Eleven Paths

SASE:
El futuro de las redes y la seguridad ya está aquí

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Resumen ejecutivo

Desde que en agosto de 2019, Gartner publicara su informe "The Future of Security Networks is in the Cloud " en el que señalaba el concepto SASE como la clave del futuro de las redes y la seguridad, el murmullo a su alrededor no ha dejado de crecer. Pero a pesar de todo lo que se ha escrito desde ese momento, seguimos escuchando con frecuencia preguntas como: ¿Qué es realmente SASE? o ¿dónde puedo comprarlo?

Lo cierto es que SASE no es un producto o servicio que uno pueda adquirir directamente de un proveedor, sino un nuevo modelo en entrega de servicios de red y seguridad. Supone una evolución relevante de tendencias que han surgido en los últimos años como Security as a Service o Network as a Service. Además, SASE pretende cubrir un ingente número de escenarios, tecnologías y servicios de red y seguridad por lo que no es de extrañar que exista cierta confusión en torno a este concepto.

A continuación, trataremos de clarificar la problemática que propicia la aparición de SASE, describir el modelo, los beneficios para el cliente y cuáles son las claves para su adopción.

01 El origen de SASE: las redes y la seguridad se adaptan a la transformación digital

1 LA TRANSFORMACIÓN DIGITAL

› **La adopción del modelo en nube:**
Las arquitecturas hasta ahora vigentes, en las que el CPD era elemento centralizador de las TI, de las comunicaciones y de la seguridad, han evolucionado a arquitecturas hibridas y distribuidas con nuevos formatos como Software as a Service (SaaS), Platform as a Service (PaaS) o Infrastructure as a Service (IaaS).

› **La adopción de modelos de trabajo fuera de la oficina:**
La mejora generalizada del acceso a Internet móvil y fijo ha facilitado la explosión del teletrabajo: desde cualquier sitio y con todo tipo de dispositivos

2 SITUACIÓN EN EL ÁMBITO DE LAS COMUNICACIONES

› **Internet:**
Se han generalizado la disponibilidad de accesos a Internet de alta velocidad y fiables.

› **La WAN definida por Software:**
Las empresas apuestan por construir sus redes mediante un modelo más flexible y escalable, que hace uso tanto de sus accesos MPLS como Internet, y con una gestión de los flujos de tráfico mediante políticas que se adaptan en tiempo real al estado de la red. Es el despegue de la tecnología SD-WAN.

Este despegue se adapta al desplazamiento de ciertos tráficos desde la VPN MPLS a Internet propiciado por la adopción del modelo IaaS.

› **Virtualización de funciones de red (arquitectura NFV – Network Function Virtualization)**
La virtualización de las funciones de red dentro de una arquitectura NFV, aporta beneficios tales como la reducción de costes al utilizar hardware de propósito general, mayor agilidad en la implementación de nuevos servicios de red, o la escalabilidad.

› **Acceso Remoto:**
Las compañías han incrementado las capacidades de sus servidores de acceso remoto a medida que ha crecido la demanda interna, manteniendo esquemas centralizados, fundamentalmente en el entorno del CPD.

3 SITUACIÓN EN EL ÁMBITO DE LA SEGURIDAD DE RED

› **Soluciones de seguridad ofrecidas desde la nube (Cloud SecaaS):**
Hemos visto como los proveedores de seguridad adoptaban también el modelo Cloud Software as a Service, creando versiones de sus productos o nuevos productos enfocados a proteger entornos de nube, dando lugar al modelo Cloud Security as a Service (SecaaS).

Proxys de navegación y firewals existen ahora en modelo SaaS, y han surgido nuevos servicios como CASB (protección de aplicaciones SaaS).

› **Virtualización de funciones de seguridad de red (arquitectura NFV)**
También las funciones de seguridad de red han hecho aparición en la arquitectura NFV, y especialmente en entornos SD-WAN, con despliegues en el CPE. Entre estás funciones están los firewalls, firewalls de nueva generación o sistemas de detección de intrusiones.

› **La pila de seguridad en entornos IaaS:**
Las empresas han extendido sus actuales mecanismos de seguridad de red a los entornos iaaS, desplegando nuevos dispositivos, pero en sus versiones virtualizadas, o utilizando servicios creados por el propio proveedor de nube.

4 EL PROBLEMA REVOLUCIÓN VS. EVOLUCIÓN

La transformación digital basada en arquitecturas de nube y los modelos de trabajo en movilidad han significado una profunda revolución, sin embargo, las comunicaciones y la seguridad de red no han evolucionado al mismo ritmo.

Se han mantenido arquitecturas de red que fueron diseñadas bajo ciertas premisas que ya no son ciertas, y esto genera muchas ineficiencias:

- El CPD (No) es el punto central de las TI, las comunicaciones y la propia seguridad, alrededor del cual todo orbita.
- Los empleados (No) trabajan casi por completo desde sus oficinas con sus dispositivos corporativos y controlados, y (No) utilizan una red privada para comunicarse con las aplicaciones corporativas.

5 LAS DEBILIDADES DE LA SITUACIÓN ACTUAL

› **Aumento de la complejidad de despliegue, mantenimiento y gestión de la seguridad:**

Con la adopción de los modelos de nube pública (IaaS, PaaS, SaaS) y la proliferación de accesos a Internet en las sedes, el perímetro de red de la empresa aumenta y a menudo ni siquiera está bien definido. El despliegue de mecanismos de protección independientes en cada nuevo punto del perímetro es una empresa complicada.

Aplicar la pila de seguridad de red actual (IDS, DLP, filtrado URL, detección de vulnerabilidades, etc.) a cada uno de los silos resulta en un problema de difícil gestión y mantenimiento.

› **Aumento de los costes de seguridad:**

El despliegue de mecanismos de seguridad en el nuevo perímetro implica un incremento de la inversión y de costes de gestión (más complejidad, nuevos perfiles especialistas requeridos). Tampoco el modelo NFV con despliegue de las funciones de seguridad virtualizadas en el CPE parece que va a ayudar reduciendo costes, a pesar de las expectativas iniciales.

› **Mayor riesgo de seguridad:**

Si consideramos que cada punto del nuevo perímetro sobre el que desplegamos mecanismos de protección es un eslabón de una cadena, a medida que aumentan, mayor es la probabilidad de que uno se rompa (una vulnerabilidad, un fallo de configuración, una inconsistencia en la política) lo que conlleva una brecha de seguridad.

› **Inconsistencia de las políticas de seguridad:**

La necesidad de implantar mecanismos específicos para cubrir los nuevos escenarios hace aumentar el riesgo de inconsistencia en las políticas de seguridad. La falta de interoperabilidad entre soluciones diferentes, y a menudo de diferentes proveedores, hace peligrar objetivos de seguridad transversales, para los que se precisa colaboración. Por ejemplo, la prevención de fuga de información o la detección de intrusiones.

› **Acceso remoto no adaptado a los patrones de movilidad actuales ni a los entornos cloud:**

El acceso remoto centralizado en el CPD se adapta mal a las características del tráfico de red actual. Por ejemplo, un usuario situado cerca del servicio al que quiere acceder podría verse obligado a pasar previamente por el CPD, situado muy lejos de ese servicio. Además, las soluciones de acceso remoto tradicionales son complejas de gestionar y presentan debilidades, puesto que siguen un modelo obsoleto de confianza en la IP del origen de la conexión y carecen de la granularidad suficiente.

02 | Los fundamentos del modelo SASE

02.1. ¿Qué es SASE?

Security Access Service Edge (SASE) es un "modelo de entrega de servicio" que combina capacidades WAN y funciones de seguridad de red. En realidad, SASE no incluye conceptos verdaderamente novedosos, sino que ratifica la validez de los modelos emergentes de Security as a Service y Network as a Service. Y, además, apuesta por la integración de ambos modelos en un único servicio convergente, en el que se integren múltiples funciones tanto de red como de seguridad.

Es importante destacar, además, que SASE se entrega siempre en modo servicio y se accede a sus capacidades a través del llamado "Borde de servicio" (Service Edge).

¿Qué es el "Borde de Servicio"?

Este concepto suscita ciertas dudas. Cabría considerar que este borde queda fuera de las instalaciones del cliente, o incluso se asocia a la huella de un proveedor cloud. Desde nuestro punto de vista, el "Borde de servicio" debe interpretarse, literalmente, como el punto por el cual se accede al servicio.

La localización de este borde (un nodo con sus capacidades) puede situarse en la red de acceso de un operador, en un proveedor de nube, en las instalaciones del cliente, o en cualquiera de ellos según convenga. La clave es que, para el cliente, en todos los casos esta puerta de acceso al servicio resulte una caja negra, ya que como se ha dicho la solución se entrega siempre en modo servicio.

02.2. ¿Cuáles son las características principales de SASE?

1. Huella global de nodos:
La existencia de un **"borde de servicio" que permita un acceso eficiente cercano** (en términos de networking) a la propia huella del cliente.

2. Una capacidad SD-WAN global:
Fundamentado en el enrutamiento entre nodos, la capacidad SD-WAN debe **evitar los problemas inherentes a la Internet global**, como son las altas o impredecibles latencias.

3. Implementación distribuida de la seguridad:
Los mecanismos de seguridad se implementan sobre los nodos del servicio, **sin necesidad de redirigir el tráfico a otros nodos para su inspección.**

4. Una arquitectura nativa cloud multi-tenant:
Destaca Gartner en su propuesta la importancia de **evitar arquitectura encadenamiento** de dispositivos de seguridad y red.

5. Consolidación de funciones:
Un servicio tipo SASE debe consolidar la mayor cantidad de las funciones de seguridad en sus nodos. Esto, unido a evitar modelos de encadenamiento de funciones independientes, lleva también inevitablemente a una consolidación de fabricantes.

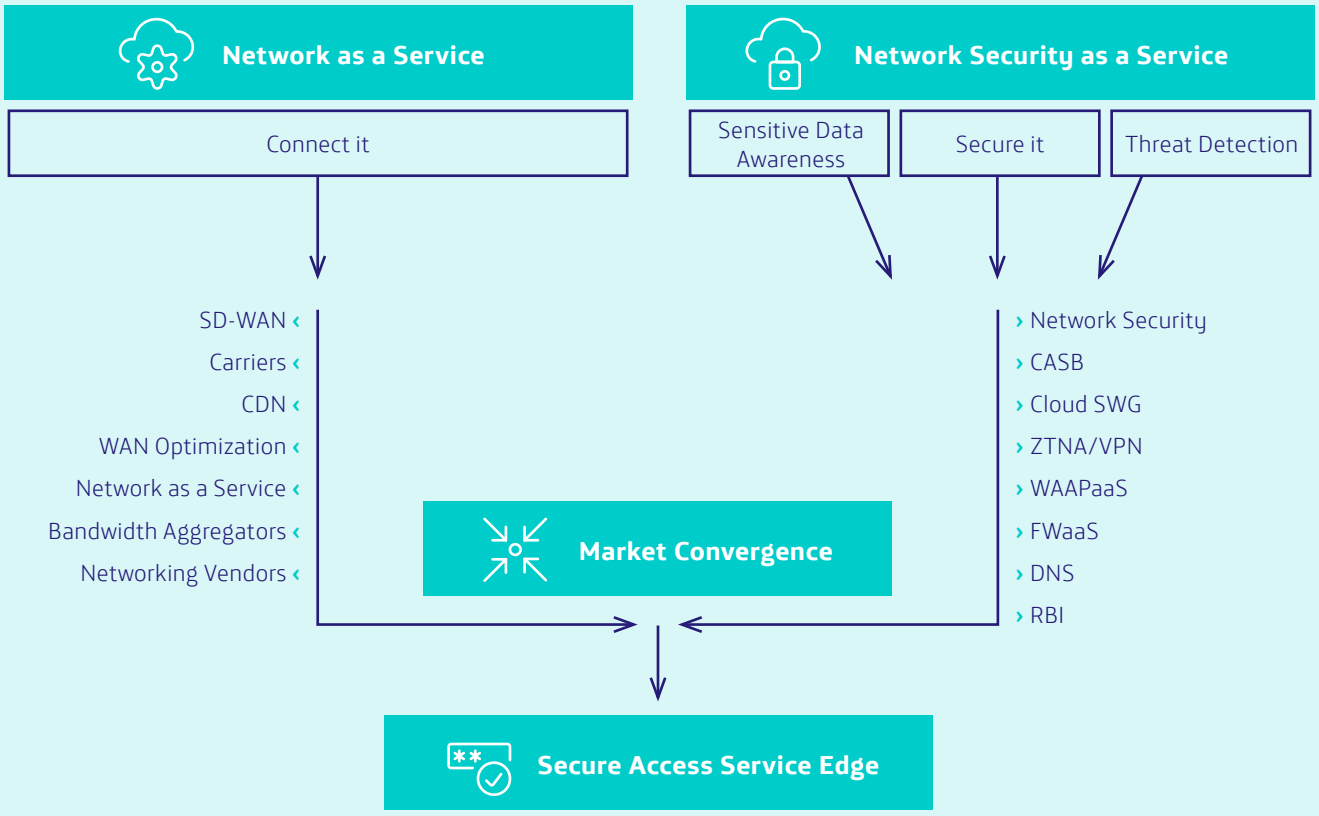
6. La identidad como pilar:
La dirección IP como parámetro que decide el control de acceso a un servicio debe desaparecer, y "la identidad" debe ocupar su lugar. Debe asegurarse la identidad de la entidad que accede a un servicio en cada conexión, y limitar este acceso exclusivamente a los recursos necesarios.

Esta aproximación se alinea a su vez con el modelo de acceso Zero Trust Network Access (ZTNA) que forma parte de la propuesta SASE, y que se presenta como alternativa a los sistemas de acceso remoto tradicionales, que presentan debilidades de seguridad y falta de adaptación a los modelos de nube y movilidad.

7. Basado en políticas:
La definición de políticas debe ser el mecanismo mediante el que el cliente interacciona con del servicio. Cualquier detalle relativo a los nodos o la arquitectura debería ser transparente al usuario.

2.3. Casos de uso

La siguiente figura, extraída del propio artículo de Gartner, muestra las tecnologías de red y seguridad que debería contemplar un servicio construido con modelo SASE.



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a Service. Source: Gartner

En la figura vemos que tanto el catálogo de tecnologías de seguridad como de red es muy diverso y aplicable a problemáticas diferentes.

Esta variedad de tecnologías consolidadas en un solo servicio permite abordar problemas fundamentales de seguridad de una forma global y consistente. La definición de un conjunto reducido de políticas se traslada, de manera transparente para el cliente, a configuraciones concretas en múltiples tecnologías, dependiendo de los escenarios contemplados.

Por otro lado, la forma de adopción del modelo SASE que más garantías de éxito ofrece es mediante un proceso gradual. No se trata de reemplazar de la noche a la mañana toda nuestra infraestructura de red y seguridad. Es fundamental identificar y priorizar los problemas que queremos resolver y evolucionar a partir de ahí añadiendo nuevos casos de uso.

Consideremos algunas problemáticas fundamentales de seguridad como casos de uso a resolver con el modelo SASE:

- Prevenir y detectar fugas de información (DLP)
- Prevenir y detectar intrusiones en la red
- Controlar el acceso a las aplicaciones corporativas
- Proteger los servicios on line de la empresa

Y ahora tomemos, por ejemplo, el primero de ellos. Existen múltiples flujos de tráfico que interesaría controlar para detectar la prevención y detección de fugas de información:

- En la navegación por internet de los empleados en la oficina o fuera de la oficina
- Durante el acceso a las aplicaciones SaaS de la empresa
- Durante el acceso remoto a las aplicaciones corporativas
- O incluso en el tráfico que circula entre diferentes VPNs de mi red SD-WAN

Con una aproximación tradicional tendríamos proveedores y tecnologías diferentes para cada uno de estos flujos. En una visión SASE, un único servicio tendría la visibilidad de todos ellos, a medida que gradualmente fuéramos incorporando los escenarios.

Internamente el servicio SASE se encarga de orquestar la implementación de las políticas de DLP en las tecnologías que correspondan:

1

Navegación Segura en Internet

Secure Web Gateway, Security by DNS, Remote Browser Isolation, FW/Next Generation Firewall as a service, Cloud Access Security Broker

2

Acceso seguro a aplicaciones corporativas

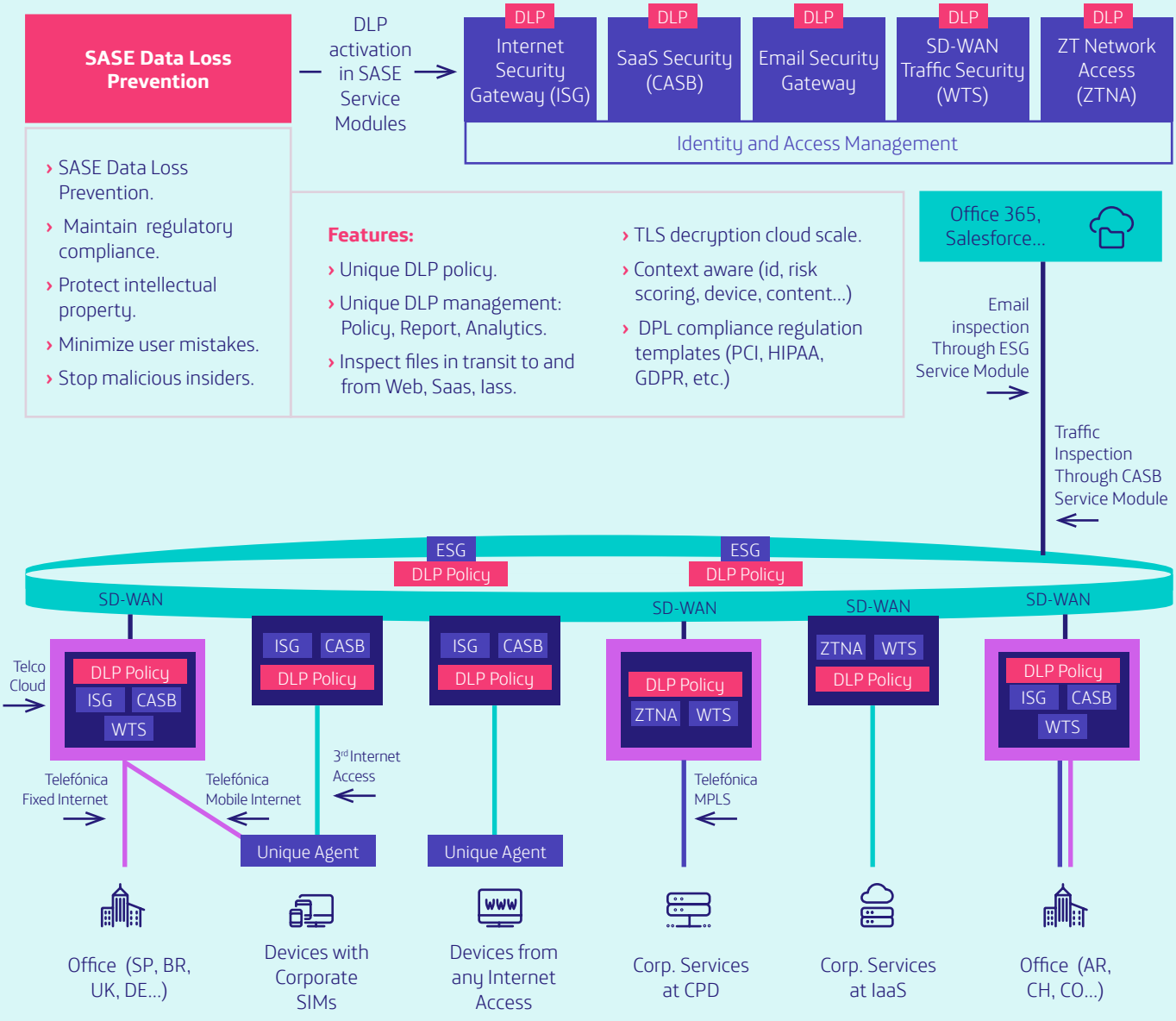
Zero Trust Network Access, Cloud Access Security Broker (aplicaciones SaaS)

3

Seguridad en el tráfico WAN

FW/Next Generation Firewall as a service, Intrusion Prevention and Detection

La siguiente figura muestra cómo se implementaría un ejemplo como el descrito, donde además de ver las diferentes tecnologías involucradas, puede apreciarse cómo el "borde de servicio" está constituido por nodos en Internet y en la propia red del operador, asegurando así la visibilidad de todos los tráficos y un tratamiento eficiente.



Ejemplo de función activación función transversal de Data Loss Prevention sobre diferentes módulos (ISG, CASB, ESG y ZTNA)

Vemos que el establecimiento de una única política de DLP activa mecanismos en diferentes tecnologías, ya sea el módulo Web Security Gateway utilizado para la navegación de los empleados, el modulo ZTNA para acceso a aplicaciones corporativas, y en definitiva todas las tecnologías asociadas a los distintos flujos de tráfico.

Además, se aprecia cómo el borde de servicio, a través del cual el cliente accede a las capacidades SASE, está constituido por nodos en la nube y en la propia red del operador, asegurando así la visibilidad de todos los tráficos y una gestión eficiente.

03 Beneficios para el cliente y cómo resuelve sus problemas actuales

A continuación, detallamos los principales beneficios que se proporcionan al migrar hacia un modelo SASE.

Reducción de costes

Reducción de elementos de seguridad, de la carga operacional, y de la cantidad de proveedores.

Reducción de complejidad

Integración de todos los componentes en **una solución construida con un modelo nativo de nube**, basada en definición de políticas y alrededor de la identidad

Mejoras de rendimiento

La optimización de enrutado de tráfico entre los nodos de servicio debería permitir ofrecer mejores rendimientos y baja latencia, lo cual es crítico para ciertos servicios como video conferencias, VoIP, etc.

Mejoras de seguridad

Mediante la **implementación de un modelo Zero Trust**, toda sesión es inspeccionada y autorizada en tiempo real. La visión se hace más holística y la gestión unificada hace disminuir la aparición de errores o inconsistencias que crean puntos de ataque.

Facilidad de uso para el usuario

Un único software agente debería cumplir todas las necesidades, y proporcionar una experiencia consistente con independencia de donde esté el usuario y a qué accede.

04 Conclusiones

Una vez identificados los problemas que la transformación digital ha hecho aflorar en el actual estado de las comunicaciones y de la seguridad de red, y una vez entendido SASE como modelo de entrega de servicios de seguridad de red y seguridad de manera unificada y en modo cloud, es el momento de preguntarse si es SASE esa **evolución rupturista que permite afrontar con garantías los desafíos de la adopción de los modelos de nube y la fuerza de trabajo en movilidad.**

En nuestra opinión, sí, la convergencia de las capacidades de red y seguridad, así como el consumo en modelo de servicio de nube es el c amino. Si analizamos los beneficios que persigue el modelo y que, sin duda, se conseguirían con una buena implementación, vemos que elimina los problemas que existen actualmente, y es un habilitador de la transformación digital.

En relación con una implementación real, creemos que es clave la definición del "borde de servicio". La aplicación de las funciones de seguridad a todos los flujos de tráfico aplicables es absolutamente dependiente de la visibilidad que de estos flujos tengan los nodos. Por esta razón, **un "borde de servicio" adecuado debería tener una huella global adaptada a las necesidades de los clientes,** incluir nodos integrados en la red de los operadores, así como nodos en la nube, o incluso en ocasiones despliegues en casa del cliente (caja negra modo servicio).

Por otro lado, en el momento actual vemos que existen algunos casos de uso más susceptibles que otros de formar parte desde un principio de un servicio en modelo SASE, tanto por características técnicas como por las necesidades actuales de los clientes. Especialmente las que se refieren a la navegación segura de los empleados y el acceso seguro a las aplicaciones.

Esto está en consonancia con la evolución que vemos en la mayoría de los proveedores tecnológicos que actualmente se enmarcan en el dominio de SASE, y también con una visión de adopción gradual del modelo por parte de los clientes.

Sobre ElevenPaths

En ElevenPaths, la compañía de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información:
elevenpaths.com | @ElevenPaths | blog.elevenpaths

ElevenPaths

Telefónica CYBER SECURITY COMPANY