EuskoData
Soluciones Tecnológicas

Por qué su organización Necesita adoptar el SASE Modelo

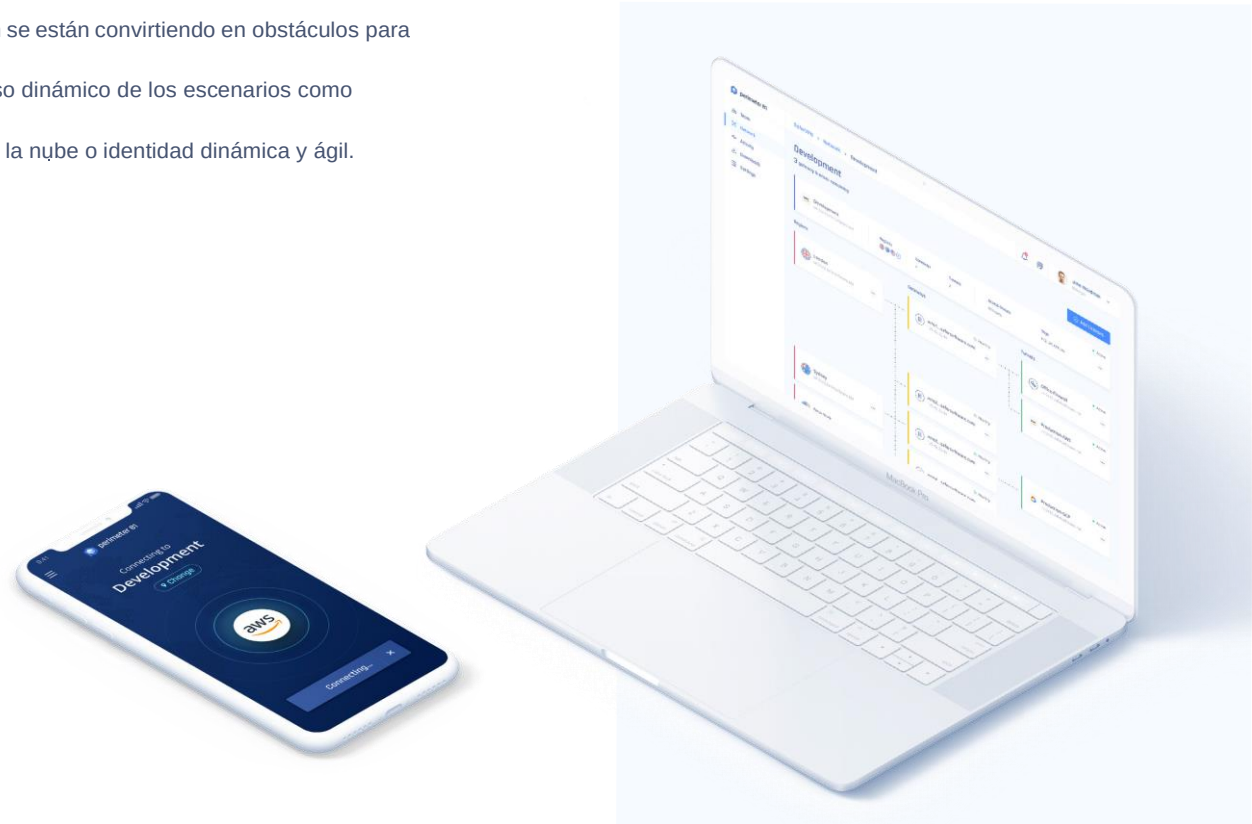
EuskoData
Soluciones Tecnológicas

Introducción

A medida que las organizaciones continúan impulsando las cargas de trabajo informáticas a la nube y proliferan los dispositivos móviles, la informática de borde está cambiando los requisitos de acceso con miles de millones de dispositivos conectados que requieren servicios en la nube y recursos locales. Al mismo tiempo, se generan y ubican más usuarios, dispositivos, aplicaciones, servicios y datos fuera de una organización que dentro.

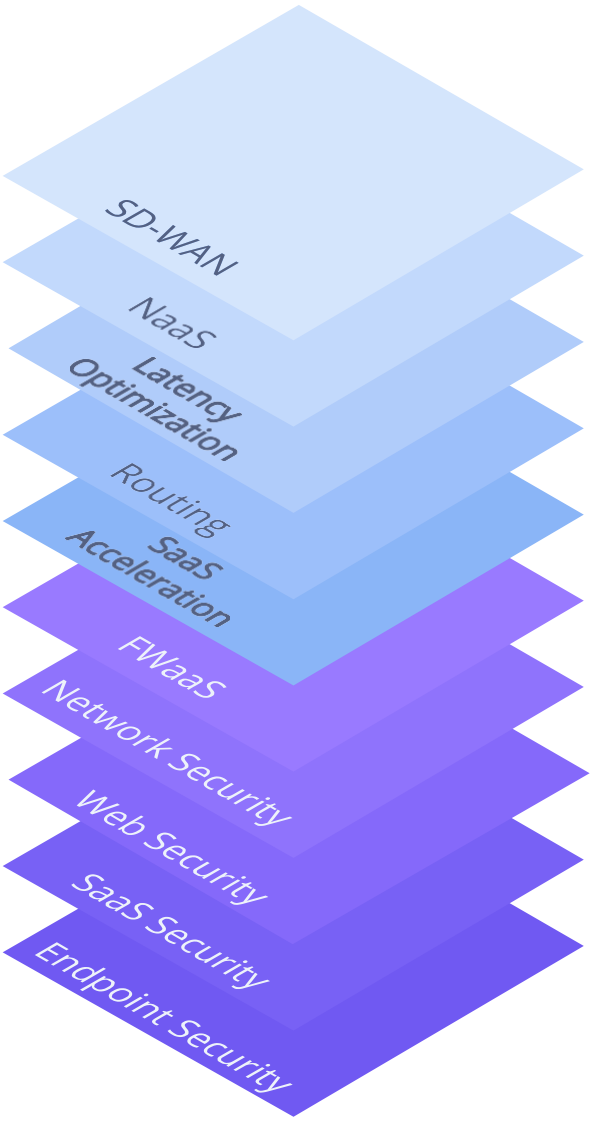
Las arquitecturas de seguridad de red tradicionales que suelen colocar a los centros de datos empresariales en el centro de los recursos de TI también se están convirtiendo en obstáculos para los requisitos de acceso dinámico de los escenarios como tecnologías nativas de la nube o identidad dinámica y ágil.

Con numerosas soluciones de seguridad de red y ciberseguridad ofrecidas en un espacio de mercado altamente segmentado, demasiados servicios y categorías de seguridad están complicando lo que debería ser un enfoque integrado para el entorno de seguridad de red de una organización. Toda la comunidad de proveedores de ciberseguridad debe unirse y proporcionar un enfoque holístico de la ciberseguridad, y aquí es donde entra en juego el concepto de Secure Access Service Edge o SASE.



El borde del servicio de acceso seguro (SASE)

Secure Access Service Edge (SASE) es un nuevo modelo de seguridad de red basado en la nube propuesto por la firma de investigación Gartner que combina múltiples tecnologías de red entregadas como un servicio, incluidos SWG, CASB, FWaaS y ZTNA con capacidades WAN (es decir, SDWAN) para respaldar el acceso seguro y dinámico a los activos de la organización. Este nuevo modelo permite a los equipos de seguridad de TI conectar y proteger fácilmente todas las redes y usuarios de su organización de una manera ágil, rentable y escalable.



“Básicamente, SASE es un nuevo paquete de tecnologías que incluye SD-WAN, SWG, CASB, ZTNA y FWaaS como capacidades centrales, con la capacidad de identificar datos confidenciales o malware y la capacidad de descifrar contenido a la velocidad de la línea, con monitoreo continuo de sesiones. para los niveles de riesgo y confianza”, dice Andrew Lerner, vicepresidente de investigación de Gartner. (Figura Imagen)

Gartner también cree que las ofertas de SASE proporcionarán acceso seguro "definido por software" basado en políticas desde una estructura de red infinitamente flexible a través de la cual los profesionales de seguridad empresarial pueden especificar con precisión el nivel de rendimiento, confiabilidad, seguridad y costo de cada sesión de red en función de la identidad y contexto.

Beneficios de SASE y casos de uso

SASE permite la entrega de servicios de seguridad de red seguros integrados que respaldan la transformación empresarial digital, la informática de punta, la movilidad de la fuerza laboral y la gestión de identidades y accesos. Además de la seguridad mejorada y el rendimiento de la red, los beneficios clave incluyen una mayor productividad de los usuarios y del personal de TI, eficiencia operativa, reducción de costos y habilitación de nuevos escenarios de negocios digitales. Además, las ofertas de SASE basadas en la nube permiten a las organizaciones actualizar sus soluciones de seguridad contra nuevas amenazas y establecer políticas más rápidamente para la adopción ágil de nuevas capacidades de seguridad.

Los dispositivos virtuales se reducirán junto con la cantidad de agentes necesarios para el usuario final y los dispositivos de borde. A medida que se adopten más servicios SASE a largo plazo, se realizarán reducciones de costos adicionales a través de una mayor consolidación de los proveedores y la simplificación de la pila de tecnología de seguridad.

Los servicios SASE también permitirán a las organizaciones hacer que sus aplicaciones, servicios, API y datos sean accesibles de manera segura para terceros, como socios y contratistas, sin la exposición al riesgo de las arquitecturas heredadas de VPN y de zona desmilitarizada (DMZ).

El rendimiento de la red se puede aumentar con las soluciones SASE que brindan un enrutamiento de tráfico optimizado a través de puntos de presencia (POP) globales.

- Complejidad
- Habilitar nuevo digital
- Mejorando la red
- Facilidad de uso y
- Seguridad
- Operativo bajo gastos generales
- Confianza cero
- Seguridad incrementada
- Política centralizada

Mediante el uso de controles y aplicación de políticas, los usuarios serán enrutados a través de socios de interconexión y redes de alto ancho de banda que cumplen con SASE.

La cantidad de agentes requeridos en un dispositivo se reducirá con soluciones compatibles con SASE, como Zero Trust Network Access a un solo agente o dispositivo con políticas de acceso optimizadas que no requieren la interacción del usuario y, al mismo tiempo, brindan una experiencia de acceso constante independientemente de la ubicación. y recurso solicitado.

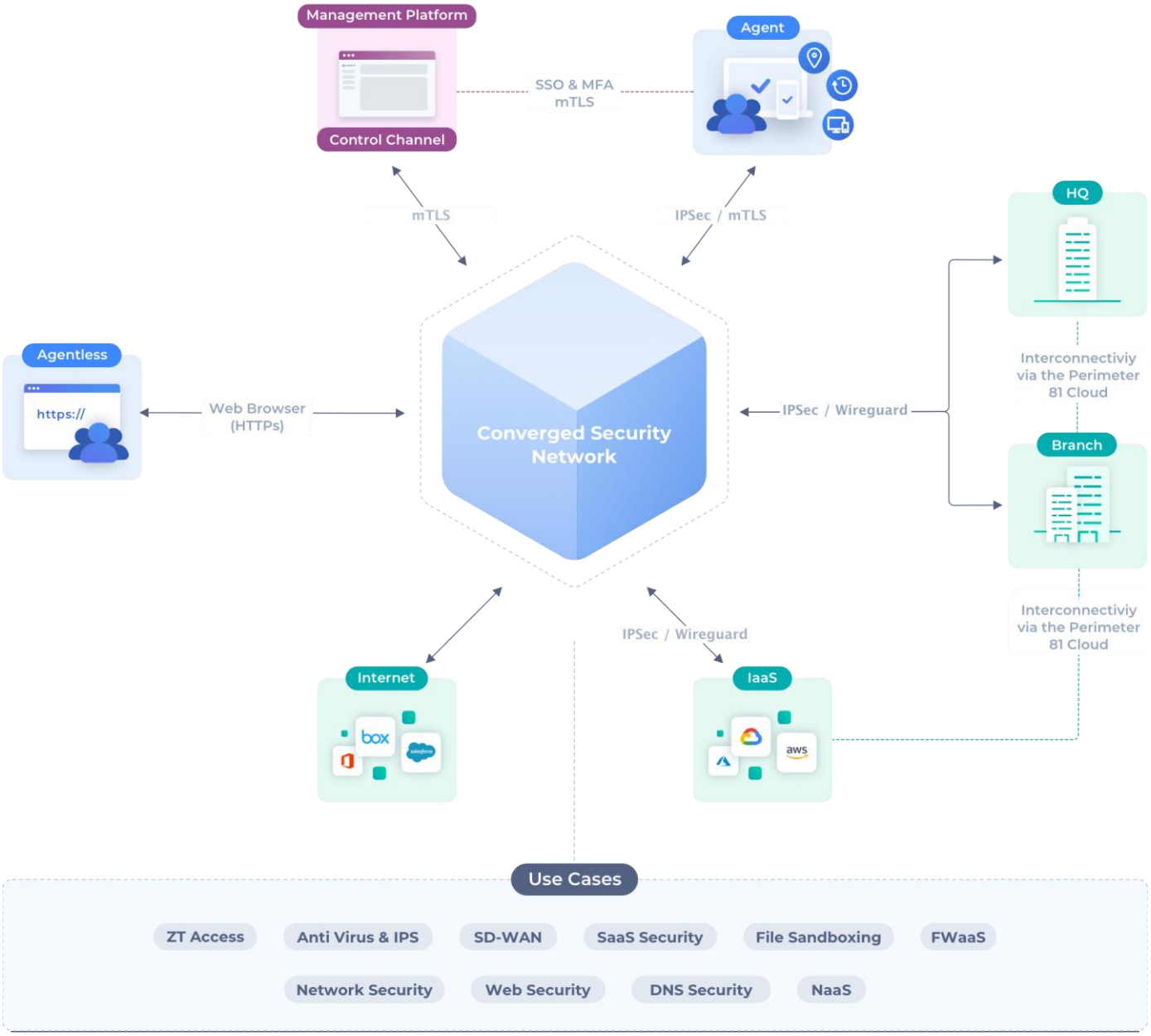
Al proporcionar protección de confianza cero de las sesiones de los usuarios de manera transparente y constante dentro y fuera de la red empresarial, las soluciones SASE proporcionarán cifrado de extremo a extremo, así como servicios de protección de aplicaciones web y API (WAAP). Usando Zero Trust Network Access, las soluciones SASE también extenderán la protección a los dispositivos terminales para la protección de la red Wi-Fi pública para proteger a los trabajadores remotos.

El uso de controles de políticas SASE consistentes permitirá la inspección de contenido para la identificación de datos confidenciales o malware "a la velocidad de la línea" según el usuario y el dispositivo en cualquier red o recurso en la nube, a nivel mundial. Además, los controles de políticas permiten puntos de cumplimiento distribuidos cerca de los recursos de la nube y los dispositivos de los usuarios para la toma de decisiones locales donde sea necesario.

Por último, SASE puede aumentar la eficacia del personal de seguridad de red y de TI al eliminar la necesidad y el tiempo de configurar la infraestructura física, lo que les permite centrarse en los requisitos de acceso a aplicaciones, cumplimiento y negoc

Enfoque SASE

La plataforma SASE combina funciones de red y seguridad en una solución de servicio de seguridad de red unificada. Las ofertas nativas de la nube se incluyen en la red SASE y las soluciones de seguridad de punto final administradas y entregadas a través de la plataforma Perimeter81 para brindar administración de políticas y redes centradas en el usuario para organizaciones de todos los tamaños.



La red en la nube, multirregional y multiusuario proporciona un conjunto completo de capacidades de red segura que incluye seguridad SaaS para Office 365, Google Drive y Dropbox, así como un cortafuegos como servicio (FaaS) para proteger las redes centradas en el sitio de una organización de posibles amenazas, mientras se implementan las funciones de seguridad modernas de un cortafuegos de próxima generación.

Cloud Sandboxing analiza archivos desconocidos en busca de exploits de día cero y amenazas persistentes avanzadas tanto dentro como fuera de la red, y DNS Security bloquea automáticamente los dominios maliciosos que se identifican con análisis en tiempo real con inteligencia de amenazas global. Esta palatforma también predice y detiene dominios maliciosos que contiene cargas útiles de malware basadas en algoritmos con aplicación instantánea.

Para una seguridad completa de los terminales, ofrece múltiples capacidades de protección de terminales, incluida la protección Wifi, protección contra malware de próxima generación y soporte para la visibilidad del tráfico cifrado. Con el cumplimiento de terminales, busca actualizaciones de funciones de seguridad, incluidos firewalls, antivirus, parches de Windows y malware para una red más segura y libre de amenazas.

Zero Trust Network Access (ZTNA) proporciona protección y aplicación de políticas al aislar las aplicaciones y segmentar el acceso a la red según los permisos, la autenticación y la verificación del usuario. La solución integral de perímetro definido por software (SDP) de la plataforma ofrece seguridad de migración a la nube simple, acceso sin privilegios mínimos a los recursos y acceso seguro a entornos en la nube, incluidos IaaS y PaaS.

EuskoData
Soluciones Tecnológicas

Contáctenos

www.euskodata.com 943 317 301

Solicite una demostración gratuita