paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Los 10 preceptos de una solución de servidor SASE eficaz

Contenido

Introducción

La pandemia de COVID-19 ha traído consigo grandes cambios, y ningún negocio funciona como antes ni volverá a hacerlo. Ante el gran aumento del número de teletrabajadores que necesitan acceder desde casa a los servicios, las aplicaciones y los datos empresariales, las organizaciones han tenido que transformar sus redes y tratar de garantizar una conectividad ininterrumpida y segura.

Incluso antes de iniciarse la crisis sanitaria, el uso de tecnologías obsoletas ya complicaba muchísimo la gestión de distintos tipos de tráfico y de un sinfín de amenazas en constante evolución. Las necesidades de las organizaciones habían cambiado y, para satisfacerlas, fue preciso adoptar distintos productos independientes, como cortafuegos, puertas de enlace web seguras, agentes de seguridad de acceso a la nube y redes de área extensa definida por software (SWG, CASB y SD-WAN, respectivamente, por sus siglas en inglés). La pandemia empeoró aún más la situación, ya que, en todo el mundo, las empresas tuvieron que ingeniárselas para implantar el teletrabajo en poco tiempo, pero con las garantías de privacidad y seguridad necesarias.

El concepto de servidor perimetral de acceso seguro (SASE, por sus siglas en inglés) se remonta al año 2018. Lo acuñó Gartner para referirse a una solución que brinda servicios de seguridad y conectividad en red desde la nube para ayudar a las organizaciones a adoptar la tecnología en la nube y la movilidad a partir de la típica arquitectura en la nube. Una solución de este tipo debe ofrecer servicios de seguridad coherentes y acceso a todo tipo de aplicaciones en la nube —ya se alojen en la nube pública o privada o funcionen en régimen de software como servicio (SaaS, por sus siglas en inglés)— a través de un marco común.

Prescindir de varios productos independientes y adoptar una única solución SASE basada en la nube ayuda a las organizaciones a reducir la complejidad, ampliar con rapidez el número de sucursales o trabajadores remotos y garantizar una seguridad coherente estén donde estén los usuarios, al tiempo que ahorran una cantidad sustancial en recursos técnicos, humanos y financieros.

Este libro electrónico le ayudará a entender los 10 preceptos de un servidor SASE eficaz.

Precepto 1: Red de área extensa definida por software

LO QUE NO ESTÁ FUNCIONANDO

Las empresas han apostado por las redes de área extensa definidas por software (SD-WAN) para conectar sus sucursales a la red corporativa y proporcionar salida directa a Internet en cada sitio («Local Internet Breakout») como alternativa a las costosas conexiones de conmutación de etiquetas multiprotocolo (MPLS, por sus siglas en inglés). Sin embargo, las soluciones SD-WAN obsoletas plantean numerosas dificultades, ya que introducen sin más el modelo tradicional de enrutamiento de paquetes en las empresas listas para la nube. Además, carecen de escalabilidad y, cuando hacen falta servicios para las sucursales (por ejemplo, para mejorar la conectividad o la visibilidad), obligan a incluirlos a modo de añadido.

LA PROPUESTA DE SASE

En una solución SASE, la arquitectura de las sucursales está totalmente basada en la nube. Todos los servicios que las organizaciones desean poner a disposición de las sucursales, incluidos los de seguridad y conectividad, se pueden prestar desde la nube, lo que simplifica la gestión de la WAN y mejora la rentabilidad de la inversión.

CONCLUSIÓN PRINCIPAL

Si lo que busca es simplificar sus redes SD-WAN, plantéese adoptar una solución autónoma y alojada en la nube, como un servidor perimetral de acceso seguro (SASE). Una solución SD-WAN que no se base en paquetes y esté definida por aplicaciones mejorará la visibilidad de estas últimas y también su rendimiento, en virtud de los acuerdos de nivel de servicio aplicables a la nube, el software como servicio (SaaS) o las comunicaciones unificadas como servicio (UCaaS, por sus siglas en inglés). Las soluciones SASE son fruto de la convergencia de la tecnología de red y de seguridad. Por tanto, para ser eficaces, deben aunar la tecnología SD-WAN con políticas coherentes que se integren en una plataforma cohesionada: lo opuesto a añadir productos independientes de distintos proveedores.

«En 2024, más del 60 % de los clientes que utilizan soluciones de red de área extensa definida por software (SD-WAN) habrán implementado una arquitectura de servidor perimetral de acceso seguro (SASE). En 2020, este porcentaje era del 35 % aproximadamente».

Cuadrante Mágico de Gartner de 2020 para las infraestructuras WAN perimetrales

Precepto 2: Acceso Zero Trust (confianza cero) a la red

LO QUE NO ESTÁ FUNCIONANDO

Las empresas siguen careciendo de las medidas de defensa y políticas de seguridad necesarias para proteger a sus usuarios y datos. El acceso Zero Trust (confianza cero) a la red (ZTNA, por sus siglas en inglés) obliga a los usuarios que quieran conectarse a una aplicación a autenticarse a través de una puerta de enlace antes de poder acceder. Así, los administradores de seguridad disfrutan de la capacidad para identificar a los usuarios y crear políticas que restrinjan el acceso, minimicen la pérdida de datos y mitiguen rápidamente cualquier posible amenaza.

Muchos productos ZTNA están basados en arquitecturas de perímetro definido por software (SDP, por sus siglas en inglés) que, al no inspeccionar el contenido, crean una discrepancia en los tipos de protección de que dispone cada aplicación. En términos de protección coherente, la organización debe incorporar controles adicionales al modelo ZTNA y establecer un sistema de inspección que opere en todo el tráfico que circula por todas las aplicaciones.

LA PROPUESTA DE SASE

Las soluciones SASE se basan en los principios clave del acceso ZTNA, que también se aplican al resto de los servicios que ofrecen. La identificación de usuarios, dispositivos y aplicaciones, al margen del lugar desde el que se conecten, simplifica la creación y gestión de políticas. SASE elimina la complejidad de conectarse a una puerta de enlace incorporando los servicios de red a un solo marco de nube unificado.

CONCLUSIÓN PRINCIPAL

Además de proteger las aplicaciones, una solución SASE adecuada debe incorporar los principios del acceso ZTNA para proporcionar otros servicios de seguridad que garanticen la aplicación coherente de las políticas de prevención de pérdida de datos (DLP, por sus siglas en inglés) y de prevención de amenazas. Aunque los controles de acceso son útiles para establecer la identidad del usuario, hay que asegurarse de que este no se comporta ni actúa de maneras que puedan poner en peligro a la organización, para lo cual se necesitan otros controles de seguridad. Y estos mismos controles deberán aplicarse, además, para regular el acceso a todas las aplicaciones.

«Muchas empresas no controlan de ninguna manera qué aplicaciones utilizan sus empleados. Solo el 62 % tienen políticas de uso aceptable (AUP, por sus siglas en inglés) que prohíban la instalación de aplicaciones no autorizadas».

Informe Mobile Security Index 2020 de Verizon (disponible en inglés)

Precepto 3: Agente de seguridad de acceso a la nube

LO QUE NO ESTÁ FUNCIONANDO

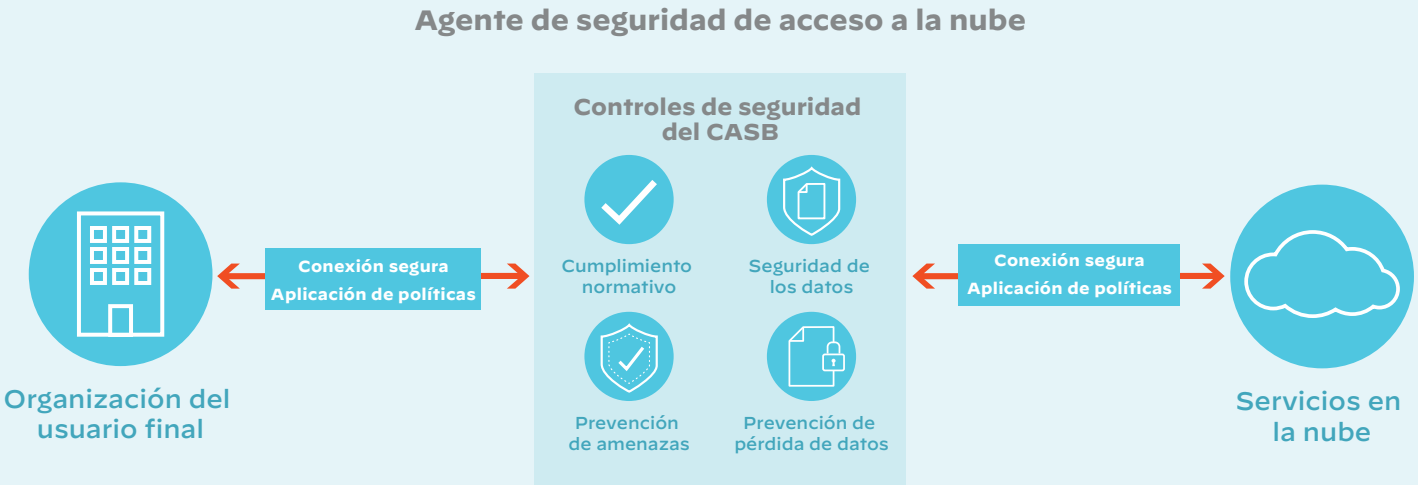
Muchas organizaciones dependen de agentes de seguridad de acceso a la nube, o CASB, para saber dónde residen sus datos (por ejemplo, en las aplicaciones SaaS), aplicar las políticas corporativas al acceso de los usuarios y proteger sus datos de los hackers. Los CASB son puntos de aplicación de políticas de seguridad basados en la nube que ofrecen una puerta de enlace tanto para su proveedor de SaaS como para sus empleados.

LA PROPUESTA DE SASE

Si quiere que los responsables de la seguridad de las aplicaciones (sean del tipo que sean) puedan gestionarlo todo desde una única plataforma, necesita una solución SASE que incluya un agente de seguridad de acceso a la nube. Una solución SASE le ayuda a entender qué aplicaciones SaaS se están utilizando y adónde se están enviando los datos, con independencia de la ubicación de los usuarios.

CONCLUSIÓN PRINCIPAL

Su solución SASE debería incorporar controles de SaaS tanto en línea como basados en API para gobernar, controlar el acceso y proteger los datos. Esta combinación de seguridad en línea y basada en API con controles contextuales — que también recibe el nombre de CASB multimodo— mejora muchísimo la visibilidad, la gestión, la seguridad y la protección de día cero frente a las amenazas emergentes.



Precepto 4: Cortafuegos como servicio

LO QUE NO ESTÁ FUNCIONANDO

Dondequiera que haya aplicaciones o usuarios (en la sede central, las sucursales, los centros de datos o la nube), se necesitan cortafuegos físicos o virtuales que los protejan. El problema es que, ahora que hay tantas aplicaciones y que cada vez más usuarios acceden a ellas de forma remota desde cualquier lugar, a las organizaciones no les resulta fácil gestionar decenas o cientos de cortafuegos. El cortafuegos como servicio (FWaaS, por sus siglas en inglés) es un método de implementación que convierte el cortafuegos en un servicio basado en la nube. Los mejores cortafuegos de este tipo incluyen las mismas funciones que los de nueva generación.

LA PROPUESTA DE SASE

Una solución SASE incorpora cortafuegos FWaaS en su plataforma unificada y proporciona exactamente los mismos servicios que los cortafuegos de nueva generación, solo que como un servicio en la nube. Gracias a la combinación del modelo de servicio FWaaS con un marco SASE, las organizaciones pueden gestionar fácilmente sus implementaciones desde una única plataforma.

CONCLUSIÓN PRINCIPAL

Una solución SASE debería brindar funciones FWaaS que, mediante la implementación de políticas de seguridad de la red en la nube, proporcionen una protección equivalente a la de un cortafuegos de nueva generación. Es importante que se asegure de que la solución SASE elegida no solo brinde un servicio básico de bloqueo de puertos o la seguridad mínima de un cortafuegos. Necesita tanto las funciones que ofrece un cortafuegos de nueva generación como las que se consiguen con la seguridad basada en la nube, como los servicios de prevención de amenazas y la seguridad DNS.

«En 2025, el 30 % de las nuevas implementaciones de cortafuegos para entornos distribuidos de sucursales se habrán pasado al modelo de cortafuegos como servicio, un porcentaje que en 2020 ni siquiera llegaba al 5 %».

Cuadrante Mágico de Gartner de 2020 para cortafuegos de red

Precepto 5: Puerta de enlace web segura

LO QUE NO ESTÁ FUNCIONANDO

Las organizaciones recurren a la tecnología de puertas de enlace web seguras (SWG) para proteger a los usuarios y dispositivos del acceso a sitios web malignos o inapropiados. La tecnología SWG puede combinarse con la seguridad DNS para bloquear contenido inapropiado (p. ej., pornografía o juegos y apuestas) o sitios web a los que las empresas simplemente no quieren que los usuarios accedan mientras están trabajando, como los servicios de transmisión de contenido tipo Netflix. Lo malo es que, como las SWG suelen ser dispositivos o servicios independientes, suelen aplicarse políticas distintas dependiendo de dónde estén los usuarios (dentro o fuera de la oficina).

LA PROPUESTA DE SASE

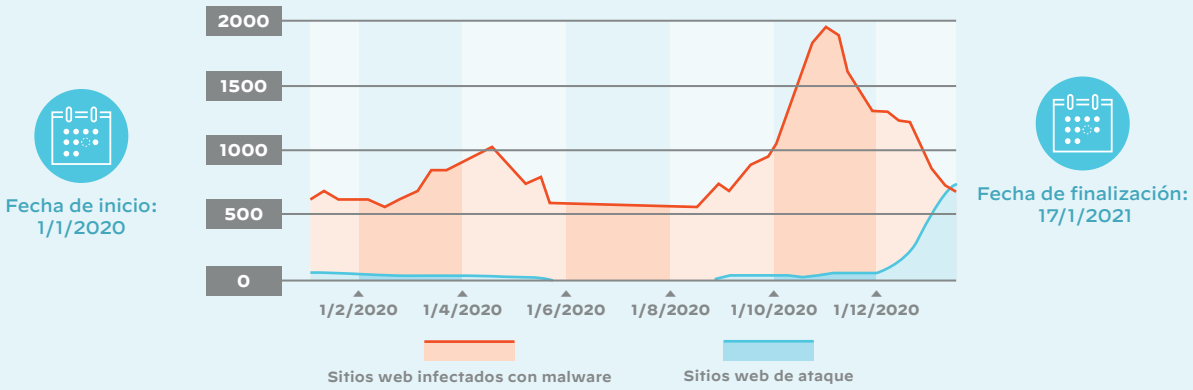
SWG no es más que uno de los muchos servicios de seguridad que una buena solución SASE debería ofrecer. Esté donde esté el usuario, una SWG en la nube que forme parte de una plataforma SASE ofrece una visibilidad y un control totales del conjunto de la red, lo que garantiza el uso seguro de las aplicaciones basadas en la nube y de otros servicios web. Conforme las organizaciones aumentan de tamaño y añaden cada vez más usuarios remotos, las SWG de la solución SASE, alojadas en la nube, se adaptan automáticamente a este crecimiento.

CONCLUSIÓN PRINCIPAL

Una solución SASE incluye los mismos servicios de seguridad que una SWG tradicional, lo que permite a las organizaciones controlar el acceso a la web y aplicar políticas de seguridad que protejan a los usuarios de los sitios web hostiles o de contenido inapropiado. Si el objetivo es adoptar una arquitectura SASE, utilizar una SWG y combinarla con funciones de seguridad DNS y un proxy explícito puede ser un primer paso bastante sencillo.

Informe de transparencia de Google: sitios web con malware, de enero de 2020 a enero de 2021

https://transparencyreport.google.com/safe-browsing/overview?hl=es



Precepto 6: Supervisión de la experiencia digital

LO QUE NO ESTÁ FUNCIONANDO

La experiencia del usuario es crucial para la satisfacción y la productividad de los empleados. Ahora que el teletrabajo se ha vuelto habitual, ofrecer a los empleados una experiencia digital es imprescindible. Los equipos de TI no tienen una buena visibilidad de la red ni de los dispositivos y, cuando hay algún problema, es frecuente que solo logren resolverlo tras largas sesiones de trabajo manual.

LA PROPUESTA DE SASE

La supervisión autónoma de la experiencia digital (ADEM, por sus siglas en inglés) brinda la visibilidad integral y la información útil necesarias para que el usuario disfrute de una experiencia digital impecable. Si, además, se integra en una solución SASE, ADEM proporciona información útil sobre segmentos específicos a lo largo de todo el proceso de prestación del servicio. Gracias a esta característica, es posible analizar el tráfico real y sintético, lo que permite a las organizaciones corregir de manera autónoma los problemas relacionados con la experiencia digital en cuanto surgen.

CONCLUSIÓN PRINCIPAL

El teletrabajo ha puesto de relieve la necesidad de optimizar la experiencia del usuario. Para que su solución SASE beneficie tanto a quien la usa como al equipo de TI, debería contar con un sistema ADEM que ofrezca una visibilidad total, corrección automatizada e información de rendimiento detallada sobre los endpoints, la red inalámbrica, las rutas de red y las aplicaciones.

«Los responsables de TI tendrán que informar de distintos parámetros relacionados con la experiencia del usuario para el 70 % de las iniciativas tecnológicas que acometan sus empresas en 2025. Según datos de Gartner, en 2019 solo tuvieron que hacerlo para el 15 %».

Market Guide for Digital Experience Monitoring (Gartner, 2020; disponible en inglés)

Precepto 7: Prevención de amenazas

LO QUE NO ESTÁ FUNCIONANDO

En un mundo como el actual, en el que hay brechas de seguridad a pequeña y gran escala y todos los días nos despertamos con un nuevo ataque por ransomware, la prevención de amenazas es fundamental para proteger tanto al personal como los datos de la organización. Existen en el mercado diversas herramientas de prevención —desde software antimalware y de prevención de intrusiones hasta tecnologías de bloqueo de archivos— para que las organizaciones puedan detener las amenazas por todos los medios. Sin embargo, estos productos requieren soluciones independientes que, además de dificultar la gestión y la integración, suelen tardar demasiado en detectar las amenazas y responder a ellas.

LA PROPUESTA DE SASE

En una solución SASE, todos estos productos y servicios independientes se integrarían en una única plataforma en la nube para facilitarle la gestión y la vigilancia de todas las amenazas y vulnerabilidades que afectan a sus entornos de red y en la nube. También es aconsejable que la solución SASE incorpore funciones de aprendizaje automático. Así, será más fácil combatir otras amenazas desconocidas casi en tiempo real y tener más controlados todos dispositivos (incluidos los dispositivos IdC nunca vistos), así como protegerlos mejor.

CONCLUSIÓN PRINCIPAL

Detener los exploits y el malware mediante el uso de los datos más recientes de inteligencia sobre amenazas es decisivo para proteger tanto a sus empleados como su información. Su solución SASE debería incorporar herramientas de prevención de amenazas en su marco para que pueda bloquearlas rápidamente. El aprendizaje automático integrado le ayudará a prevenir al instante las amenazas desconocidas basadas en archivos y en la web, y la recomendación de políticas automatizada ahorra tiempo y reduce la posibilidad de errores humanos.

Por qué resulta tan complicado contar con un sistema de detección y respuesta a amenazas eficaz hoy en día

Resultados de la encuesta maestra de ESG:
***The Threat Detection and Response Landscape* (disponible en inglés)**

Precepto 8: Internet de las cosas

LO QUE NO ESTÁ FUNCIONANDO

Pese a que los dispositivos de Internet de las cosas (IdC) se conectan a la red de la organización, es habitual que estén sin gestionar. Esto genera lagunas de seguridad, ya que a menudo se trata de dispositivos con vulnerabilidades que los propios usuarios se encargan de actualizar y que, muchas veces, se conectan a recursos que escapan al control de los equipos de TI. Implementar costosos sensores o dispositivos que mejoren la seguridad de IdC puede resolver parcialmente el problema, pero es una fuente de preocupaciones y no resulta eficiente desde el punto de vista operativo.

LA PROPUESTA DE SASE

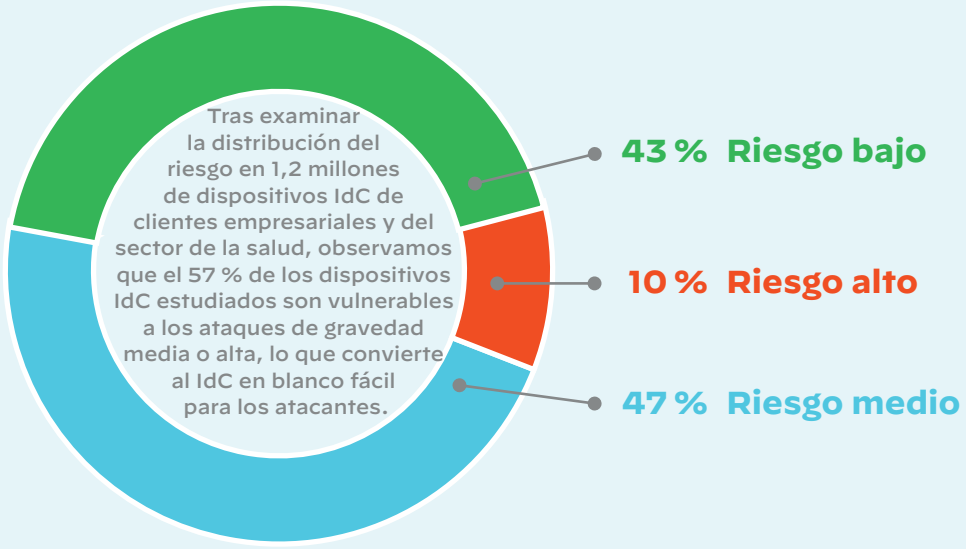
Con SASE, es vital que la seguridad de IdC esté integrada en la plataforma, de manera que la nube garantice la seguridad de las sucursales, los sitios remotos y los empleados que teletrabajan. Gracias a la nube, SASE detecta los dispositivos con precisión, haciéndolos totalmente visibles, y aplica políticas que protegen toda la red para que no sea necesario utilizar otras soluciones de seguridad de IdC.

CONCLUSIÓN PRINCIPAL

La tecnología de siempre se está modernizando. Ahora, un termostato o un sistema de iluminación inteligentes ya no nos sorprenden, y los dispositivos IdC también están ganando terreno en el ámbito empresarial. Los ordenadores portátiles y los teléfonos o relojes inteligentes ya no son los únicos dispositivos que hay que proteger en la red corporativa. Una buena solución SASE debe incluir funciones de aprendizaje automático e IA que den más autonomía a las organizaciones y les permitan detectar y corregir las amenazas con rapidez.

«El 57 % de los dispositivos IdC son vulnerables a los ataques de gravedad media o alta, lo que convierte al IdC en blanco fácil para los atacantes».

2020 Unit 42 IoT Threat Report (disponible en inglés), Palo Alto Networks



Precepto 9: Prevención de pérdida de datos

LO QUE NO ESTÁ FUNCIONANDO

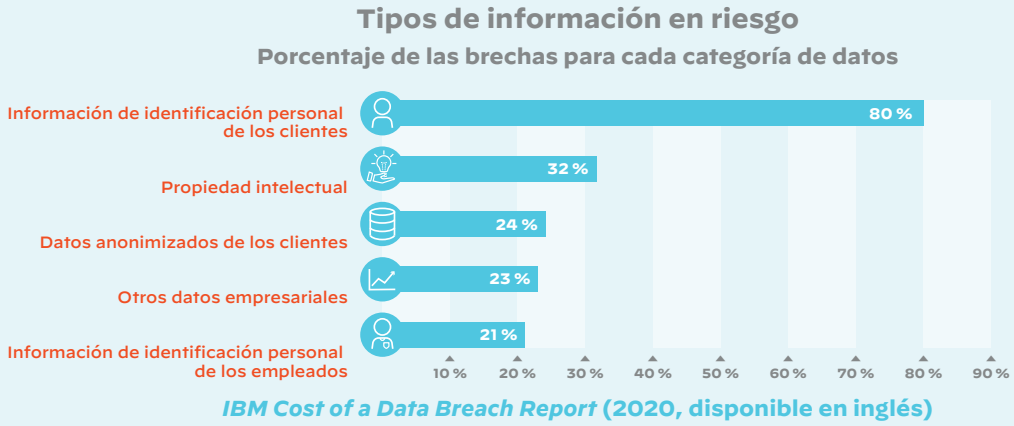
Las herramientas de prevención de pérdida de datos, o DLP, protegen los datos confidenciales y evitan su pérdida, robo o uso indebido. DLP es una solución compuesta que supervisa los datos, tanto los alojados en los entornos en los que está implementada (como las redes, los endpoints y las nubes) como a través de sus puntos de salida. También alerta a quien corresponda cada vez que se infringen las políticas. Debido a los requisitos fijados por la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA), la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) y el Reglamento General de Protección de Datos (RGPD), entre otras normativas, DLP es una condición sine qua non para garantizar la seguridad de los datos y el cumplimiento normativo. Las soluciones de DLP heredadas se basan en tecnologías básicas obsoletas que originalmente estaban pensadas para los perímetros locales y, sucesivamente, se fueron ampliando y adaptando a las aplicaciones en la nube. Los productos de DLP, que incluyen infinidad de funciones, políticas inconexas, configuraciones y soluciones alternativas, se han vuelto muy complejos, difíciles de implementar a gran escala y demasiado caros. La transformación digital y los nuevos modelos de uso de datos demandan una manera de abordar la protección de datos más actualizada.

LA PROPUESTA DE SASE

Con la metodología SASE, la tecnología DLP se convierte en una solución basada en la nube orientada a los datos en sí, estén donde estén. La ubicación es lo de menos: las políticas aplicadas a los datos confidenciales, en reposo, en transmisión y en uso son siempre las mismas. En la arquitectura SASE, DLP deja de ser una solución independiente y pasa a integrarse en los puntos de control que la organización ya utiliza, por lo que ya no es necesario implementar y mantener varias herramientas. Con SASE, las organizaciones pueden por fin disfrutar de una solución de protección de datos integral que, además de estar basada en una arquitectura escalable y sencilla, tiene acceso al tráfico global para poder aprovechar las ventajas del aprendizaje automático.

CONCLUSIÓN PRINCIPAL

DLP es una herramienta necesaria para proteger datos confidenciales y garantizar el cumplimiento normativo en todos los sistemas de una organización. Con este fin, la solución SASE debe incluir esta función esencial. Con SASE, DLP es un servicio integrado basado en la nube que sirve para identificar, supervisar y proteger los datos confidenciales de manera precisa y sistemática en cualquier punto de las redes, las nubes y los usuarios.



IBM Cost of a Data Breach Report (2020, disponible en inglés)

Precepto 10: Capacidad de ampliación de la plataforma

LO QUE NO ESTÁ FUNCIONANDO

Aunque cada vez más organizaciones utilicen la nube, añadir e integrar servicios en la nube de distintos proveedores puede resultar complejo. Es difícil encontrar una herramienta que lo resuelva todo, así que es importante elegir productos que se comuniquen entre sí y ofrezcan una protección sin fisuras. Lamentablemente, hay pocas soluciones en la nube diseñadas para integrarse con fluidez con servicios de terceros, y los proveedores no siempre se prestan a colaborar con quien les pide ayuda.

LA PROPUESTA DE SASE

Una buena solución SASE debe integrarse fácilmente con servicios de terceros mediante una plataforma que, además, simplifique el trabajo de los administradores. Con una plataforma de este tipo, las organizaciones pueden añadir rápidamente los servicios que necesitan y contar con el respaldo total de su proveedor SASE.

CONCLUSIÓN PRINCIPAL

Con una solución SASE ampliable, las organizaciones pueden ir añadiendo servicios a la plataforma con facilidad y utilizarlos como prefieran. Este método les permite ampliar sus funciones y capacidades según sus necesidades, ayudándose de los servicios de terceros que ya usan y sin el obstáculo que supone la falta de integración entre soluciones independientes.

«Para reducir la complejidad, los responsables de la seguridad y la gestión de riesgos deberían buscar un solo proveedor que ofrezca puertas de enlace web seguras (SWG), agentes de seguridad de acceso a la nube (CASB), seguridad DNS, acceso Zero Trust (confianza cero) a la red (ZTNA) y funciones de aislamiento remoto del navegador».

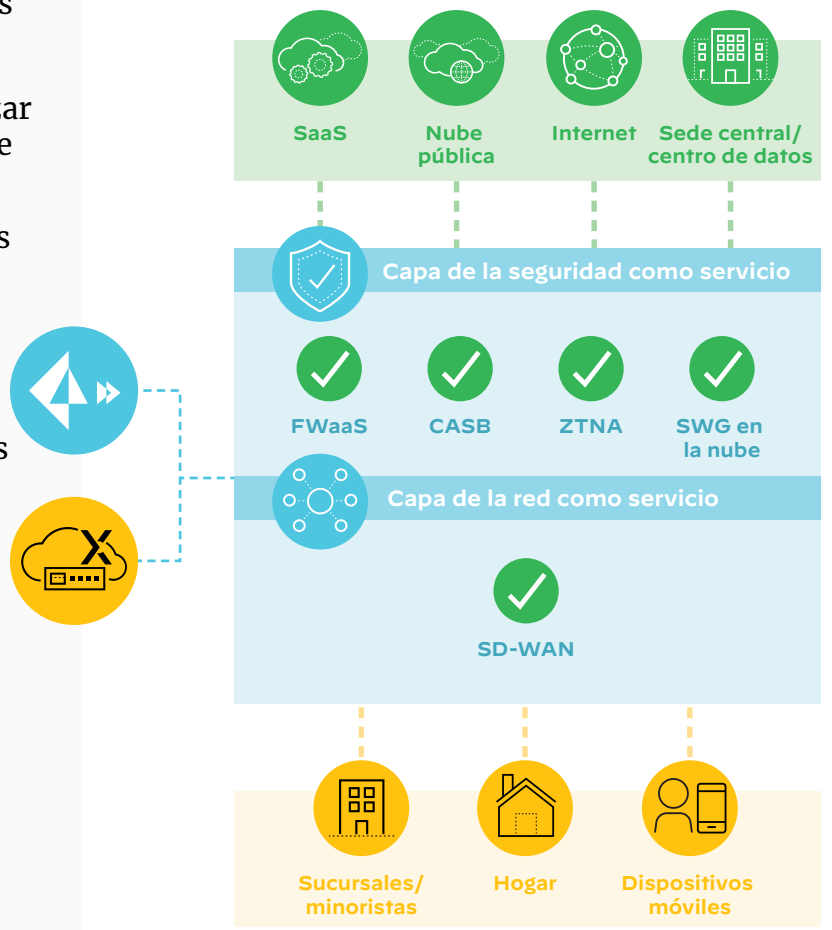
The Future of Network Security Is in the Cloud (Gartner, 2019; disponible en inglés)

Cómo puede ayudar Palo Alto Networks

Gracias a sus productos Prisma® Access y CloudGenix® SD-WAN, Palo Alto Networks ofrece la solución SASE más completa del sector. Prisma Access previene los ciberataques con un modelo de seguridad basado en la nube y protege de forma coherente todo el tráfico, en todos los puertos y desde todas las aplicaciones. CloudGenix SD-WAN, por su parte, es la primera solución SD-WAN de nueva generación del sector que utiliza la automatización y el aprendizaje automático para garantizar una experiencia del usuario excepcional y simplificar las operaciones de seguridad y de red.

Integrar en profundidad ambas soluciones permite a las organizaciones adoptar sin miedo el teletrabajo, ya que tendrán la certeza de estar satisfaciendo las necesidades de los usuarios remotos y las sucursales en materia de seguridad y conectividad. Cuando se utilizan productos independientes, lo habitual es superponer distintas tecnologías, cada cual con un fin específico. Prisma Access, por el contrario, se sirve de una infraestructura común basada en la nube que proporciona distintos tipos de servicios de seguridad y que, junto con CloudGenix SD-WAN, ofrece una solución completa con diferentes servicios de red. Además, los clientes pueden beneficiarse de la inteligencia sobre amenazas integral basada en datos de amenazas automatizadas de Palo Alto Networks y cientos de fuentes de terceros.

Prisma Access y CloudGenix SD-WAN: el SASE más completo del sector



Conclusión

Ante el auge imparable de la nube y el teletrabajo, haría bien en adoptar una solución SASE completa que le ofrezca la conectividad que necesita y proteja bien sus redes. Las principales tres ventajas estratégicas de las que se beneficiará su empresa con una solución de servidor perimetral de acceso seguro son las siguientes:

1

GESTIÓN Y OPERACIONES SIMPLIFICADAS

- Preste todas las funciones de red (y las relacionadas con la seguridad de esta) a través de un solo servicio en la nube que se gestiona desde una única consola.
- Automatice la implementación en las sucursales y la gestión continua.
- El aprendizaje automático y las metodologías de la ciencia de datos simplifican las operaciones de la red y reducen las incidencias relacionadas con los problemas de esta.

2

RENDIMIENTO Y ESCALA ILIMITADOS

- Benefíciese de una arquitectura nativa en la nube sumamente escalable y adecuada para redes globales de alto rendimiento con más de 100 ubicaciones.
- Preste servicios a las sucursales desde la nube, con un retorno de la inversión de hasta el 243 % y una gestión de la WAN más sencilla.
- Obtenga inteligencia definida por aplicaciones de capa 7 y úsela para tomar decisiones de enrutamiento, políticas y visibilidad mejor fundadas.

3

EXPERIENCIA DEL USUARIO EXCEPCIONAL

- Garantice un cumplimiento normativo y una seguridad coherentes, estén donde estén los usuarios.
- Cumpla los acuerdos de nivel de servicio de todas las aplicaciones (incluidas las SaaS, de nube o UCaaS).

En resumen, una buena solución SASE ofrece una visión global de toda su red a la vez que brinda una protección y un rendimiento superiores desde una única plataforma unificada basada en la nube.

Obtenga más información sobre los productos SASE de Palo Alto Networks:
Prisma Access • **CloudGenix SD-WAN**

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam, Países Bajos
Tel.: +31 20 888 1883
www.paloaltonetworks.es