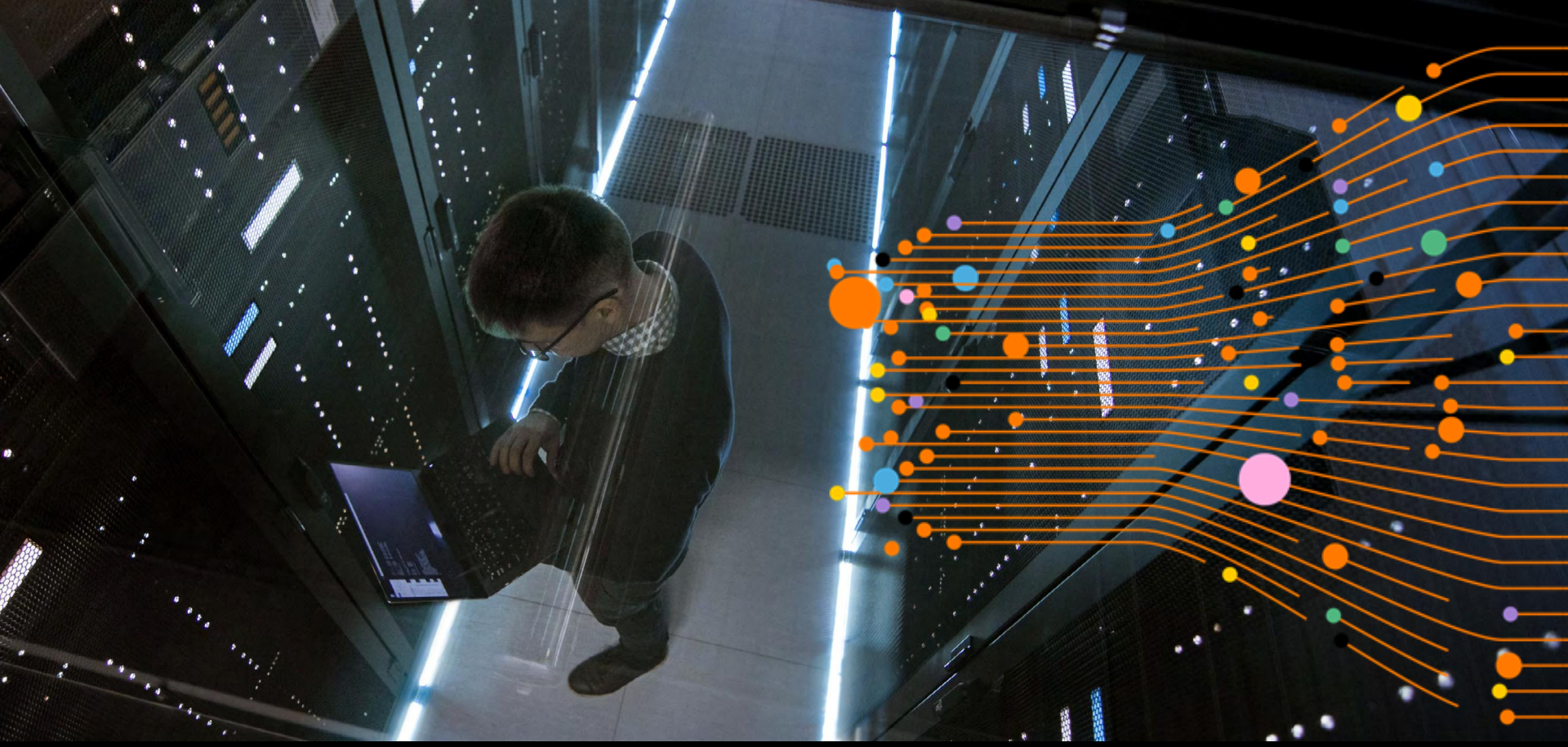


Su viaje a SASE

Garantía de seguridad a través de Secure Access Service Edge

orange™ Business Services

paloalto® NETWORKS

Resúmen ejecutivo

Los requisitos de TI corporativos son amplios y ambiciosos. La mayoría busca una más flexibilidad, una experiencia de usuario mejorada, optimización organizacional y la capacidad de administrar una fuerza laboral cada vez más distribuída. Probablemente haya escuchado que Secure Access Service Edge (SASE) promete ofrecer todo eso. Lo que quizás no se dé cuenta es que ya está en el camino de SASE.

La mayoría de las empresas se encuentran en la fase inicial de la transformación SASE. A medida que avanzamos, todas las empresas que han adoptado SD-WAN para brindar servicios basados en la nube deberían adoptar SASE. Sin embargo, es esencial tener en cuenta que SASE se trata de adquirir una metodología, no una plataforma. Se trata de dar pequeños pasos hacia la gran visión comenzando con el mayor desafío, como acceso remoto, y luego sumar los siguientes peldaños hacia SASE.

En este e-book, Orange Business Services se une a Palo Alto Networks para abordar lo que SASE aporta a las empresas y cómo pueden acelerar su viaje SASE a través de esta asociación. También examinamos cómo las empresas pueden implementar una estrategia SASE proactiva que apunte a resultados comerciales individuales, identificando dependencias y prioridades que impulsarán el éxito.

Siga leyendo para saber cómo beneficiarse de SASE en su organización.

60% **Para 2025, al menos el 60 % de las empresas tendrán estrategias y cronogramas para la adopción de SASE, cubriendo el acceso de usuario, industria y perímetro, frente al 10 % en 2020.[1]**

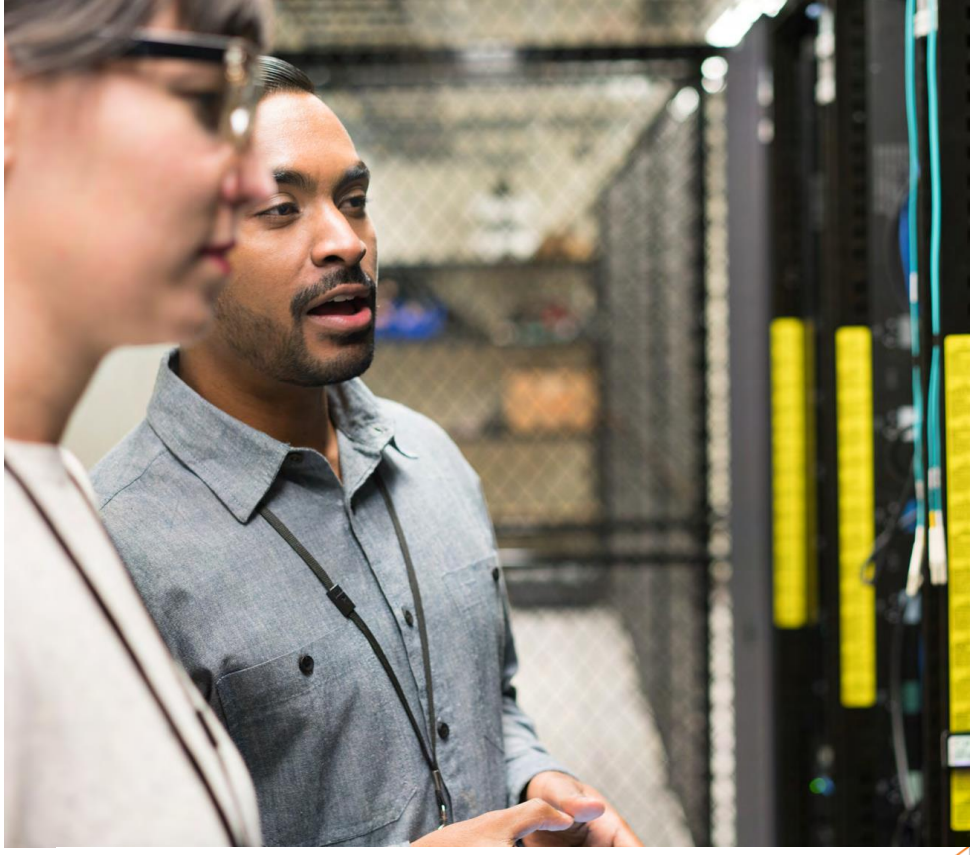
Índice

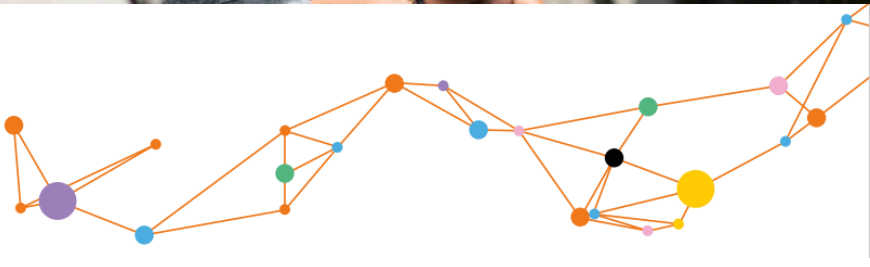
¿Por qué SASE?

***Cloud-frist* se está convirtiendo rápidamente en la norma para las empresas, y el procesamiento se está alejando del centro de datos hacia el perímetro de la red en algunos casos, pero no necesariamente en todos, lo que requiere la integración de la nube primero con cargas de trabajo que no necesariamente se prestan a la migración a la nube. Los usuarios necesitan acceso inmediato e ininterrumpido a los datos y las aplicaciones donde sea que estén trabajando. El gran desafío en este entorno cada vez más dinámico y en expansión es mantener todo seguro.**

¿SASE podría ser la respuesta? Una estrategia emergente de red y ciberseguridad orientada a la nube converge los servicios de red y seguridad para proteger a los usuarios, las aplicaciones y los datos. Una arquitectura SASE identifica dispositivos y usuarios, aplica seguridad consistente basada en políticas y proporciona acceso seguro a aplicaciones o datos.

Fundamentalmente, SASE combina las capacidades de la red de área amplia definida por software (SD-WAN) con un conjunto de estrategias de seguridad prescriptivas orientadas en torno a la seguridad de los activos, de manera significativa a medida que se acelera la tecnología en la nube "como servicio". Este enfoque de seguridad ofrece servicios de red y seguridad de nivel secundario y superpuesto como un solo servicio, lo que reduce la complejidad. Combina las mejores funciones de seguridad y SD-WAN para brindar una experiencia de usuario única al tiempo que reduce los riesgos de seguridad.

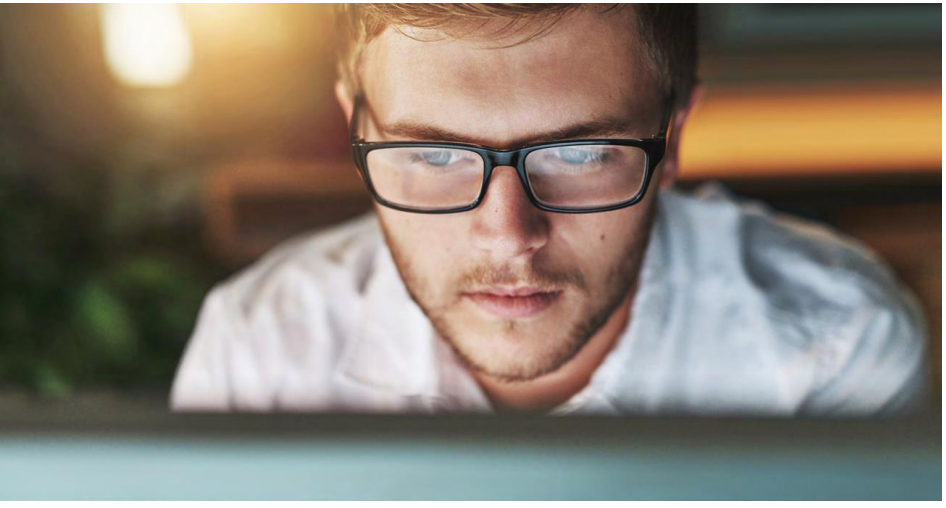




El viaje a SASE

A medida que las empresas se trasladan a la nube, rápidamente se dan cuenta de que la infraestructura y la seguridad de la red ya no pueden operar en silos. Muchas organizaciones ya han comenzado su viaje SASE, pero a veces no saben exactamente dónde se encuentran en el proceso. Por lo tanto, comience abordando sus desafíos de transformación digital, edge computing y su fuerza laboral móvil.

SASE no es un producto independiente que se pueda comprar. En su nivel más alto, la implementación de una arquitectura SASE se basa en la idea de permitir conectividad y acceso seguros a los recursos del perímetro. Para funcionar de manera eficiente, todos los componentes del modelo de conectividad, la red y la seguridad de SASE deben integrarse perfectamente como parte de un sistema administrado centralmente.

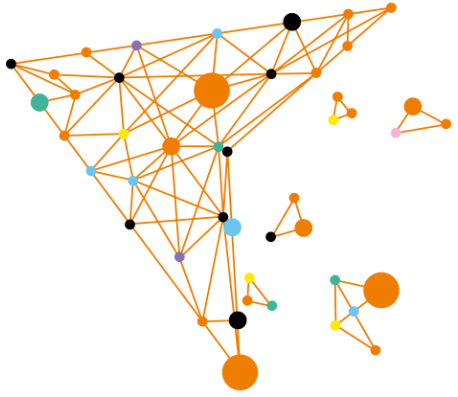


No existe una solución preparada para SASE

El camino hacia SASE está lejos de ser simple. Cada empresa tiene su punto de partida que requiere reflexión, flexibilidad y personalización.

SASE brinda mayor flexibilidad y protección de datos, menor complejidad y mayor rendimiento, lo que genera ganancias en productividad y rentabilidad. En lugar de comprar y administrar productos desde múltiples puntos, una sola plataforma aumentará significativamente la eficiencia de los recursos de TI y brindará a la empresa una mayor agilidad, integrando las redes y la seguridad en un solo panel.

En 2023, para proporcionar un ancho de banda flexible, rentable y escalable, el 30% de los sitios corporativos tendrán únicamente conectividad internet WAN, en comparación con aproximadamente el 15% en 2020.[2]



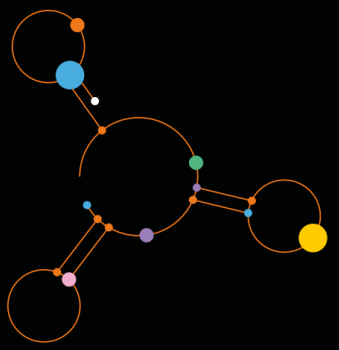
Habilitando Zero Trust

Zero Trust Network Access (ZTNA) es un componente esencial en la arquitectura SASE, imprescindible para proporcionar seguridad de extremo a extremo. ZTNA está diseñado para hacer cumplir una política de confianza cero basada en el concepto de "nunca confíes, siempre verifica". Básicamente, el nivel de confianza se establece en "cero". La inspección completa del contenido integrado con SASE proporciona una mejor seguridad y visibilidad en la red.

La necesidad de respaldar la transformación digital corporativa con una postura de seguridad de confianza cero mientras se gestiona la complejidad es crucial para la adopción de SASE.[3]

Juntos, SASE y ZTNA pueden mejorar significativamente su postura de seguridad general al:

- Aportar escalabilidad segura a una plataforma multiusuario nativa de la nube
- Aumentar la granularidad en términos de visibilidad de red y control de políticas
- Proporcionar seguridad sin degradación del rendimiento
- Proporcionar seguridad en cualquier momento y en cualquier lugar trabajando sin afectar la productividad



60% **Para 2023, junto con SASE y ZTNA, el 60% de las empresas eliminarán sus VPNs en favor de soluciones basadas en ZTNA.** [4]

SASE apoya el negocio digital

Con la explosión de los negocios digitales, las redes se distribuyen y virtualizan cada vez más. SASE puede ayudarlo a entregar de forma segura la nube y otras aplicaciones a los usuarios finales.

La transformación digital y la rápida adopción de la nube han cambiado la red empresarial. Más usuarios trabajan de forma remota y se almacenan más datos confidenciales en la nube y fuera del perímetro empresarial tradicional. Tener este acceso a la empresa desde cualquier lugar es otro factor que contribuye a la adopción de SASE.

La ventaja de la arquitectura SASE es que incorpora tecnologías adquiridas por suscripción para integrar la seguridad en la red en cualquier momento y en cualquier lugar. Así, la prestación de servicios en la nube es más segura y fluida. Se pueden aplicar políticas de seguridad coherentes a todos los usuarios y activos, independientemente de su ubicación, ya sea en centros de datos, la nube o como SaaS, sin ninguna degradación en términos de rendimiento.

"La gran mayoría de la adopción de SASE corporativa se llevará a cabo durante los próximos años, priorizando las áreas de mayor oportunidad en ganancias de eficiencia, eliminando la complejidad y la redundancia de proveedores, y reduciendo el riesgo mediante la adopción de una postura de confianza cero".[5]
Neil McDonald, vicepresidente analista de Gartner.

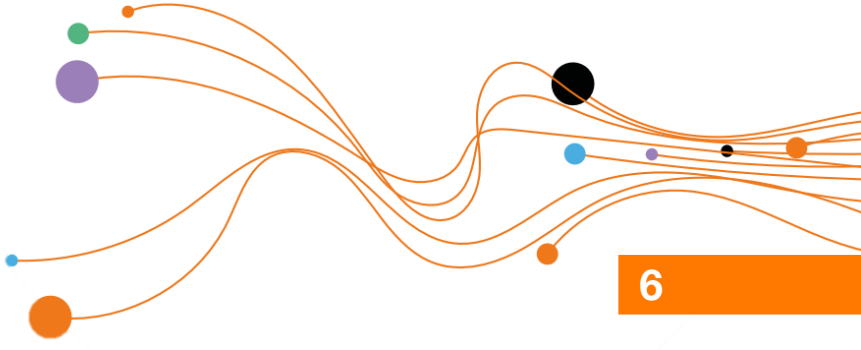
Un proceso de transformación

Una estrategia de infraestructura SASE no se puede lograr de la noche a la mañana. Es un proceso de transformación que reemplazará las VPNs, los firewalls de hardware y los dispositivos de protección DDoS existentes con el tiempo.

SASE proporciona un conjunto de funcionalidades que puede introducir a su propio ritmo, lo que le permite adoptar los servicios adecuados a las necesidades de su negocio. Estos suelen incluir SD-WAN, web gateways seguras (SWG), Cloud Access Security Brokers (CASB), firewalls de última generación y ZTNA. Una arquitectura SASE puede coexistir con su solución actual de red y seguridad hasta que los activos lleguen al final de su vida útil o se retiren.

Según Gartner, la adopción de SASE estará impulsada en parte por los ciclos de actualización de las soluciones de red y seguridad de la red y los programas de descarga de MPLS diseñados para hacer que el tráfico en la nube sea más eficiente[6] . Aquí, las conexiones directas a internet se pueden usar para descargar el tráfico destinado a la web si es necesario. Algunas empresas, sin embargo, tienen políticas que restringen esto.

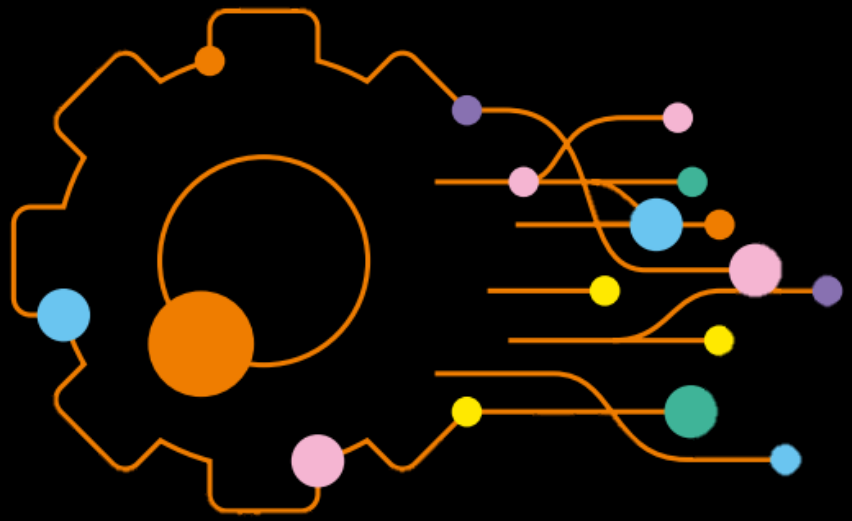
Si aún no ha analizado SASE, ahora es el momento de delinear una estrategia global para reemplazar los activos heredados por un modelo SASE convergente. Esto es esencial para administrar de manera efectiva el costo, la complejidad y las demandas de soporte comercial en un entorno dinámico en evolución.



Beneficios comerciales estratégicos de SASE

A medida que el trabajo remoto continúa convirtiéndose en lo "normal" y el enfoque “cloud first" continúa creciendo, SASE también brinda los siguientes beneficios estratégicos para su negocio:

- Convierte la funcionalidad de redes y seguridad en un único servicio en la nube gestionado desde una única consola, lo que reduce los costos y la complejidad.
- Hace cumplir el acceso a la red con privilegios mínimos mediante ZTNA, lo que mejora la seguridad
- La aplicación constante de políticas de seguridad reduce los requisitos de recursos, lo que libera a los equipos para que se centren en proyectos generadores de ingresos.
- El uso de políticas contextuales y de identidad ofrece un enfoque más dinámico y granular de la seguridad, lo que le permite abrir sus puertas virtuales a los socios comerciales mientras mitiga el riesgo.
- La gestión en la nube permite a las empresas implementar y escalar servicios rápidamente sin dispositivos adicionales ni conexiones de hardware.
- Garantiza la seguridad corporativa y regulatoria sin importar dónde o cuándo los empleados inicien sesión
- Aporta escalabilidad segura a una plataforma multiusuario nativa de la nube
- Incrementa la granularidad en términos de visibilidad de red y control de políticas
- Aumenta el nivel de seguridad sin degradación del rendimiento
- Brinda seguridad en cualquier momento y en cualquier lugar trabajando sin afectar la productividad



Pasos estratégicos para reemplazar sus activos heredados

Una transformación a una arquitectura SASE lleva tiempo. Es posible que las inversiones en hardware y software aún no estén listas para ser reemplazadas.

Para complicar aún más el panorama, muchas grandes empresas tienen equipos separados de seguridad y operaciones de red que operan en silos. Gartner sugiere crear equipos unificados responsables de la ingeniería de acceso para unificar las redes y las políticas de red en toda la organización, de la misma manera que la ingeniería de plataformas funciona con DevOps.

Sin embargo, muchas empresas han comenzado su viaje SASE (lo sepan o no) y es posible que no hayan evaluado qué tan lejos están en sus estrategias de seguridad y redes frente a SASE como arquitectura de referencia. Un primer paso esencial para continuar su viaje SASE es seleccionar un socio de confianza. Éste puede ayudar con la evaluación de la tecnología, el establecimiento de pruebas de valor o las adaptaciones que puede necesitar para integrar componentes específicos de SASE. Esto puede guiarlo a crear sus hojas de ruta de seguridad y red.

Además, aunque muchos proveedores están promocionando soluciones SASE, no todos ofrecen las capacidades SASE necesarias. Es importante medir sus requisitos frente a las mejores ofertas hasta que el mercado madure y se cierren las brechas.

Para 2025, al menos el 60% de las empresas tendrán estrategias y plazos explícitos para la adopción de SASE que abarca el acceso de usuario, sucursal y perímetro, frente al 10% en 2020.[8]

Gartner [7] incluso establece un plan de tres a cinco años para la transformación de SASE, que abarca enfoques de acceso seguro para usuarios, sucursales, ubicaciones perimetrales y aplicaciones distribuidas. Los cambios sugeridos incluyen:

- **VPN:** reemplace el acceso VPN a nivel de red con acceso de confianza cero. Además, adopte ZTNA basado en la nube para complementar el acceso VPN heredado para escenarios de mayor riesgo, como el acceso a dispositivos no administrados.
- **Zona desmilitarizada (DMZ):** comience a eliminar gradualmente los servicios basados en DMZ para el acceso de usuarios designados.
- **Inicie el reemplazo de dispositivos físicos SWG, CASB y VPN a** través de la nube cuando surjan oportunidades de actualización.
- **Implemente firewall como servicio (FWaaS)** que traslada la funcionalidad del firewall del perímetro de la red tradicional a la nube.

Hoja de ruta de migración robusta

Es importante reiterar que SASE no es un caso "plug and go". Requiere un plan de migración estratégico que cubra los requisitos de sucursal, perímetro, campus, sede y acceso remoto. El plan de migración debe reevaluarse constantemente a medida que madura el mercado SASE.

El uso de un solo proveedor para la seguridad de la red como servicio y la consolidación de stacks de tecnología reduce el costo y la complejidad. Sin embargo, no hay dos viajes SASE iguales. Cada empresa deberá prepararse de manera diferente y planificar en función de los resultados esperados.

Una cosa que SASE hace por todas las empresas es alinear procesos y simplificar redes complejas y sus operaciones de seguridad. Esto le permite rediseñar las políticas de red y crear un modelo que permita negocios seguros en la nube.

El enfoque Orange de SASE

El modelo SASE puede tardar varios años en funcionar de manera efectiva. Esto requiere una estrategia SASE a largo plazo bien pensada y la identificación de tácticas de consolidación SASE a corto plazo.

No todas las empresas tienen las habilidades, los recursos o el tiempo para investigar, construir, diseñar e implementar un modelo SASE. Aquí en Orange Business Services, podemos poner su negocio por delante de la curva SASE, lo que le permite realizar cambios en su red y en la seguridad de la red con una interrupción mínima, mientras capitaliza los beneficios comerciales.

Podemos proporcionar una evaluación SASE inicial en tres pasos:

1. ¿Dónde estásen relación al modelo SASE?
2. ¿Dónde quiere llegar? ¿Cuáles son sus ambiciones? ¿Qué tecnologías de SASE son objetivos de adopción indispensables? ¿Cómo funciona su política de seguridad actual dentro de un modelo SASE?
3. ¿Cómo podemos llevarlo allí? En otras palabras, cómo Orange puede ayudarlo a establecer su estrategia SASE.

Podemos planificar el viaje SASE de acuerdo con sus requisitos específicos, asumiendo la migración y gestionando el riesgo si es necesario. Este es un diferenciador crucial cuando se trata de nuestra oferta SASE.

SASE requiere un cambio en la cultura de TI para adoptar una red integrada y equipos de seguridad. Esta es un área que a menudo se pasa por alto. Pero si los equipos no pueden salir del trabajo en silos y compartir el control, su plan SASE se enfrentará a algunos obstáculos complicados. Podemos ayudarlo a garantizar que su recorrido por SASE impulse el rendimiento y la calidad general de su organización.

Una oferta única de SASE con Palo Alto Networks

No todas las ofertas de SASE son iguales. Lo que distingue nuestro enfoque es que se basa en Prisma® SASE, una de las soluciones SASE más completas de la industria de Palo Alto Networks. Junto con los servicios gestionados por Orange Business Services, proporciona servicios de seguridad y acceso a la red consistentes para todo tipo de aplicaciones a través de un marco común y unificado.

Orange Business Services y Palo Alto Networks brindan la interoperabilidad, la consultoría, el soporte, las habilidades de migración y los modelos flexibles de administración y consumo que las empresas exigen para lograr sus objetivos de SASE.

Esta oferta integral de SASE proporciona:

- Convergencia sin concesiones: la mejor seguridad de su clase y SD-WAN integrado de forma nativa.
- La mejor seguridad de su clase: seguridad constante en todas las aplicaciones, independientemente de la ubicación.
- Experiencia de usuario excepcional con visibilidad e información de extremo a extremo para usuarios remotos y presenciales.

¿Por qué Orange?

SASE es un proyecto integral y multidisciplinario con muchas partes móviles. Por eso es fundamental trabajar con un socio de confianza que entienda SASE y que pueda vincular la seguridad de manera efectiva a su infraestructura de red.

En Orange Business Services, ofrecemos servicios SASE integrados mientras aprovechamos nuestro ecosistema ampliado de socios tecnológicos de vanguardia. Aprovechar las integraciones entre ZTNA, CASB, SWG en la nube, VPN en la nube, FWaaS, SD-WAN y otras tecnologías heterogéneas será crucial para obtener todos los beneficios de una estrategia SASE.

Ante la continua escasez de habilidades, también puede aprovechar nuestro equipo global de profesionales de TI y seguridad que tienen experiencia en la optimización de redes, conocen las tecnologías nuevas y emergentes y están familiarizados con las medidas reglamentarias y de compliance.

Nuestros expertos en la nube, la seguridad y la conectividad de todo el mundo pueden ayudarlo en su camino hacia SASE. Pueden apoyarlo de principio a fin, permitiéndole lograr una estrategia SASE efectiva.

- **8.900 expertos en la gestión de su transformación digital**
- **18 Centros de Operaciones de Seguridad (SOC) en todo el mundo**
- **2.500 profesionales de la seguridad en un momento en el que el mercado laboral de la ciberseguridad tiene desempleo negativo**
- **El expertise edge-to-cloud garantiza la seguridad, el rendimiento y la optimización de costos para su red**
- **160 países con oficinas comerciales y soporte local**
- **Nuestro equipo de expertos brinda excelencia operativa combinada con herramientas sólidas para crear un rico catálogo de APIs para mejorar cualquier modelo de cogestión.**
- **Las capacidades de MSI ofrecen simplicidad y una gestión optimizada de múltiples proveedores de servicios**

Para obtener más información sobre nuestra oferta SASE con Palo Alto Networks,
https://www.orange-business . com/es/partners/palo-alto-networks-prisma-sase-partner-especializado

orange™ Business Services

Sources:
1. Gartner 2021 roadmap for strategic SASE convergence.
2. Gartner 2021 roadmap for SASE convergence
3. Gartner 2021 roadmap for SASE convergence
4. Gartner Zero trust architecture and solutions 2020
5. Gartner 2021 strategic roadmap for SASE convergence
6. Gartner: e Service Access Secure the Into Converge Security and Edge WAN as Win to How: Trends Market July 2019
7. Gartner 2021 roadmap for strategic SASE convergence
8. Gartner 2021 roadmap for strategic SASE convergence

paloalto® NETWORKS