junto con las capacidades de detección y respuesta de red (NDR) impulsadas por IA para identificar comportamientos anómalos y localizar amenazas, como ransomware, con una precisión incomparable. Respalda por datos de entrenamiento de casi cuatro millones de dispositivos y más de mil millones de clientes, la plataforma ofrece una precisión de detección de amenazas líder en el sector.

La solución SASE de un solo proveedor HPE Aruba Networking ofrece confianza cero al combinar HPE Aruba Networking EdgeConnect SD-WAN con HPE Aruba Networking SSE.

HPE Aruba Networking SSE es una solución nativa de la nube donde ZTNA, SWG, CASB y DEM comparten una única base de código. Todas las políticas se gestionan desde una única interfaz de usuario, lo que hace que el control de acceso sea increíblemente sencillo para los administradores de TI. Permite a los usuarios y a terceros autorizados acceder a los recursos ZTNA con y sin agente. Los usuarios están protegidos contra amenazas basadas en la web con SWG a través del filtrado de URL y la inspección SSL. Los datos confidenciales alojados en aplicaciones SaaS se supervisan de forma segura para evitar la filtración externa de datos con CASB y DLP. La DEM garantiza la productividad del usuario mediante la medición de las métricas salto a salto y la supervisión del rendimiento de las aplicaciones, los dispositivos y la red. La solución armoniza el acceso en todo el mundo a través de una red troncal en la nube de Amazon Web Services (AWS), Microsoft Azure y Google Cloud™.

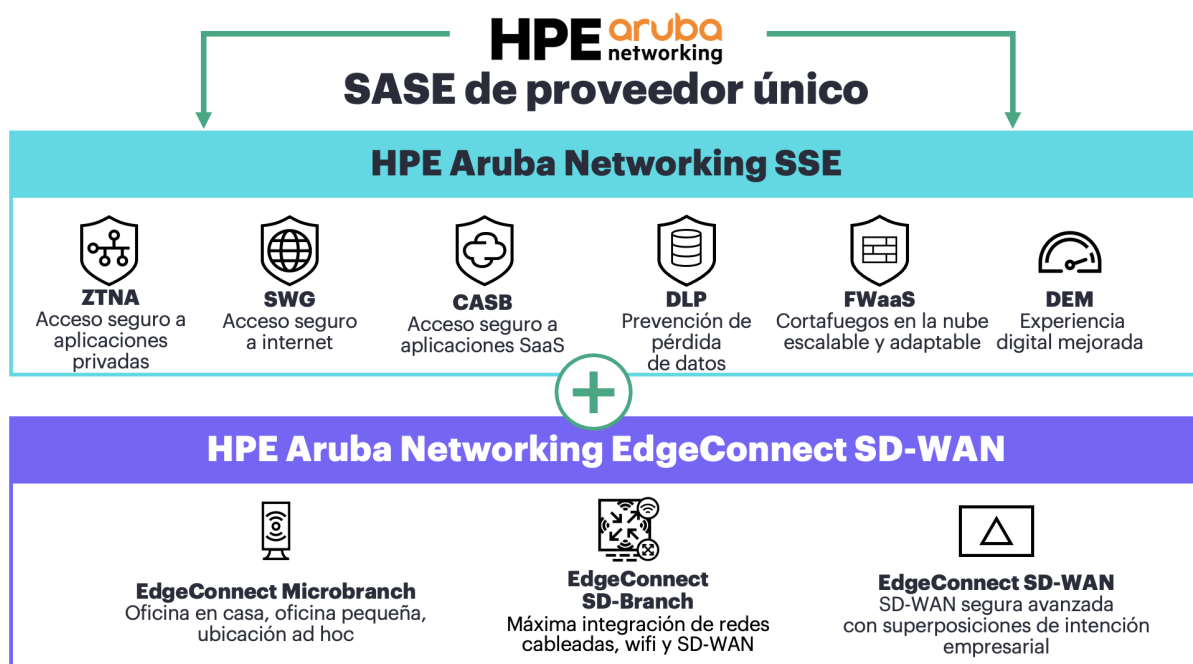


Figura 4. Plataforma de confianza cero desde el extremo hasta la nube HPE Aruba Networking

La familia HPE Aruba Networking EdgeConnect SD-WAN incluye EdgeConnect SD-WAN, EdgeConnect SD-Branch y EdgeConnect Microbranch. Se ha diseñado para proporcionar un acceso seguro y de alta disponibilidad al tráfico de red 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 ofrece una flexibilidad avanzada. HPE Aruba Networking 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 que proporciona capacidades de seguridad avanzadas en las sucursales, como segmentación basada en roles, IDS/IPS y DDoS adaptativa. La DDoS adaptativa aprovecha el aprendizaje automático para automatizar la gestión del umbral de DoS, lo que elimina la necesidad de realizar ajustes manuales del umbral de DoS. La familia HPE Aruba Networking EdgeConnect SD-WAN también se integra con SWG, para ofrecer protección integral a todos los usuarios y cosas en la red sin necesidad de instalar un agente SSE en cada dispositivo. Este enfoque integrado permite a las organizaciones evolucionar sin problemas hacia HPE Aruba Networking SASE mediante la incorporación posterior de capacidades ZTNA y CASB.

HPE Aruba Networking combina su solución SASE de un solo proveedor con soluciones NAC impulsadas por IA, incluidas HPE Aruba Networking Central y HPE Aruba Networking ClearPass, para proporcionar confianza cero universal con un enfoque integral y uniforme.

HPE Aruba Networking Central es una solución de gestión nativa de la nube que refuerza el equipo de TI con AIOps integral y grandes modelos de lenguaje (LLM) de GenAI, conocimientos más profundos y automatización del flujo de trabajo para gestionar redes de campus, sucursales, remotas, de centros de datos e IoT desde un solo panel. Si se combina con HPE Aruba Networking EdgeConnect SD-WAN y HPE Aruba Networking SSE, proporciona acceso a la confianza cero universal para usuarios y dispositivos, incluido IoT, a recursos empresariales independientemente de su ubicación. Ayuda a garantizar que siempre se conecten a destinos alineados con su rol en la empresa, tanto si se encuentran en la oficina, teletrabajando o de viaje.

HPE Aruba Networking ClearPass ofrece NAC seguro y basado en roles y dispositivos para IoT, BYOD, dispositivos empresariales, así como para empleados, contratistas e invitados a través en cualquier infraestructura con cable, inalámbrica o VPN de múltiples proveedores. La integración de HPE Aruba Networking ClearPass dentro de la infraestructura de red, incluidos conmutadores y puertas de enlace, así como HPE Aruba Networking EdgeConnect SD-WAN, aumenta la inteligencia de las aplicaciones con la identidad del usuario y del dispositivo y el contexto basado en roles para aplicar una arquitectura de confianza cero que segmenta dinámicamente la red y ajusta de manera continua el acceso en función del rol y la identidad.

HPE Aruba Networking Central y HPE Aruba Networking ClearPass ofrecen un conjunto integral de funcionalidades de seguridad como se muestra en la siguiente tabla:

Tabla 1. Componentes de HPE Aruba Networking Central y HPE Aruba Networking ClearPass para la confianza cero

Denominación	Detalles
Client Insights impulsado por IA con HPE Aruba Networking Central	Client Insights impulsado por IA ofrece la elaboración de perfiles y la visibilidad más granulares del sector. Client Insights aprovecha la telemetría nativa de la infraestructura procedente de puntos de acceso, conmutadores y puertas de enlace, así como de clientes, sin necesidad de instalar agentes o colectores físicos. Se utilizan modelos de clasificación basados en el aprendizaje automático para registrar la huella digital, identificar y elaborar perfiles detallados de todos los usuarios y puntos de conexión de IoT conectados por wifi o cableados para la asignación y aplicación de políticas.
Autenticación en la nube para HPE Aruba Networking Central	La solución permite la incorporación de usuarios finales y dispositivos cliente, bien a través de la autenticación basada en direcciones MAC, o bien a través de integraciones con los almacenes de identidades en la nube más habituales, como Google Workspace o Microsoft Entra ID.
HPE Aruba Networking Central NetConductor	HPE Aruba Networking Central NetConductor aplica políticas de seguridad de control de acceso granular en entornos distribuidos en el campus y el centro de datos utilizando estándares abiertos EVPN/VXLAN para facilitar la aplicación de políticas en línea.
HPE Aruba Networking ClearPass Policy Manager	HPE Aruba Networking ClearPass Policy Manager proporciona un motor integrado de políticas basadas en el contexto con opciones de elaboración de perfiles de dispositivos, evaluación de la postura, incorporación y acceso para invitados. Es compatible con la aplicación de RADIUS, TACACS+ y 802.1X para una autenticación segura. HPE Aruba Networking ClearPass Policy Manager también admite la autenticación de direcciones MAC para dispositivos IoT que no son compatibles con 802.1X y admite múltiples fuentes de autenticación/autorización (AD, LDAP, SQL). El inicio de sesión único (SSO) funciona con Ping, Okta y otras herramientas de gestión de identidades.
HPE Aruba Networking Central NetConductor	HPE Aruba Networking Central NetConductor aplica políticas de seguridad de control de acceso granular en entornos distribuidos en el campus y el centro de datos utilizando estándares abiertos EVPN/VXLAN para facilitar la aplicación de políticas en línea.

HPE Aruba Networking Central incluye un paquete de servicios integrales de AIOps que automatiza las actividades de solución de problemas más comunes, como:

- Información de red para diagnosticar automáticamente problemas comunes de red
- Búsqueda de IA para buscar sugerencias para la resolución de problemas y guías de soluciones utilizando lenguaje natural. La búsqueda de IA integra múltiples LLM de GenAI. A diferencia de otros enfoques de red de GenAI que utilizan LLM públicos, HPE Aruba

Networking GenAI fue diseñado con preprocesamiento y protecciones innovadoras para mejorar la experiencia del usuario y la eficiencia operativa mediante la recopilación de telemetría de casi cuatro millones de dispositivos gestionados por la red y más de mil millones de puntos de conexión cliente únicos, con uno de los lagos de datos más grandes del sector.

- Asistencia de IA para recopilar automáticamente archivos de registro y datos de resolución de problemas

Conclusión

A medida que las organizaciones digitales modernas se enfrentan a amenazas cada vez mayores con usuarios y dispositivos que se conectan desde cualquier lugar, HPE Aruba Networking presenta un enfoque integral de la confianza cero gracias a su plataforma edge-to-cloud. Al combinar las capacidades de NAC con una solución SASE de un solo proveedor, la plataforma no solo simplifica el panorama de seguridad, sino que también aprovecha el aprendizaje automático para mejorar la visibilidad y la detección de amenazas. El acceso de confianza cero garantiza que nunca se asume la confianza y que cada usuario y dispositivo, desde donde sea que se conecte, se somete a una verificación continua, en línea con los estándares de seguridad más estrictos. Este enfoque integral proporciona a las organizaciones gestión centralizada, políticas de seguridad coherentes y la capacidad para adaptarse sin fisuras al cambiante paisaje de amenazas.

Visita [HPE.com](https://hpe.com)

Más información en

[SASE en HPE](#)

[Iniciar chat ahora](#)

© Copyright 2025 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 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.

Google Cloud y Google Workspace son marcas comerciales de Google Inc. Azure y Microsoft son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y/u otros países. Todas las marcas de terceros son propiedad de sus respectivos titulares.

a00138196ESE, rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com

