Por gentileza de:

netskope

Security Service Edge (SSE)

para dummies

Diseña tu TI para el futuro de la seguridad de la nube

Implementa CASB, SWG, ZTNA y firewalls desde una sola plataforma

Domina SSE como parte de una arquitectura de SASE y Zero Trust

Edición especial de Netskope

Jason Clark

Steve Riley

Acerca de Netskope

Netskope, el líder en SASE, conecta a los usuarios de forma segura y rápida directamente a internet, a cualquier aplicación y a su infraestructura desde cualquier dispositivo, dentro o fuera de la red Con CASB, SWG, firewall como servicio y ZTNA incorporados de forma nativa en una única plataforma, la plataforma Netskope Security Cloud proporciona el contexto más detallado (a través de una tecnología patentada) para permitir el acceso condicional y el conocimiento del usuario, al tiempo que aplica los principios de Zero Trust a la protección de datos y la prevención de amenazas en cualquier lugar. A diferencia de otros que obligan a hacer concesiones entre la seguridad y la red, la nube privada de seguridad global de Netskope proporciona capacidades de procesamiento completas en el borde.

Netskope ofrece rapidez integral, se centra en los datos y ofrece seguridad inteligente en la nube, al tiempo que habilita una buena ciudadanía digital y permite un coste total de propiedad más bajo. Más información en www.netskope.com.

Nos gustaría mostrar nuestro agradecimiento a una serie de personas que han hecho posible este libro:

De Netskope: Amanda Anderson, Lauren Baker, Chad Berndtson, Jeff Brainard, Tim Chiu, Tom Clare, Catie Halliday, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Sasi Murthy, Shamla Naidoo, Lauren Polito, Zoe Revis, James Robinson, James Yokota, Svetlana Rubin

De Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Security Service Edge (SSE)

para dummies®

Security Service Edge (SSE)

Edición especial de Netskope

por Jason Clark y Steve Riley

para dummies®

Security Service Edge (SSE) Para Dummies®, edición especial de Netskope

Una publicación de
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Para obtener información general sobre nuestros productos y servicios, o sobre cómo crear un libro *Para Dummies* personalizado para tu empresa u organización, ponte en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono +1 (877) 409 4177, ponte en contacto con info@dummies.biz, o visita www.wiley.com/go/custompub. Para obtener información sobre licencias de la marca *Para Dummies* para productos o servicios, ponte en contacto con BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-89738-5 (pbk); ISBN 978-1-119-89739-2 (ebk)

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora del proyecto:
Elizabeth Kuball

Editora de adquisiciones:
Ashley Coffey

Director editorial jefe: Rev Mengle

Representante de expansión comercial: Jeremith Coward

Editor de producción:
Tamilmani Varadharaj

Colaboración especial: Nicole Sholly

Índice

Introducción

La transición empresarial general hacia la nube se está produciendo mucho más rápido de lo que muchos expertos habían previsto. Esta velocidad ha hecho que la mayoría de las empresas dependan de plataformas de seguridad que se construyeron para un mundo ya desaparecido en el que dominaban los centros de datos locales. La pandemia de COVID-19 aceleró y complicó aún más la situación, y añadió presión sobre los directores de seguridad de la información que son los responsables de proteger al personal que trabaja desde su domicilio y que quizá nunca vuelva del todo a la oficina.

La buena noticia es que el servicio de acceso seguro en el borde (SASE), un marco de arquitectura de seguridad, apunta a un cambio hacia una solución basada en la nube que ofrece la protección que toda empresa necesita, independientemente de dónde se encuentren sus empleados. Pero una noticia aún mejor es que el servicio de seguridad en el borde (SSE), que es el conjunto esencial de servicios de seguridad en SASE, ofrece las capacidades necesarias para implementar servicios de seguridad con el fin de proteger a los trabajadores remotos, la tecnología basada en la nube y las aplicaciones y la infraestructura que existen a nivel local.

SASE es el marco. SSE es un conjunto de servicios que puedes adquirir actualmente. En este libro, explicamos qué es SSE y analizamos sus fundamentos, que se derivan de ideas innovadoras como Zero Trust, seguridad adaptativa basada en el contexto, y novedosos enfoques para el diseño de la red. En el libro veremos también cómo los servicios conocidos se vinculan dentro del SSE junto a tecnologías nuevas y avanzadas que pueden mejorar la seguridad de forma considerable.

Acerca de este libro

Ha llegado el momento de rediseñar el panorama de la seguridad actual. Aprender qué es el SSE ayudará al personal comercial y de seguridad a prepararse para dar los pasos necesarios que conviertan la seguridad de la empresa, que actualmente se encuentra atascada, en un amplificador y habilitador de la transformación digital. El libro prepara el terreno con explicaciones de SASE y SSE y, a continuación, ofrece una hoja de ruta que te enseñará cómo hacer realidad esta nueva seguridad. Para usar la nube, todas las empresas tienen que transformar su seguridad. En este libro, encontrarás consejos sobre cómo puedes prepararte.

Algunas suposiciones obvias

Ya sabes de qué va esto de internet y la seguridad. Sabes que el modelo de seguridad tradicional que usamos todos está ya al límite. También sabes que la nube sirve para aumentar la productividad, pero también es un lugar peligroso en el que las credenciales y los datos tanto de las personas como de las empresas sufren ataques. Por último, te interesa mitigar el reto que todo esto supone para tu empresa, empleados, accionistas, clientes y socios de negocio usando las potentes capacidades que ofrecen SASE y SSE.

Iconos utilizados en este libro

En todo el libro, utilizamos iconos para llamar la atención sobre información importante.

CONSEJO

El icono «Consejo» te ofrece atajos y otra información que puede facilitarte la vida.

RECUERDA

El icono «Recuerda» te ofrece información que es especialmente importante conocer.

ADVERTENCIA

Presta atención a cualquier cosa que lleve el icono «Advertencia» para ahorrarte algún que otro dolor de cabeza.

Más allá del libro

Para obtener más información sobre las soluciones de Netskope, visita `www.netskope.com`. Si quieres conocer más a fondo el servicio de seguridad en el borde (SSE), visita `www.netskope.com/security-defined/security-service-edge-sse`.

EN ESTE CAPÍTULO

- Analizamos el futuro de la seguridad
- Explicamos cómo afectan a la seguridad las transformaciones digitales
- Descubrimos cómo alcanzar el nirvana de la seguridad que todos queremos

Capítulo 1
El contexto y la integración como impulsores de la transformación de la seguridad

Las organizaciones han comenzado a usar las aplicaciones en la nube para aprovechar los claros beneficios empresariales en cuanto a velocidad, eficiencia e información que proporciona la nube. Para que los datos, las personas y las aplicaciones en la nube estén realmente protegidos, la seguridad tiene que ser algo más que las simples decisiones binarias de aceptar/denegar que se utilizaban cuando la red era lo más importante y la mayoría de los trabajadores estaban en un mismo lugar. Hay que hacer que la seguridad sea más inteligente con el uso de un contexto detallado, de forma que pueda ofrecer la protección adecuada a tu organización independientemente de dónde se encuentren tus trabajadores. La seguridad debe seguir a los datos allá donde vayan, y debe ser fácil de aplicar para no ralentizar el funcionamiento de la empresa.

El futuro de la seguridad

Este es el momento para entrar a fondo en la seguridad. El poder y la calidad de la tecnología en torno a la ciberseguridad avanza a una velocidad asombrosa. Los profesionales de la seguridad nunca han tenido que enfrentarse a tantos cambios tan rápidamente, ni nunca han tenido una

oportunidad como la actual para convertir la seguridad en un catalizador empresarial estratégico. Los datos, las aplicaciones y los trabajadores han migrado a la nube y la seguridad debe seguir sus pasos.

Las empresas que adoptan una posición de seguridad basada en la nube para materializar la transformación digital innovarán de forma más rápida y segura que aquellas empresas cuya posición de seguridad esté arraigada en ideas que forman parte del pasado. Prevemos una nueva era en la que los profesionales de la seguridad se adelantarán finalmente a los atacantes y defenderán sus empresas a medida que se acelere la transformación digital con la ayuda de la nube.

Los esfuerzos para que los sistemas de seguridad heredados puedan funcionar en la nube no están funcionando. En un marco descrito como servicio de acceso seguro en el borde (SASE), la seguridad se está transformando para responder al lugar de trabajo híbrido basado en la nube.

ADVERTENCIA

Los mejores productos y servicios de seguridad del pasado no funcionarán en la nube. Tampoco servirá de nada acondicionar la antigua tecnología de seguridad ni decir que está «habilitada para la nube».

En lugar de esto, los proveedores de tecnología de seguridad ofrecen nuevos productos y servicios nativos de la nube para brindar protección cuando los datos se almacenan y las aplicaciones se ejecutan en una infraestructura que las empresas no controlan por sí mismas. La nueva tecnología de seguridad debe proteger no solo el *acceso* a los datos, sino también el *uso* de esos datos.

Pensar en cuatro ideas fundamentales nos ayudará a entender la seguridad lista para la nube:

- **SASE** es el marco para implementar una infraestructura convergente en la nube destinada a las funciones de red y seguridad. SASE combina conceptos como Zero Trust, SD-WAN y el servicio de seguridad en el borde (SSE) para guiarnos hacia una posición de seguridad y redes que protege y gobierna la nube y el nuevo entorno de trabajo desde cualquier lugar. Los analistas reconocen que esta nueva arquitectura proporciona seguridad integral para un mundo centrado en la nube. (Consulta *Diseño de una arquitectura SASE para Dummies* de Netskope para obtener una presentación completa).
- **SSE** es la forma en que todos los servicios de seguridad necesarios para SASE —que anteriormente eran aplicaciones, productos o servicios independientes, a menudo de distintos proveedores— se unen de una manera unificada e integrada para proporcionar mayor capacidad y eficiencia y reducir la complejidad y el coste. El SSE tiene capacidades de seguridad profundamente integradas que se reconocen entre sí, funcionan bien juntas y proceden de un único proveedor. Netskope define

además un conjunto de capacidades extendidas al que llamamos SSE propiamente dicho (consulta el capítulo 3).

- El **contexto** determina cómo se aplican las capacidades de seguridad integradas del SSE como mecanismo de control para mantener la seguridad de los datos, las aplicaciones y las personas en todo momento. El contexto, que permite comprender en profundidad *quién* es la persona, *qué* intenta hacer y *por qué* intenta hacerlo (además de cuándo, por qué y cómo), también permite aplicar políticas de seguridad adaptativas a fin de reducir el riesgo en tiempo real. Antes, «permitir» o «bloquear» eran las únicas opciones. Ahora, el contexto enriquecido admite matices de control de acceso, como «permitir, con condiciones», para ofrecer una seguridad que no afecta a la productividad. La calidad y amplitud del contexto es un factor diferenciador fundamental entre los proveedores de seguridad.
- Los principios de **Zero Trust** diferencian las políticas verdaderamente adaptables de la autenticación condicional simple basada en la familiaridad. El objetivo es algo más que limitarse a proporcionar el acceso y la autorización que cada persona necesita para llevar a cabo una tarea determinada conforme al nivel de confianza derivado de una evaluación en tiempo real de la identidad del trabajador y el método de acceso. El acceso adaptativo requiere información sobre lo que sucede *después* de iniciar sesión: señales ambientales que cambian con el tiempo, comportamiento histórico y actual, y características de los propios datos. En Netskope, consideramos que Zero Trust es el punto de partida (no hay confianza al comienzo de cada interacción) y tratamos de conseguir el objetivo de una *confianza adaptativa continua*, donde el grado de confianza es acorde con el nivel de confianza determinado y las señales ambientales.

En este libro, explicamos cómo se fusionan estos conceptos en el SSE implementado de manera eficaz para crear un nuevo nirvana de seguridad (consulta el capítulo 3). Por fin, las empresas disfrutarán de una seguridad basada en la nube con todo lo necesario para proteger a un mundo de datos y aplicaciones centrados en la nube a los que acceden trabajadores que están –y permanecerán– diseminados y, a menudo, lejos de la ubicación de la oficina central.

Forzar la transformación de la seguridad

Las explosiones en varias áreas de la transformación digital están remodelando el mundo empresarial. La transformación de la seguridad es fundamental para lograr y mantener el éxito del trabajo dedicado a la transformación digital.

RECUERDA

Las tecnologías como la nube, internet de las cosas (IoT), el aprendizaje automático/la inteligencia artificial (AA/IA) y los análisis mejoran los resultados empresariales de forma considerable. Si la seguridad no puede seguir este ritmo, ese progreso corre peligro.

- **La explosión de los datos:** para el año 2025, IDC prevé que habrá 175 zettabytes (ZB) de datos en todo el mundo (25 veces más que en 2010). Como puedes ver en los titulares de prensa, los atacantes roban los datos de las empresas con fines funestos: para venderlos, modificarlos maliciosamente o pedir rescates. Netskope Threat Labs descubrió que la nube es un patio de recreo para los atacantes; en 2021, el 68 % del *malware* llegó a través de la nube (en comparación con menos de la mitad en el no tan lejano 2020). La explosión de los datos a los que se accede desde la nube genera más objetivos para los atacantes y más dificultades para los defensores.
- **La explosión de la nube:** las empresas están adoptando infraestructura y aplicaciones basadas en la nube para obtener velocidad, flexibilidad y agilidad. Según Netskope Threat Labs, la empresa media se suscribe a más de 800 aplicaciones distintas de *software* como servicio (SaaS). Una cifra tan elevada como el 97 % de estas aplicaciones es lo que llamamos la «TI en la sombra», es decir, aplicaciones que no están administradas (y en muchos casos ni siquieran pueden ser vistas) por los equipos de TI de la empresa. Además, la configuración de seguridad predeterminada de muchas aplicaciones en la nube está totalmente abierta, otra razón por la que la nube es un objetivo especialmente atractivo para los atacantes.
- **La explosión de los dispositivos:** los cálculos sobre el número de dispositivos que estarán conectados a internet en el futuro varían considerablemente y van de los 25 000 millones en 2030 a la impresionante cifra de 75 000 millones quizás para 2025. Cuantos más dispositivos y más conectividad haya, mayor será la expansión tecnológica y mayor la superficie de ataque. Sin embargo, las explosiones de dispositivos a menudo aceleran la innovación.

RECUERDA

La transformación de la seguridad consiste en crear una nueva forma de gestionar todas estas explosiones para que la empresa pueda hacer lo que necesite para tener éxito.

Las empresas que no se unan a la transformación de la seguridad basada en la nube se enfrentan a riesgos cada vez mayores. El panorama actual de la seguridad se ha vuelto demasiado complejo y esto supone un gran desembolso para las empresas: gastos de capital (CapEx), gastos operativos (OpEx) y horas de personal, incluso a medida que la eficacia disminuye. Los proveedores deben, por lo tanto, reconstruir funciones para crear sistemas que faciliten las cosas.

Alcanzar el nirvana de la seguridad

Las empresas que planifican el futuro de su seguridad deben visualizar cómo es el nirvana de la seguridad, tanto a grandes rasgos como con todo lujo de detalles. Los consejos prácticos, y no el *marketing* ni la propaganda (si es que hay alguna diferencia), deben guiar sus decisiones.

A grandes rasgos, esta transición podría producirse así:

1. **Transformación de la red.**

   La red debe mover los datos de la manera más eficiente posible entre todos los puntos, incluidos los servicios en la nube y el centro de datos, sin sacrificar el rendimiento comercial ni la experiencia de los trabajadores a favor de la seguridad. El tráfico se enruta a través de una red creada para funcionar con el SSE que consta de puntos de presencia (PoP) distribuidos por todo el mundo. El personal que se encuentra en la oficina, en su domicilio o en la cafetería cuenta con seguridad y rendimiento de alto nivel y los datos de la empresa siguen estando protegidos.

2. **Consolidación de los servicios de seguridad.**

   Un conjunto de servicios unificado de un solo proveedor con un SSE completo sustituye al mosaico de dispositivos de seguridad heredados. Las capacidades fusionadas simplifican la gestión y la administración, garantizan la aplicación coherente de las políticas y agilizan el procesamiento del tráfico.

3. **Extensión del uso del SSE e implementación de servicios de seguridad avanzados.**

   Con SSE, los equipos de seguridad pueden introducir potentes funciones, como el aislamiento remoto del navegador (RBI), la gestión de la posición de seguridad en la nube (CSPM) y la gestión de la posición de seguridad en SaaS (SSPM). Las capacidades avanzadas como la prevención de la pérdida de datos (DLP) y la protección avanzada contra amenazas (ATP) funcionan mejor que en los modelos antiguos obstaculizados por una integración mínima y una visibilidad restringida.

4. **Protección de los datos en la nube y en los dispositivos de la empresa.**

   El mismo proveedor de SSE también debe proporcionar un *firewall* como servicio (FWaaS) para proteger las aplicaciones en la nube, los dispositivos que son propiedad de la empresa y los repositorios de datos.

5. **El centro de datos como otro destino más.**

   El centro de datos corporativo tradicional, que antes era el único destino a través del cual retornaba todo el tráfico, se convierte en un destino más desde y hacia el cual el SSE enruta el tráfico. La eliminación de conexiones entre nodos reduce el coste y la complejidad y aumenta el rendimiento.

6. **Aplicación de los principios de Zero Trust para conseguir un estado de confianza adaptativa continua.**

   Debido a que el SSE controla el tráfico constantemente después de que se haya otorgado el acceso, los profesionales de la seguridad pueden llevar a cabo un análisis contextual exhaustivo de la sesión, tomar decisiones a partir de información externa sobre riesgos, detectar cambios en los perfiles de riesgo y neutralizar las acciones peligrosas. Las notificaciones pueden ayudar a los trabajadores a mejorar sus hábitos de seguridad.

7. **Mejora de la gestión de riesgos en toda la empresa con mayor visibilidad.**

   La capacidad de ver, guiar y controlar la actividad de todas las personas de la empresa mejora drásticamente la concienciación y detección de los riesgos. El equipo de seguridad puede centrarse en áreas de alto riesgo e implantar con más rapidez políticas mejoradas en el SSE para reducir el riesgo. Los responsables de seguridad pueden participar en conversaciones sobre riesgos y estrategia empresarial, desempeñando así un papel clave en la toma de decisiones.

La transformación de la seguridad no es tarea fácil. En el capítulo 4 veremos cómo los principios de Zero Trust permiten un cambio gradual hacia la total implementación de la seguridad basada en la nube. En el capítulo 5, destacamos los errores frecuentes y los principios del éxito, además de describir la ruta representativa que muchas empresas seguirán si adoptan SSE, Zero Trust y, en definitiva, SASE de la manera correcta.

EN ESTE CAPÍTULO

- Revisamos la historia del *firewall*
- Exploramos por qué la nube ha llegado para quedarse
- Reconocemos las limitaciones de los productos puntuales
- Estudiamos cómo se debe integrar la seguridad para que siga a los datos
- Comprendemos cuál es el papel de SSE en las necesidades de seguridad

Capítulo 2
Cómo la nube acabó con el modelo de seguridad tradicional

Hace una década, algunos líderes pronosticaron la rapidez con la que todas las formas de nube se arraigarían en el sector empresarial. Hoy en día, las empresas se suscriben, de media, a más de 800 aplicaciones de *software* como servicio (SaaS), según Netskope Threat Labs.

La informática en la nube y el procesamiento perimetral sacan cada vez más cargas de trabajo empresarial fuera del centro de datos. Las iniciativas del trabajo remoto, aceleradas por la pandemia de COVID-19, sirvieron de inspiración para que más personas, dispositivos, aplicaciones, servicios y datos se escaparan de los confines tradicionales del centro de datos de la empresa. La nube es hoy en día un aspecto fundamental de la productividad empresarial. Pero a medida que surgen nuevos riesgos, la nube nos está obligando a replantearnos la seguridad.

Pensemos en cómo protegen los padres a sus hijos cuando son bebés y niños pequeños. En sus casas, colocan barreras de seguridad para las escaleras, cubren los enchufes y bloquean los armarios y la tapa del

inodoro. Los padres protegen el perímetro interior con una alarma que les avisa cada vez que se abre una puerta. Protegen el perímetro exterior con una valla en el jardín. Después de dejar a los niños en la guardería, en el colegio y más tarde (¡aah!) en la universidad, el objetivo de proteger a sus hijos sigue siendo el mismo, pero el papel de los padres ha cambiado.

Del mismo modo, para que la nube sea segura, hay que reconocer que el objetivo de la seguridad —proteger los datos, las aplicaciones y las personas— no ha cambiado. Lo que ha cambiado es que los datos, las aplicaciones y las personas se han ido de casa, lo que reduce el papel del *firewall* dejándolo muy relegado. Mientras tanto, las amenazas que crecen más rápidamente están en la nube, no en tu centro de datos. El resultado: las tácticas en torno a la seguridad deben cambiar.

La época en la que el firewall dominaba la seguridad

Hubo un tiempo en el que el *firewall* era el punto de control de la seguridad más importante y también probablemente el elemento más caro en el presupuesto de seguridad. La mayoría de las empresas diseñaban las arquitecturas de seguridad de la red en torno al centro de datos, rodeado por un perímetro bien definido. Tener seguridad suponía tener una red segura.

En el mundo anterior a la nube, esto tenía sentido. El centro de datos era, al fin y al cabo, un solo lugar en el que la empresa guardaba sus valiosos activos digitales. Al igual que un hogar actual con un buen sistema de alarma, una empresa construía un perímetro impenetrable (en la mayoría de los casos) en torno a su centro de datos. Una imponente puerta formada por dispositivos de seguridad limitaba estrictamente el acceso. Como los padres que ponen alarmas en las puertas y ventanas, en aquel mundo anterior a la nube se tenía un control considerable de la seguridad de la empresa.

Los trabajadores se movían por una red exclusiva y privada que los conectaba a las áreas que necesitaban para hacer su trabajo. Los que estaban en otras oficinas alejadas de la empresa o trabajaban de forma remota se movían por la red privada, introducían el código de alarma y conseguían permiso para acceder no solo a las aplicaciones y datos del interior, sino también a todos los destinos externos conectados. Hacer que el tráfico de los trabajadores remotos pasara a través de este centro de datos centralizado dentro del perímetro y volviera a salir después añadía gastos y complejidad, y además perjudicaba al rendimiento.

La antigua seguridad con *firewalls* consistía simplemente en permitir o denegar el acceso. Una vez conseguido ese acceso, la presencia y las

buenas intenciones de cada persona se daban por hecho. Como parte de la seguridad basada en el perímetro, las empresas adoptaron una seguridad diseñada para impedir las amenazas individuales o las categorías de amenazas a medida que estas surgían. Veían una amenaza y compraban otro equipo más. En el modelo local, una empresa podía tener una línea de diez cajas de seguridad conectadas con un cable.

Cada caja llevaba a cabo su propia inspección particular. Aplicaba su propio método de: «Oye, quiero detectar *malware*... Quiero comparar firmas y bloquear intrusiones... Quiero filtrar correos electrónicos, o quiero analizar datos sensibles... Quiero proteger frente a ataques de resolución de nombres... Quiero bloquear puertos y protocolos con listas de control de acceso». Cada función hacía su trabajo y después enrutaba paquetes a la siguiente función en la línea, lo que añadía latencia y complejidad.

La nube ha cambiado todas las suposiciones.

Cómo facilita la nube el trabajo de las empresas

La informática en la nube ofrece tanta flexibilidad y valor empresarial que, llegados a este punto, ya no podemos volver atrás. (Olvídate de las tempestuosas declaraciones sobre «repatriación» a los centros de datos empresariales. Excepto en casos muy raros y concretos, eso no va a ocurrir). La nube resulta atractiva para los consejeros delegados, los directores financieros y los directores de sistemas de información, así como para las empresas en general, porque la mayor parte de la infraestructura está ampliamente disponible y lista para usar. La nube evita que tengas que dedicar mucho tiempo y dinero a invertir en tu propia infraestructura. Te suscribes a una nube, la activas, la personalizas para que se ajuste a tus requisitos de negocio únicos, y la usas. A medida que las empresas tratan de acelerar su forma de generar ingresos y obtener más rentabilidad, el paso a la nube es parte de la respuesta.

La nube también es atractiva para los trabajadores que tan ocupados están. Para ellos, resulta atractiva la gran disponibilidad de aplicaciones de SaaS que ofrecen plataformas modernas, y a menudo entretenidas, para colaborar, comunicarse, gestionar finanzas, cerrar ventas y gestionar las relaciones con los clientes. Estas aplicaciones de terceros en la nube son más amenas, rápidas y eficaces que cualquiera de las demás antiguas y engorrosas aplicaciones de empresa dentro de los rígidos confines del centro de datos de una organización.

ADVERTENCIA

Pero aquí está la trampa, y el peligro: la mayoría de estas aplicaciones de la nube no cuentan con la aprobación, y mucho menos el control, del departamento informático de la empresa; y apenas son seguras. Tienes que seguir encargándote de la protección, pero ya no tienes el tipo de control al que estabas acostumbrado. Adoptar la nube es como mandar a tus hijos al colegio o incluso a la universidad: ya no puedes verlos y dejas de saber lo que hacen.

En la era de la nube, el *firewall* ya no es tu control de seguridad más importante, porque no protege a la empresa en su totalidad de las amenazas que hay en la nube. Sin la seguridad adecuada para proteger y cubrir nuestros procesos digitales, empleados, clientes y (ejem) activos en este nuevo panorama abierto, los esfuerzos de aceleración digital serán arriesgados. En la era de la nube, el papel de la seguridad es materializar el valor empresarial creado por la nube gestionando la responsabilidad que también ha creado la propia nube.

Los productos puntuales ayudan en un momento dado, pero no solucionan los grandes problemas

Cuando los empleados empezaron a trabajar fuera de las oficinas y los datos y aplicaciones pasaron a la nube, las herramientas de seguridad heredadas que tan a gusto estaban en el centro de datos dejaron de ver las actividades que tenían lugar más allá del perímetro. Para que las aplicaciones de SaaS fueran útiles, necesitaban que los datos se originaran *dentro* de los perímetros. Pero las propias aplicaciones estaban fuera del perímetro, por lo que los datos migraban a ellas sin el control y la protección del sistema de seguridad de la empresa.

Si las empresas querían aprovechar con seguridad las aplicaciones basadas en la nube, había que cambiar algo. Las empresas configuraron nuevos productos puntuales centrados en cosas concretas para todas sus redes privadas y la nube con el fin de abordar los problemas de seguridad más apremiantes y las debilidades relacionadas con el uso de la nube. Entre estas herramientas se incluían:

- **Agentes de seguridad para el acceso a la nube (CASB):** estos agentes ayudan a gobernar y proteger los datos empresariales almacenados en un ordenador ajeno, lo que es una forma honesta de conceptualizar la nube.
- **Puertas de enlace web seguras (SWG):** las SWG protegen a los trabajadores y organizaciones frente a las amenazas en la web, es decir, las páginas que visita un trabajador cuando está en línea y navegando por sitios web públicos.

- **Acceso a la red Zero Trust (ZTNA):** los productos de ZTNA protegen simultáneamente las aplicaciones privadas de una empresa frente al público y hacen que las aplicaciones estén disponibles para un grupo de trabajadores conocidos.

Estas herramientas fueron una primera generación de la seguridad de la nube. Pero a esta primera generación le faltaba algo crítico: la integración.

La integración de la seguridad no puede faltar

Los productos de seguridad en la nube de primera generación eran a menudo de distintos proveedores, por lo que no funcionaban bien juntos. Cada uno de ellos tenía su propia consola y era necesario configurar políticas duplicadas y solapadas (piensa en DLP). Cada uno podía necesitar un agente dedicado, lo que generaba dificultades de implementación y enrutamiento de tráfico. Y cada uno exigía negociaciones contractuales y acuerdos de compra diferentes.

Imagínate que tu oído, olfato, gusto, vista y tacto estuvieran conectados a cerebros diferentes. Sin la integración, cuando ves un incendio, lo hueles o lo ves, no sabes qué hacer, porque el cerebro que lo ve, el cerebro que lo huele y el cerebro que lo oye no comparten la misma información. No correlacionan la información que les llega de todos tus sentidos.

Con una infraestructura de seguridad así, tienes muchos sistemas diferentes, cada uno de ellos con un cerebro que sirve para algo en particular. Por ejemplo, CASB es un cerebro que se centra principalmente en «Tengo a un trabajador que está intentando acceder a una aplicación SaaS».

RECUERDA

Del mismo modo que tu único cerebro adquiere información de todos tus sentidos para tomar decisiones sobre cómo actuar en el mundo, tus servicios de seguridad deben estar plenamente integrados para tomar decisiones eficaces que respalden tu estrategia para la nube. SSE es el cerebro que integra categorías de seguridad dispares. En lugar de funcionar por separado en secuencia, SSE permite que todos estos «sentidos» de la seguridad se activen en paralelo. El resultado: una seguridad que es más rápida y, a su vez, más eficaz. Además, SSE es mucho más fácil de adquirir, ya que todas las capacidades (CASB, SWG, ZTNA y aquellas afines) se obtienen a la vez con una sola transacción.

La seguridad debe seguir a los datos

Como explicamos en el capítulo 1, el servicio de acceso seguro en el borde (SASE) describe una visión en la que deja de existir el perímetro empresarial tradicional. En lugar de eso, todo el conjunto de funciones de red y capacidades de seguridad se traslada a la nube, donde está

inmediatamente cerca de los trabajadores, de los datos almacenados en la nube y de las aplicaciones SaaS.

SASE nos permite ajustar nuestra perspectiva en un mundo en el que prima la nube y el trabajo remoto, donde la vieja noción de un perímetro físico se ha desvanecido. En este nuevo mundo, la seguridad debe llegar mucho más allá de las fronteras del centro de datos. La seguridad debe seguir ahora al activo más importante de la empresa, los datos, con un nivel de conocimiento contextual que sea suficiente para protegerlos dondequiera que estén e independientemente de cómo se acceda a ellos.

Para proporcionar seguridad destinada a la nube, deben existir nuevas suposiciones y capacidades de seguridad. La seguridad debe:

- Seguir a los datos.
- Basarse en un contexto enriquecido.
- Adaptarse a las características específicas del contexto del trabajador.

Otro aspecto clave del que se encarga un modelo SASE es el equilibrio entre la seguridad y el rendimiento de la red. No podemos sacrificar una cosa por otra, necesitamos las dos. Las personas son más productivas cuando cuentan con una tecnología que facilite y agilice su experiencia. Cuando las herramientas de seguridad ralentizan las redes, el rendimiento se reduce y la productividad sufre. O incluso peor, los trabajadores tratan de saltarse los controles de seguridad completamente, lo que crea un enorme riesgo y exposición.

El paso fundamental para lograr ese equilibrio es que la empresa traslade sus capacidades de red y seguridad esenciales a la nube mientras que elimina al mismo tiempo los dispositivos perimetrales y (prepárate porque habrá gente en contra) todos los productos heredados.

Un método así proporcionará un acceso seguro y fiable a las aplicaciones, datos y servicios web, donde se aplicarán los principios Zero Trust para conseguir una confianza continua y adaptativa durante cada interacción.

SSE: las necesidades de seguridad para facilitar el SASE

SASE y SSE representan el modo en que la seguridad se traslada a la nube para convertirse en lo más eficaz que hemos tenido hasta la fecha.

SASE es una visión general para la transición de las capacidades de la red y la seguridad a la nube. SSE es el cerebro que integra, identifica y ejecuta un conjunto específico de servicios de seguridad que resulta necesario para conseguir SASE. El conjunto de servicios integrado se convierte en

el punto de inspección principal, donde una inspección y un control de la seguridad coherentes se aplican a todo el tráfico. SSE no sustituye al *firewall* (seguirás teniendo uno), pero sí sustituye a la posición del *firewall* como tu función central de seguridad.

No cabe ninguna duda de que CASB, SWG, ZTNA y otros servicios relacionados aportan valor de forma individual. La mayoría de las empresas ya han implementado uno o dos de ellos. Sin embargo, para sacar el máximo partido a la nube, estos servicios deben integrarse y funcionar juntos.

Para Netskope, las funciones esenciales de SSE pueden aumentarse con muchas capacidades que faltan actualmente en la seguridad empresarial, pero que son cruciales para asegurar los activos digitales con confianza más allá de los confines del centro de datos. Estas incluyen:

- **Clasificación:** identifica y etiqueta información confidencial, de forma ideal, cuando se crea, pero también mediante análisis periódicos de los almacenes de datos.
- **Prevención de la pérdida de datos (DLP):** supervisa y controla activamente el movimiento de la información confidencial.
- **Conocimiento y neutralización de amenazas (también llamada protección avanzada contra amenazas o ATP):** encuentra indicios de que un entorno se ha visto comprometido y toma medidas para reducir o eliminar la probabilidad de ataques futuros.
- **Gestión de la posición de seguridad en la nube (CSPM):** evalúa la configuración de las nubes de infraestructuras y plataformas y emprende acciones para solucionar configuraciones erróneas que puedan hacer correr riesgos.
- **Gestión de la posición de seguridad en SaaS (SSPM):** evalúa la configuración de las aplicaciones SaaS y elimina las configuraciones erróneas que puedan permitir la exfiltración, suplantación de identidad y otros tipos de ataque.
- **Gestión de la experiencia digital (DEM):** analiza los datos recopilados con fines de seguridad además de otras señales de disponibilidad y rendimiento para medir la experiencia del trabajador y ayudar a resolver problemas con rapidez.

RECUERDA

Al combinar todas estas capacidades en un solo producto de seguridad integrado implementado en la nube, donde esté lo más cerca posible de las personas, los datos y las aplicaciones, SSE se convierte en el punto de inspección más importante para proteger tu empresa. (Analizaremos más de cerca SSE en el capítulo 3.)

Necesitamos seguridad para el futuro, no para el pasado

Debemos implementar herramientas que funcionen en la nube, el factor clave para generar valor y beneficios comerciales. Debemos implementar herramientas que resistan la interrupción del servicio por parte de adversarios. Por último, debemos implementar herramientas que no obstaculicen las operaciones. Compara este concepto con la idea de hacer que un guardaespaldas invisible acompañe a tu hijo a la guardería, al colegio y a la universidad. Ese guardaespaldas portátil es SSE.

EN ESTE CAPÍTULO

- Por qué necesitamos SSE
- Analizamos las capacidades y requisitos de SSE
- Evaluamos las ventajas de SSE

Capítulo 3
Servicio de seguridad en el borde: un plan para el futuro de la seguridad basada en la nube

El servicio de acceso seguro en el borde (SASE) cambia nuestro punto de vista sobre cómo se garantiza la seguridad en un mundo basado en la nube en el que se puede acceder a los datos desde cualquier lugar. Cuando los trabajadores son remotos, las aplicaciones se convierten en *software* como servicio (SaaS) y los datos se trasladan a la nube, las tareas de ciberseguridad de una organización también deben trasladarse a la nube. SASE implementado correctamente nos muestra que la seguridad debe también estar lo más cerca posible del lugar donde residen los datos y desde el que se accede a ellos. En SASE, la seguridad protegerá los intereses de la organización y proporcionará controles coherentes independientemente de lo lejos que estén esos intereses, sin deteriorar la conectividad de la red ni la experiencia del usuario.

Una forma de conseguir SASE es mediante la consolidación y la integración de la seguridad, que es la pura esencia de SSE.

SSE reubica los puntos de inspección y control críticos a la/s nube/s donde funciona tu negocio. Este cambio coloca a la seguridad junto al lugar donde trabajan los datos, las aplicaciones y las personas... Y también donde está el peligro. Con SSE, los servicios de inspección y control para SaaS, web y datos, además del conocimiento y neutralización de las amenazas, funcionan como un único sistema coherente e interoperable.

CONSEJO

No tienes un problema de red. Tienes un problema de seguridad en la red. La única conversación sobre la red que debes mantener es la que trata sobre la adopción de una arquitectura que haga de SSE el punto de inspección principal en la nube.

SSE ofrece capacidades que trascienden lo que pueden hacer los *firewalls* tradicionales. Un SSE correctamente implementado también distingue el contexto, los detalles de a qué datos se accede, cómo y por qué, lo que le permite tomar decisiones de seguridad con matices en tiempo real. SSE conecta todos tus «sentidos» de seguridad a un solo cerebro que interpreta los datos, comprende el alcance de los riesgos presentes y negocia el nivel de acceso adecuado en cualquier momento y situación determinados.

Más adelante, echaremos un vistazo a cómo funciona SSE.

Por qué necesitamos SSE

El antiguo enfoque ante la seguridad se basaba en establecer un perímetro e instalar un *firewall* para intentar ahuyentar a los atacantes cuyo objetivo era tu centro de datos corporativo. Pero como ningún tipo de seguridad es infalible, el atacante que conseguía atravesar el perímetro tenía libertad para moverse lateralmente en toda tu red, dejando tus datos y aplicaciones sin una defensa eficaz.

Las arquitecturas SASE todavía dependen de la gestión de identidades y accesos para autenticar al trabajador y de las plataformas de protección de *endpoints* para proteger los dispositivos. Pero el SASE eficaz también pone en práctica los principios de Zero Trust que otorgan accesos y supervisan la confianza según un completo conjunto de condiciones. En la nube, el contexto que rodea a la persona se convierte en el perímetro.

Zero Trust es una filosofía basada en tres propuestas que son fundamentales para SSE y, por lo tanto, para SASE:

- La confianza implícita presente en los diseños heredados ha perdido su utilidad. Zero Trust invierte la confianza, pero verifica para verificar, después, confía. Para cada persona o acción que solicita acceso a los datos se debe verificar su identidad y contexto, cada vez, para lograr un cierto nivel de confianza. Sin excepciones.

- Se proporciona solo el acceso mínimo (lo que también se conoce como privilegio mínimo) que es adecuado para el nivel de confianza determinado. El acceso se limita a un recurso específico y no es transferible a otros recursos.
- El contexto debe evaluarse una y otra vez de manera constante, según señales como la identidad del trabajador, identidad del dispositivo, posición de seguridad del dispositivo, hora del día, geolocalización, puesto en la empresa, y confidencialidad de los datos. Cada cambio de señal debe desencadenar una nueva evaluación. (Netskope llama a esto *confianza adaptativa continua*, de lo que hablaremos en profundidad en el capítulo 4.)

SASE ofrece un marco para un programa de Zero Trust eficaz que abarque por completo entornos en los que las personas, las aplicaciones y los datos están en cualquier lugar. Pero, como veremos más adelante en el capítulo 4, Zero Trust consiste en un conjunto de principios, no en una arquitectura técnica sobre cómo implementar distintas funciones de seguridad de manera unificada.

SSE ofrece esa arquitectura técnica. SSE unifica, integra y coordina muchos servicios de seguridad, mejora las capacidades de la seguridad y proporciona un alto rendimiento para satisfacer las necesidades de los trabajadores y la empresa, y lo hace de forma integrada y personalizada en función del contexto. Para conseguir los resultados deseados, SSE proporciona lo siguiente:

- Un contexto detallado que incluye el historial del trabajador, dispositivo, datos solicitados, aplicación, red e incluso el motivo de la solicitud.
- Información sobre los recursos a los que tiene permitido acceder la persona para responder a la solicitud, que SASE puede recoger de los datos de autorización y derechos.
- Información granular que clasifica la confidencialidad de los distintos recursos de datos (para evitar la pérdida de datos).
- Guías y un conjunto de políticas detallado que describen el resultado de seguridad deseado según distintas combinaciones de personas, datos, aplicaciones y otra información contextual.

La dificultad radica en que muchos de los resultados de seguridad, como DLP y el conocimiento y neutralización de amenazas, necesitan que varios componentes trabajen juntos.

ADVERTENCIA

Implementar cada servicio de manera independiente exige la repetición de una buena cantidad de trabajo de seguridad en las consolas de una herramienta después de otra. Esto es engorroso y puede provocar errores cuando una venta, o una vida, dependen de ello.

SSE elimina la repetición. Cuando se implementa correctamente, combina esos servicios y los habilita para que compartan contexto, derechos, políticas de seguridad, información sobre riesgos, aislamiento de navegadores, cifrado/descifrado de datos, y mucho más. Esta cohesión capacita a los servicios de seguridad para que procesen transacciones en un único paso y concedan el acceso adecuado con rapidez.

Cómo integra SSE los servicios de seguridad

SSE se basa en la integración de muchos servicios de seguridad respaldados por un gran número de capacidades relacionadas. Hay una sola manera correcta de construir un SSE... Pero hay muchas maneras incorrectas de hacerlo.

ADVERTENCIA

A medida que el término SSE cobra popularidad, crece también la publicidad engañosa. Es fácil reconocer cuándo SSE se ha construido de forma incorrecta debido a la falta de integración. Los métodos que simplemente unen procesos diferentes o actualizan las conexiones en cadena de viejos dispositivos son ejemplos de sistemas montados a partir de componentes individuales, construidos con estilos anteriores a la nube y posiblemente adquiridos de distintos proveedores. Estos sistemas unidos introducen una latencia significativa, no ofrecerán las grandes ventajas de SSE y no son acciones coherentes en tu camino general hacia SASE.

SSE no es nunca una conexión en cadena de dispositivos ni una secuencia de procesos separados en los que los datos pueden pasar a través de un motor DLP, luego a través de un evaluador de listas de control de acceso, después a través de una puerta de enlace web, y así sucesivamente. Sin embargo, es útil desglosar las características que describen un SSE totalmente integrado.

Análisis en fases y en un único paso

RECUERDA

En un SSE ideal, los servicios de seguridad integrados funcionan en paralelo. Todas las inspecciones tienen lugar de forma simultánea, en tiempo real, independientemente de si el tráfico llega de la web, la nube o el centro de datos.

Un único paso ofrece un filtrado de tráfico cada vez más preciso para garantizar la seguridad de los datos y las aplicaciones. Imagínate el tráfico pasando por un embudo.

Un SSE adecuado sabe diferenciar entre las aplicaciones de la empresa (por ejemplo, Salesforce, Workday), las aplicaciones personales (como una cuenta personal de Gmail), y las aplicaciones/servicios de terceros (como las instancias de la empresa de Microsoft Office 365 o Dropbox). Utiliza esos conocimientos para iniciar las conexiones adecuadas que se necesitan a fin de proteger cada aplicación o servicio conforme a la política pertinente.

Un SSE adecuado evalúa el contexto y ajusta el acceso según, por ejemplo, si un médico (consulta el capítulo 4) está usando una tableta propiedad del hospital en una habitación de un paciente, su teléfono con el wifi de la cafetería o el ordenador de videojuegos en la habitación de su hija.

Un SSE adecuado impone políticas que evitan que los datos se filtren o se pierdan. Los controles pueden evitar descargas de documentos, capturas de pantallas, introducciones de datos en formularios web o publicaciones en redes sociales.

Un SSE adecuado ofrece una supervisión continua. Mientras el trabajador lleva a cabo sus tareas normales, SSE observa para detectar anomalías. Cuando se clasifican los objetos de datos, SSE puede diferenciar entre contenido confidencial y no confidencial y modificar dinámicamente permisos de acceso y actividades permitidas. SSE puede desencadenar una alerta, emitir advertencias o solicitar al trabajador más información para que lleve a cabo su actividad con mayor seguridad.

Con tecnología de servicios compartidos

Todas las funciones de seguridad de alto nivel, como la DLP, el conocimiento y la neutralización de amenazas y la gestión de la experiencia digital (DEM), entre otras, pueden hacer uso de cualquiera o todos los servicios y técnicas que describimos aquí para conseguir los resultados de seguridad deseados:

- **Contexto compartido:** todos los elementos de SSE comparten una gran colección de metadatos que identifican a la persona, el dispositivo y la ubicación. Se identifica el sitio web, la aplicación o el servicio de destino, y se evalúa su riesgo y actividades. Se tienen en cuenta todos los datos solicitados o creados por el trabajador y la aplicación. El contexto enriquecido de SSE incluye una evaluación del comportamiento del trabajador, con referencias incluso a interacciones antiguas para analizar la actividad actual. Este panorama contextual actualizado constantemente fundamenta las acciones emprendidas y las políticas ejecutadas por todos los elementos de SSE. (En el SSE de Netskope, este servicio se llama Cloud XD).

- **Confianza adaptativa continua:** el acceso a los datos y las aplicaciones no es una decisión simple y binaria. El acceso debe ser flexible y basarse en requisitos y contextos cambiantes. Un SSE adecuado adapta el nivel de confianza al valor de los activos a los que se accede haciendo uso de la gran cantidad de señales contextuales disponibles y del apetito de riesgo de la organización conforme a sus políticas.
- **Administración basada en políticas:** como parte de una seguridad de un único paso, un SSE adecuado cuenta con un marco de políticas detallado y compartido que permite a la organización establecer los límites de su tolerancia al riesgo y definir con claridad los resultados de seguridad esperados. Esto representa una desviación importante de los miles de reglas que normalmente conforman los *firewalls*. Los componentes de SSE consultan el marco de políticas para controlar las actividades y los datos de todas las aplicaciones, categorías de aplicaciones y servicios web.

SSE: principales atractivos

ahora que hemos descrito los componentes subyacentes de SSE, podemos examinar las capacidades que ofrece. Algunas serán las cosas familiares que tu organización ya ha implementado de otra forma, así que es probable que SSE las sustituya con el tiempo.

RECUERDA

El objetivo de SSE es que las personas y la empresa trabajen de la forma más rápida y segura posible. Al funcionar en cualquier lugar, SSE termina con los esfuerzos inútiles para ampliar la seguridad en el centro de datos para seguir a los datos, aplicaciones y personas que han pasado a la nube.

En la tabla 3-1 se muestran los requisitos mínimos en cuanto a capacidades que debe tener un producto para que pueda considerarse un SSE según el criterio de varios analistas en 2021.

TABLA 3-1 **Requisitos mínimos para las capacidades de un SSE**

Capacidad	Qué hace	Cómo SSE lo mejora
SWG	Controla el acceso y protege solamente ante amenazas web.	También protege frente a amenazas y riesgos de datos en la nube para instancias personales de aplicaciones gestionadas, miles de aplicaciones de TI en la sombra y servicios en la nube.
CASB	Un punto de aplicación de políticas de seguridad situado entre los consumidores y proveedores de servicios en la nube para aplicar políticas de seguridad empresarial cuando se accede a los recursos basados en la nube. Evalúa el comportamiento y tiene conocimiento de la funcionalidad de las aplicaciones SaaS para otorgar el acceso adecuado a una persona determinada.	Elimina la duplicación de políticas (entre SWG y CASB), simplifica la administración (único agente para SWG, CASB y ZTNA) y ofrece visibilidad de todos los carriles de tráfico.
ZTNA	Hace cumplir el supuesto de que no se confía en nadie a ciegas ni se le permite acceder a los activos de la empresa hasta que se haya validado como persona legítima y autorizada. Defiende la implementación del acceso de privilegio mínimo, que otorga acceso de manera selectiva solamente a a los recursos que necesitan las distintas personas o grupos, y a nada más.	Complementa a ZTNA mediante una capacidad de acceso adaptativo. Armoniza la administración y la toma de decisiones en torno a políticas con otros componentes de SSE mientras mantiene la aplicación de políticas distribuidas.
Aislamiento remoto del navegador (RBI)	Separa los dispositivos de los trabajadores de la navegación por internet alojando y ejecutando toda la actividad de navegación en un contenedor remoto en la nube. Este espacio seguro protege los datos, los dispositivos y las redes frente a todos los tipos de amenazas que se originan en sitios web maliciosos.	Permite al RBI hacer uso de la clasificación de los datos y del contexto de las funciones. Añade aislamiento al conjunto de las acciones de las políticas en SWG y CASB.

(continuación)

TABLA 3-1 *(continuación)*

Capacidad	Qué hace	Cómo SSE lo mejora
Firewall como servicio (FWaaS)	Seguridad de red para todos los puertos y protocolos de salida que consigue conseguir un acceso seguro y directo a internet mediante un agente en dispositivos gestionados o a través de GRE e IPsec para las oficinas. Un motor de políticas y una plataforma de seguridad que ofrecen una gestión simplificada a los trabajadores y sucursales que usan una sola consola.	Permite a las organizaciones agregar tráfico procedente de varias fuentes, bien sea de los centros de datos locales, las sucursales, los trabajadores móviles o la infraestructura en la nube. Facilita una aplicación coherente de la seguridad y aplicaciones en relación con las políticas en todas las ubicaciones y para todos los trabajadores al mismo tiempo que facilita una visibilidad y control completos de la red sin implementar dispositivos físicos.

Capacidades de SSE: próximamente en tu equipo de seguridad

SSE desarrollará mayores capacidades a medida que los productos maduran y proliferan las iniciativas que priorizan la nube. Una arquitectura de SSE adecuada abarca mucho más que la definición inicial original, como:

- Clasificación mejorada para promover la DLP
- Gestión de la posición de seguridad para la nube y SaaS
- Conocimiento y neutralización de amenazas
- Gestión de la experiencia digital

En los apartados siguientes explicamos cada uno de estos aspectos.

Clasificación mejorada para promover DLP

DLP es un término comodín que hace referencia a una función creada para evitar la exfiltración de datos intencionada y accidental mediante un uso indebido intencionado y no intencionado. DLP detecta el movimiento de información confidencial, evita que se extienda a lugares no deseados,

interrumpe a los trabajadores con elementos emergentes educativos para detener la exposición no intencionada e incorpora el aprendizaje automático para evaluar las puntuaciones de riesgo de los trabajadores.

CONSEJO

SSE mejora la DLP al identificar y clasificar los datos de forma activa, posibilitando así el seguimiento y aplicación de reglas relacionadas con el movimiento de datos confidenciales de forma más precisa.

Gestión de la posición de seguridad para la nube y SaaS

La gestión de la posición de seguridad en la nube (CSPM) y la gestión de la posición de seguridad en SaaS (SSPM) encuentran y solucionan errores de configuración en las nubes (la forma más frecuente de fallo de seguridad en la nube). Por medio del contexto proporcionado por SSE, los controles con interfaz de programación de aplicaciones (API) y la evaluación en tiempo real de las implementaciones en la nube pública, CSPM y SSPM reducen el riesgo analizando la configuración, sugiriendo cambios que reducen o incluso eliminan la probabilidad de un ataque potencial y supervisando el cumplimiento de las normativas.

CONSEJO

En las implementaciones correctas de SSE, CSPM y SSPM reconocen las amenazas y emprenden acciones de forma activa para aumentar la posición de seguridad de una organización.

Por ejemplo, algunas implementaciones de CSPM y SSPM pueden identificar incumplimientos cuando una política de una organización requiere el cifrado de todos los datos en la nube de manera predeterminada. Esta es una postura muy fuerte porque exige controles de acceso que deben estar de acuerdo: la identidad de una persona debe figurar en la lista de control de acceso para un objeto cifrado y en la lista para la clave de cifrado asociada. CSPM y SSPM reconocen cuándo una persona tiene acceso a una de ellas y no a la otra y avisa de la incoherencia.

Conocimiento y neutralización de amenazas

El conocimiento y neutralización de amenazas encuentra señales de ataques lanzados con éxito y alerta para que pueda contenerse el peligro. Entre las señales habituales se incluyen una actividad inusual de la red, cambios en la configuración y eliminación de archivos de registro. El análisis forense determina si hay una amenaza activa en el entorno. La neutralización de amenazas es un ejemplo perfecto de un servicio que aporta pruebas a las capacidades compartidas de la arquitectura SSE, además de beneficiarse de ellas.

Gestión de la experiencia digital

Un aspecto emergente y potente de SSE es su capacidad para medir la experiencia de los trabajadores y el rendimiento de las aplicaciones, sobre todo porque el límite de la red se extiende ahora a la nube y más allá. Al proporcionar una supervisión continua de todo el tráfico, los clientes se benefician de una visibilidad de extremo a extremo del comportamiento de su red y aplicaciones, con información práctica en tiempo real basada en la actividad humana real para garantizar que SSE funciona sin sacrificar el rendimiento. Cuando surgen problemas de dispositivos, redes o aplicaciones, DEM puede ayudar a identificar las causas raíz rápidamente, acelerar la resolución de las solicitudes de asistencia técnica y proporcionar medidas proactivas para evitar que los pequeños problemas se conviertan en acontecimientos importantes que afecten a la empresa.

Las redes deben evolucionar también

Hasta ahora, nos hemos centrado en las características y capacidades de seguridad que ofrece SSE para un mundo que prioriza la nube. Pero se necesita una mayor transformación más allá de lo que consideramos que es la seguridad.

RECUERDA

El acceso a la red debe distribuirse para permitir a los trabajadores y organizaciones obtener un valor completo de los sistemas basados en la nube que protege el SSE, como se muestra en la figura 3-1.

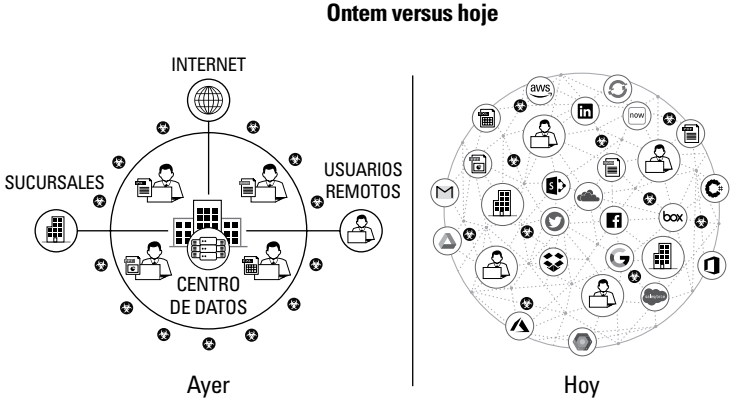

FIGURA 3-1: el modelo de acceso antiguo era ineficiente e ineficaz en comparación con el nuevo modelo, que permite el acceso en cualquier lugar.

En el antiguo modelo de acceso, los trabajadores se conectaban a una red protegida por un perímetro bien definido. Las sucursales mantenían las caras conexiones de la red privada al centro de datos. Esto se convirtió en un obstáculo a medida que las operaciones comerciales prosperaron, primero en la web y después en la nube. La única opción segura era desviar el tráfico de los trabajadores a través de la pila de seguridad del centro de datos antes de interactuar con los recursos web y en la nube.

Este método es ineficiente e ineficaz. Permitir a los trabajadores que interactúen directamente con los recursos en la nube mejora de forma considerable el rendimiento y la productividad, pero obstaculiza la visibilidad y el control del centro de datos. Persistir en el antiguo modelo de construir, mantener y supervisar las redes privadas para llegar a todo lo que la nube puede ofrecer es complicado, costoso y simplemente no es ampliable en una era en la que la seguridad debe ser una prioridad principal a todos los niveles comerciales, incluido el consejo de administración.

El nuevo modelo de red prevé una arquitectura construida para el trabajo remoto, donde las personas se conectan desde cualquier lugar e interactúan con otras personas e información principalmente en la nube. Para conseguir el mejor rendimiento y la mejor experiencia con las aplicaciones, la red de un proveedor de SSE debe:

- Estar interconectada a numerosas conexiones a los destinos más importantes.
- Constar de una cantidad suficiente de puntos de presencia equipados con recursos informáticos completos y distribuidos estratégicamente de modo que los trabajadores nunca estén lejos.

CONSEJO

La forma de lograr conexiones rápidas y sin esfuerzo es trabajar con un proveedor cuya red esté altamente interconectada con numerosas conexiones directas a los destinos más importantes. Cuantas más conexiones ofrezca tu proveedor, mejor será el rendimiento, más fuerte será su resistencia y más contentos estarán los usuarios.

RECUERDA

Un proveedor bien conectado ofrece un mejor rendimiento, una resistencia más sólida y experiencias agradables. ¡Y la experiencia de los trabajadores importa! La transformación digital tiene éxito cuando la seguridad y las redes se fusionan para formar un asociación cohesiva desde el primer momento. La seguridad que degrada el rendimiento de la red, o que obliga a adoptar un peligroso compromiso entre seguridad y productividad, no funcionará nunca.

Como todos los aspectos de SASE y SSE, la transformación de la red se optimiza con el tiempo. Tu proveedor de seguridad en la nube debe abarcar la división entre la seguridad que tienes ahora y dónde quieres estar en el futuro. Debe proporcionar SSE, ofrecer nuevas rampas de acceso para tus trabajadores distribuidos e integrarse correctamente en la infraestructura y los procesos de red existentes.

La recompensa de la seguridad SSE

Al adoptar una arquitectura SASE en cuyo núcleo se encuentran los principios de Zero Trust y asociarse con un proveedor de SSE capaz de brindar servicios de seguridad distribuidos críticos, una organización puede conseguir considerables beneficios:

- Mayor confianza a la hora de conceder acceso a datos y aplicaciones fuera del centro de datos.
- Seguridad flexible basada en conocimientos sobre riesgos con políticas adaptativas y control de actividades específicas a medida de cada aplicación.
- La capacidad para extender los principios de Zero Trust más allá de las aplicaciones privadas y abarcar las aplicaciones web y SaaS.
- Acceso a servicios de seguridad adicionales como RBI y DLP avanzada según el nivel evaluado de riesgo o confianza.
- Supervisión continua de los cambios en contexto que activan automáticamente una reevaluación de la confianza y el acceso.
- Una reducción de la superficie de ataque al eliminar la exposición de protocolos y servicios en el internet público.
- Nubes configuradas correctamente que eliminan los fallos de seguridad en la nube más frecuentes.

Todas estas ventajas representan aspectos del nirvana de seguridad que mencionamos en el capítulo 1. En el capítulo 4 analizamos los beneficios comerciales de un SSE adecuado y los pasos para materializarlo.

EN ESTE CAPÍTULO

- Conseguimos un estado de confianza adaptativa continua con los principios de Zero Trust
- Conocemos los cuatro pasos para adoptar SSE
- Descubrimos los beneficios empresariales de SSE

Capítulo 4
Los principios de Zero Trust para convertir SASE en realidad

Como dijimos en el capítulo 2, trasladar la seguridad a la nube tiene importancia ahora porque, básicamente, la nube tiene importancia ahora para la empresa. La adopción de la nube es rápida, más incluso de lo que predijeron las organizaciones más innovadoras hace cinco años. Las empresas están adoptando la nube para conseguir un desarrollo rápido, acceso a recursos bajo demanda, escalado elástico y una carga administrativa mucho menor con el fin de poder innovar y crear nuevos productos y servicios en un tiempo récord.

Los atacantes se han trasladado a la nube porque, bueno, ahí es donde están las empresas. Así que todos debemos prestar atención a cómo mantenemos la seguridad de nuestros datos, aplicaciones y trabajadores en la nube.

ADVERTENCIA

Si la nube no está protegida, sus beneficios serán inalcanzables.

Los responsables deben plantear que, en primer lugar, proteger la nube es importante y, en segundo lugar, que con SASE, SSE y las nuevas herramientas para la nube se conseguirá una mejor gestión del riesgo y se reducirá la fricción que causa la seguridad. Los planes de adopción deben explicar por qué este cambio merece la pena, prever los beneficios

empresariales concretos y exponer cómo medir esos beneficios durante la transición.

A partir de nuestras discusiones sobre la transformación de la seguridad, SASE y SSE, en este capítulo se describe el camino al nirvana de la seguridad que todos queremos, un camino en el que nuestros datos, aplicaciones y trabajadores estén seguros en la nube para que puedan generar un valor comercial considerable e incuestionable. Ese camino incluye ahora inexorablemente la aplicación de los principios de Zero Trust a cómo creamos nuestra seguridad.

De Zero Trust a la confianza adaptativa continua

Una implementación correcta de SASE y SSE es algo más que un cambio de tecnología. Como explicamos en el capítulo 3, Zero Trust renueva algunos supuestos básicos sobe cómo funciona la seguridad. En el modelo local basado en la red, el supuesto es que la red es segura y que debemos comprobar la identidad de una persona antes de otorgarle acceso. El paradigma habitual concedía acceso al usuario a todo o nada, es decir, «permitir» o «bloquear» eran las únicas opciones. Zero Trust cambia este modelo de la manera siguiente:

- **Cuando una persona solicita acceso, esta solicitud se evalúa en un contexto que tiene en cuenta varias condiciones.** La identidad es una de ellas, pero el sistema también tiene en cuenta dónde está la persona, la hora del día, el dispositivo, el tipo de conexión de la red, y muchas otras variables.
- **La aplicación a la que se conecta la persona forma parte de ese contexto.**
- **El nivel de servicio deseado es un factor importante.** ¿Se trata del uso a vida o muerte de una aplicación o de un videojuego para divertirse?
- **La forma de proteger la ruta de acceso a la red puede cambiar en función de la aplicación que se esté usando.** Si alguien accede a su cuenta de correo electrónico personal, se utiliza una conexión a internet ordinaria con protección de Seguridad de la capa de transporte (TLS) negociada entre su servidor de correo electrónico y el cliente de correo electrónico. Si un médico accede al historial clínico de un paciente, se establece una ruta segura, cifrada y con autenticación, independientemente de las capacidades de la red o la aplicación subyacentes.

Según este contexto, se determina el nivel de confianza de la sesión de una persona, y este nivel puede ser bajo o alto. Una persona que solicita acceso a una aplicación sumamente confidencial a una hora extraña y desde un lugar extraño (una instancia de nivel de confianza bajo) se encontrará probablemente con un proceso de autenticación de varios pasos. El acceso otorgado puede limitarse a un pequeño conjunto de datos y funciones, y también a un modo de solo lectura. Un trabajador que desea acceder a la hora habitual desde un lugar seguro (una instancia de nivel de confianza alto) puede obtener acceso completo a todos los datos y capacidades de las aplicaciones.

Piensa en cómo este ejemplo de un médico que accede al historial clínico electrónico ilustra la puesta en práctica de los principios de Zero Trust en SSE.

> Un médico lleva una tableta que es propiedad del hospital mientras trata a un paciente en el hospital. En función de la identidad del médico, su ubicación, dispositivo, y otros factores, SSE determina que es seguro otorgarle acceso completo al historial clínico del paciente.
>
> El médico sale del hospital y va a tomar un café. Enciende su portátil, se conecta a la red de la cafetería y trata de acceder a la historia clínica del paciente. SSE reconoce al médico, pero se da cuenta de que el portátil no es del hospital y de que está conectado a una red desconocida. El médico tendrá permiso para ver la historia clínica y añadir comentarios, pero no podrá modificar los datos.
>
> El médico está cenando en casa y recibe un aviso de una emergencia. Cierra la sesión de Minecraft de su hijo en el ordenador familiar y accede a la historia clínica del paciente. SSE se da cuenta de que este ordenador es menos seguro que la tableta del hospital. En lugar de denegar el acceso, SSE envía una serie de solicitudes que permiten al médico verificar su identidad y explicar el motivo por el que necesita ese acceso. SSE proporciona después al médico una serie segura de recursos para responder a la emergencia, por ejemplo, en una sesión de navegación aislada bajo el control de SSE.

Quizá ya conozcas el término «acceso a la red Zero Trust» (ZTNA). ZTNA es una opción excelente para aumentar tu red privada virtual (VPN) a fin de incorporar más escenarios de acceso remoto. Con ZTNA, los trabajadores no reciben acceso a una parte completa de una red que podría permitir conexiones a muchos servicios. En lugar de eso, ZTNA solo da al trabajador una conexión a la aplicación que trata de utilizar y, al igual que en la historia de nuestro médico, con solo el mínimo acceso necesario para llevar a cabo la tarea que tiene entre manos.

Si analizamos más de cerca este modelo y cómo funciona en su forma más avanzada, surgen una serie de ideas importantes que pueden guiar nuestra labor:

- **Contexto:** en la seguridad anterior al SASE, la red definía el perímetro, una barrera que había que cruzar para conseguir acceso. Una línea de pensamiento concreta sugiere que la identidad es el nuevo perímetro en Zero Trust porque debe validarse para permitir el acceso, pero ese concepto es insuficiente. Un método mejor es evaluar el contexto en su totalidad, incluida la identidad, pero también muchas otras variables, con el fin de determinar qué tipo de acceso se permite.
- **Privilegio mínimo:** Zero Trust siempre trata de otorgar solamente el acceso mínimo que se necesita para que el trabajador pueda hacer su trabajo. La forma más avanzada de Zero Trust también trata constantemente de descubrir si se ha concedido demasiado privilegio y trata de eliminar ese exceso de confianza del sistema.
- **Puntuación de riesgo:** SSE elabora un historial de actividades cuando los trabajadores interactúan con las aplicaciones. Se puede analizar ese historial para crear una representación de la actividad normal y para detectar actividad sospechosa en tiempo real. Este análisis genera puntuaciones de riesgo para un trabajador, una aplicación y un sitio web. Estas puntuaciones ofrecen contexto adicional para determinar qué tipo de acceso otorgar.
- **Ocultación de recursos:** el acceso basado en ZTNA no expone las direcciones IP públicas a las que cualquiera puede conectarse. La conectividad se facilita solo después de que se haya evaluado el contexto. De manera predeterminada, todo está oculto. (Sí, la oscuridad desempeña un papel en la seguridad, al contrario de lo que se enseña a menudo en las clases de Infosec).
- **Confianza adaptativa continua (probablemente, la mejor idea de esta lista):** la confianza adaptativa continua consiste en supervisar una conexión y ajustar constantemente los permisos en función de los cambios de contexto. ¿Está alguien que normalmente usa Salesforce intentando acceder al sistema de tesorería del director financiero? Alerta roja: se reducen el acceso y la autorización, se aumenta la puntuación de riesgo y se avisa a alguien para que tome medidas. ¿Hay otra persona tratando de acceder a un sitio web peligroso? Se muestra una ventana con una advertencia antes de otorgar el acceso. El objetivo es reaccionar constantemente a los cambios de contexto para proteger los datos, las aplicaciones y los trabajadores de la manera adecuada.

RECUERDA

La implementación de SSE con los principios de Zero Trust reduce la superficie de ataque y se centra mucho más en los datos, lo que mejora considerablemente la posición general de seguridad, ya que el nivel de riesgo que presenta una persona, aplicación o sitio web se evalúa una y otra vez de manera constante. La seguridad se adapta en tiempo real según los cambios de contexto.

Ahora que tenemos una postura firme ante la confianza adaptativa continua, podemos pasar a hablar de cómo implementar SSE de la manera adecuada.

Cuatro sencillos pasos para implementar SSE

Para la mayoría de las organizaciones, hacer que SSE sea una realidad supone pasar de una seguridad local con la red como perímetro a una seguridad basada en la nube en la que el contexto es el perímetro. Vamos a dar por supuesto un punto de partida que refleja dónde se encuentran la mayoría de las empresas hoy en día: un *firewall* local que incluye VPN para acceso remoto, un dispositivo de puerta de enlace web segura (SWG) local que controla el acceso a la web, y quizás una suscripción a un agente de seguridad para el acceso a la nube (CASB) independiente que protege el uso de las aplicaciones SaaS.

Paso 1: migración de los trabajadores remotos para recuperar la visibilidad

Lo primero que hay que hacer es evaluar qué hacen tus trabajadores y medir tu nivel de riesgo actual. La forma más fácil de conseguirlo es empezar con la población de usuarios remotos, ya que son estos trabajadores lo que potencialmente introducen más riesgos. Dirige su tráfico web y SaaS a través de las capacidades de SWG y CASB de SSE, configuradas lo más acorde posible a las políticas existentes. Después, observa.

Este ejercicio genera una visión más completa de lo que hacen los trabajadores. Las empresas que no usan CASB ni SWG descubrirán enseguida una enorme (y potencialmente alarmante) cantidad de actividad. Las empresas que ya usan CASB y SWG aprenderán cosas nuevas.

Casi seguro, descubrirás que los trabajadores remotos acceden a aplicaciones y servicios que no conocías. Te enterarás de dónde trabajan y qué tipo de redes usan normalmente.

La parte que queda del paso 1 es migrar el acceso a los sistemas internos del centro de datos, de las VPN a ZTNA en SSE. Esto mejora la experiencia del trabajador y aumenta la seguridad al mismo tiempo. Imagínate a un fontanero que va a tu casa para arreglar una fuga mientras tú estás en el

trabajo. Tiene total acceso a toda tu propiedad mientras va y viene de su furgoneta al cuarto de baño. Incluso puede que deje la puerta de la casa abierta. Mientras tanto, tú no tienes ni idea de lo que está ocurriendo. ZTNA es como si tuvieras un botón mágico de teletransporte. Llega el fontanero, le teletransportas desde la furgoneta hasta la fuga y de vuelta a la furgoneta sin que haya paradas por el camino. Es control de acceso, perfeccionado para la era de la nube.

Paso 2: migración de los demás trabajadores y aplicación de la clasificación de datos en toda la empresa

El segundo paso es trasladar a todos tus trabajadores locales (que tienen la protección de SSE para controlar el acceso) a las aplicaciones y servicios de la nube. Dar este paso para que todos tus trabajadores, tanto los locales como los remotos, estén protegidos por SSE transforma tu arquitectura de red. Ahora, todos los trabajadores transitan por el punto de presencia más cercano del proveedor de SSE, que después enruta el tráfico a su destino de la mejor manera posible, a menudo, con menos paradas que el internet público. Ya puedes simplificar la red y olvidarte de las costosas redes privadas que quizá ya no necesites. Como parte de esta transición de red, pueden introducirse redes de área amplia definidas por software (SD-WAN) para dirigir selectivamente el tráfico que proviene de las sucursales.

El objetivo es llegar a entender totalmente los datos, aplicaciones, sitios web y otros servicios de interés para nuestros trabajadores. En esta fase, la capacidad de SSE para capturar y analizar la actividad aumenta de manera considerable el alcance y la exhaustividad del contexto. En este paso, la posición de seguridad de tus políticas de SSE deberían ser probablemente parecidas a aquellas que ya existen en los productos heredados a los que SSE sustituye. Es importante adaptar un estado conocido antes de añadir nuevas capacidades que pueden requerir educación y formación.

Con este nuevo contexto, puedes establecer las bases para conseguir una seguridad mejor mediante la clasificación de los datos, las aplicaciones y las personas en función del riesgo y el comportamiento. Cuando se hayan llevado a cabo estas clasificaciones, el sistema SSE puede usar los datos internos y externos para calcular puntuaciones de riesgo en tiempo real para los trabajadores, las aplicaciones y los sitios web. Ahora podrás deshacerte de gran parte de la infraestructura de seguridad heredada y pasar a la siguiente fase en la que SSE alcanza un nuevo nivel de seguridad.

Paso 3: implementación de la confianza adaptativa continua y la ampliación de los servicios

Hasta este punto, la experiencia que han vivido los trabajadores no ha cambiado mucho. En el paso 3, la experiencia cambia de forma considerable porque la seguridad se adapta en función del contexto.

RECUERDA

La confianza adaptativa continua evalúa el contexto para equilibrar el riesgo frente a la confianza, ofreciendo el tipo de acceso adecuado en cualquier momento dado. Te permite definir con mucho más detalle las políticas de seguridad. Además, formula alertas o sugerencias con más frecuencia cuando los trabajadores están a punto de hacer algo peligroso, guiándolos hacia acciones aprobadas.

Con SSE, los profesionales de la seguridad saben qué datos son confidenciales y qué aplicaciones y sitios web suponen un riesgo. Al combinar esto con capacidades como DLP, el personal de seguridad puede controlar con precisión qué hacen los trabajadores con los datos confidenciales, a un nivel de seguridad sin precedentes. En lugar de ser una simple decisión de bloqueo o permiso, el acceso se convierte en un proceso continuo.

La confianza adaptativa continua también te permite añadir más servicios. Por ejemplo, supongamos que un médico quiere visitar un sitio web que se considera peligroso. Después de una advertencia, el médico sigue queriendo acceder a él. SSE podría desviar después al médico a una sesión de aislamiento remoto del navegador (RBI), un navegador que se ejecuta en una máquina virtual en el proveedor de SSE, para reducir aún más el riesgo. Se pueden añadir también otros servicios avanzados según sea necesario.

Paso 4: gestión proactiva del riesgo con un análisis y puntuación dinámicos

En el paso 4, el equipo encargado de SSE puede iniciar el proceso de búsqueda proactiva de riesgos y sacarlos del entorno. Un método para medir el progreso es hacer un seguimiento de las puntuaciones de riesgo de los trabajadores, aplicaciones y sitios web. El objetivo es mostrar una reducción en la cantidad de tráfico hacia sitios que suponen un riesgo y en la frecuencia de las acciones arriesgadas. Otro método es reducir los derechos mediante el seguimiento de los patrones de uso y la eliminación del privilegio excesivo.

En este punto, algunos de los controles de seguridad de mayor nivel, como DLP y la neutralización de amenazas, pueden convertirse en el foco de atención, aumentando las capacidades de CASB, SWG, ZTNA

y el *firewall* como servicio (FWaaS). En SSE, estos controles funcionan mejor que cuando eran independientes a nivel local y permiten que se haga mucho más con ellos. Por ejemplo, los reconocedores basados en el aprendizaje automático permiten a DLP identificar documentos confidenciales y reaccionar a ellos en tiempo real.

CONSEJO

La gestión de la experiencia digital (DEM), la gestión de la posición de seguridad en la nube (CSPM) y la gestión de la posición de seguridad en SaaS (SSPM) mejoran aún más la gestión del riesgo. Añaden métodos avanzados para garantizar una disponibilidad y rendimiento coherentes y para encontrar y solucionar errores de configuración. SSE permitirá que existan incluso más servicios avanzados como estos en el futuro.

RECUERDA

Tu situación única es la que te indicará cuáles son los elementos concretos de todos los pasos. Pero, a grandes rasgos, los pasos explican el proceso que seguirán la mayoría de las empresas para implementar SSE de forma completa.

Transformación de la red y del resto de la seguridad

CONSEJO

La implementación de SSE es un paso importante no negociable para SASE. Pero para alcanzar el nirvana de seguridad que todos queremos, el resto del panorama de la seguridad más allá del SASE también debe evolucionar, de manera que todas las piezas importantes funcionen al unísono. La mayoría de las empresas están cambiando a un modelo de trabajo desde cualquier lugar en el que están claros los beneficios de la seguridad en todo momento y lugar. Estos se aleja naturalmente de la conectividad basada en una red privada y las VPN, además de proporcionar la simplicidad y las ventajas en costes de SSE.

El principal aspecto a tener en cuenta es cómo al adoptar SSE (y SASE), se simplifica la infraestructura tecnológica en general. En el modelo antiguo, los controles de seguridad para protegerse frente al acceso no autorizado se colocaban en la red de la empresa porque esa red era la única ruta a los datos. En el nuevo modelo, los distintos puntos de presencia del proveedor de SSE se convierten en rutas a los datos, ofreciendo así no solo control de acceso, sino también una exhaustiva inspección del tráfico. La red subyacente puede centrarse entonces en su misión general para mover los datos de manera rápida y eficaz.

Los sistemas de gestión de identidades y accesos (IAM) llevan a cabo el importante trabajo de autenticar a los trabajadores. Muchos de estos sistemas ya son muy configurables a través de las interfaces de programación de aplicaciones (API). También se han diseñado para integrarse con otros sistemas, una característica necesaria en cualquier implementación de SSE. Las mejoras de la tecnología IAM ofrecen incluso más contexto,

supervisión y capacidades de autenticación avanzadas de las que pueden beneficiarse SASE y SSE. SSE consigue incluso más beneficios de las plataformas de protección de endpoints (EPP). Estas recogen señales importantes (generando así más contexto), llevan a cabo una supervisión detallada, e incluyen mecanismos para controlar la configuración de seguridad y comportamiento. Sincroniza tu plan de implementación de SSE con una evolución del EPP correspondiente para que puedas obtener el máximo valor de tus inversiones de seguridad.

SASE y SSE acelerarán el cambio en el papel que desempeña tu centro de datos. Cuando la nube se convirtió en algo tan importante, el centro de datos perdió su posición como el centro de actividades relacionadas con la seguridad. SSE traslada la seguridad del centro de datos a la nube.

RECUERDA

Los centros de datos continuarán desempeñando un papel importante en la mayoría de las empresas por una serie de buenos motivos, como presiones en los costes, requisitos reglamentarios, gestión de riesgos y utilidad de algunos tipos especiales de infraestructuras informáticas. El centro de datos será ahora uno de los muchos lugares donde se alojan las aplicaciones importantes protegidas por SSE.

Beneficios empresariales de SSE

El riesgo cibernético es una prioridad para la mayoría de los consejos de administración, pero como ya dejamos claro en el capítulo 2, la seguridad no es un fin en sí misma. Su misión es proteger el valor empresarial que han creado los sistemas que respaldan el negocio. Las empresas se han trasladado a la nube porque tiene sentido desde un punto de vista comercial. El trabajo de la arquitectura SASE, SSE incluido, es proteger las aplicaciones, los datos y los trabajadores. Y a continuación te explicamos cómo se traduce esto en valor empresarial:

- **La seguridad ya no es un obstáculo para la productividad de la empresa.** Se puede mantener la agilidad empresarial y los equipos de seguridad ya no tienen que desempeñar el papel de Dr. No, porque los pasos que quiera dar la empresa ahora pueden emprenderse con la seguridad adecuada. La fricción provocada por la seguridad se reduce drásticamente. Los procesos de desarrollo y mantenimiento de productos se agilizan a medida que la seguridad se incorpora con mayor facilidad. Un SSE basado en la nube es perfectamente adecuado para mantener la seguridad de un entorno multinube.
- **El consejo de administración tiene ahora una mayor confianza en que los tipos de controles que se necesitan para usar los recursos en la nube con seguridad se analizan y gestionan de manera adecuada.** El proceso para gestionar el riesgo relacionado con las personas, los datos y las aplicaciones se convierte en algo mucho más sofisticado,

al igual que los mecanismos utilizados para reducir el riesgo. Con SSE, el riesgo puede identificarse de manera proactiva y eliminarse de la empresa sistemáticamente. La seguridad en un sentido real sigue a los datos, lo que ofrece tranquilidad al consejo de administración en relación con cómo se protegen los activos más importantes.

- **El equipo de seguridad se hace más homogéneo y se centra más en la empresa.** En lugar de tener a una persona para SWG, otra para CASB y otra más para el *firewall*, dispones de un equipo centrado en una visión general con más información para que pueda actuar de forma proactiva.

RECUERDA

Convertir SSE en una realidad significa hacer realidad un mundo de seguridad mucho mejor, algo que beneficiará a todas las personas de la empresa.

Capítulo **5**

Diez cosas (más o menos) que debes y no debes hacer en tu viaje hacia SSE

Algo muy importante para poder terminar tu viaje hacia una nube ágil y segura es reconocer que tu organización de TI actual no se diseñó para este destino. Es normal que la organización de TI refleje la arquitectura de la tecnología. Así que si hay distintas personas o equipos que se encargan de tus agentes de seguridad para el acceso a la nube (CASB), tus puertas de enlace web seguras (SWG), tus redes privadas virtuales (VPN) y tus *firewalls*, además del equipo del centro de operaciones de seguridad (SOC) y del centro de operaciones de red (NOC), o como parte de ellos, te vas a enfrentar a opiniones contrarias cuando digas: «Oye, vamos a implementar ahora una nueva arquitectura integrada de servicio de acceso seguro en el borde (SASE) y servicio de seguridad en el borde (SSE) que unen también la seguridad y las redes en una ejército poderoso». Por lo general, la gente se resiste al cambio, en parte por miedo a perder el control de algo que les ha costado mucho dominar.

SASE y SSE ofrecen ventajas tácticas que mejoran la calidad de la seguridad y amplían el alcance de sus servicios, además de ofrecer ventajas

estratégicas que pueden acelerar el negocio. En los apartados siguientes, encontrarás una guía para que la adopción de SASE y SSE sea todo un éxito. En primer lugar, te presentamos cuatro principios que harán que tu viaje sea más rápido. Después, te hablamos de cuatro fallos que debes evitar.

Haz que los datos sean el centro de atención

Con SSE, la seguridad sigue a los datos allá donde vayan. Por tanto, no importa si estás creando datos en Google Workspace y en Microsoft 365, en una aplicación de *software* como servicio (SaaS) o en un almacén de objetos en la nube. SSE está siempre ahí para proteger los datos.

Debido a que SSE se convierte en un punto de inspección principal que también puede facilitar la clasificación de los datos, es importante determinar el propósito y la ubicación de todos tus datos. Utiliza este conocimiento para priorizar la protección y el uso adecuado de los datos confidenciales, estén donde estén, de forma que puedas asegurarte de que has hecho el trabajo más importante en primer lugar.

Adopta la integración

En cada paso del ciclo de respuesta ante incidentes, adquirir habilidades de automatización e integración es importante para que puedas unir los componentes de seguridad y se conviertan en una máquina sintonizada con precisión. Este proceso implica la extracción de información de varios sistemas, integrarla para analizar qué está pasando, formar el equipo adecuado, y emprender acciones automatizadas siempre que sea posible.

SSE integra los servicios de seguridad fundamentales para proteger la nube, pero forma parte de un mayor ecosistema de importantes servicios de seguridad. Las herramientas de gestión de identidades y accesos (IAM), plataformas de protección de *endpoints* (EPP) y administración de eventos e información de seguridad (SIEM) son algunos de los componentes clave que trabajan al unísono con las funciones específicas de SSE para proporcionar una seguridad integral y facilitar un diagnóstico rápido de los problemas que permita solucionarlos.

Recuerda que en la nube también hay tipos malos

SSE y SASE son un gran paso adelante en el alcance y calidad de la seguridad. Es razonable que se sientas satisfecho una vez que ya están en marcha los aspectos fundamentales. Pero recuerda, los atacantes

también usan la nube para mejorar su juego. El porcentaje de *malware* que llegó a través de aplicaciones en la nube aumentó de un 50 % en el segundo trimestre de 2020 a un máximo sin precedentes del 68 % en el segundo trimestre de 2021, según el *Cloud and Threat Report* de Netskope (`www.netskope.com/blog/july-2021-netskope-cloud-and-threat-report`). SSE te impulsa hacia adelante y te coloca por delante de los tipos malos, pero debes aprender a adaptarte continuamente para seguir en cabeza.

Reconoce que la seguridad es una parte clave de la estrategia empresarial

La seguridad debe formar parte del debate sobre estrategia empresarial desde el principio. Mostrar entusiasmo por las aplicaciones y la nube no tiene sentido si esas aplicaciones y las personas que trabajan con ellas no están protegidas. La buena noticia es que SSE ayudará a convertir los equipos de seguridad en un catalizador empresarial. Si el equipo de seguridad comprende los objetivos de la empresa y sus ramificaciones de seguridad, el equipo podrá decir que «sí» con mayor frecuencia porque tiene más poder para proteger cualquier cosa que quiera hacer la empresa.

CONSEJO

Para que una adopción de SSE y SASE tenga éxito, los promotores del programa deben explicar que los beneficios de proteger la nube son importantes a nivel de la estrategia en general. El mensaje: hemos invertido en la nube para transformar nuestra empresa y conseguir mejores resultados. Ahora, debemos proteger esa inversión. La ilusión por conseguir y proteger estos resultados será la mejor motivación para adoptar SASE y SSE con entusiasmo.

No pienses en silos

SASE y SSE solucionan los peliagudos problemas que suelen acompañar a los proyectos relacionados con la nube. Evita los intentos para implementar CASB, SWG y el acceso a la red Zero Trust (ZTNA) como proyectos independientes, ya que añadirás más proveedores nicho que harán que todo sea mucho más complejo. El objetivo es proteger la nube con una plataforma integrada que tenga en cuenta el contexto. Encontrarás resistencia al cambio que conllevan SASE y SSE.

ADVERTENCIA

Un gran error es ralentizar el proceso haciendo frente al problema a partir de los silos de TI convencionales. Estos «cilindros de excelencia» perpetúan formas de pensar anticuadas en el nuevo mundo. La seguridad no se debe ya categorizar como simplemente una cuestión de red. No mantengas una conversación de red sobre un problema de seguridad. SSE se ha convertido ya en el punto crítico de control y visibilidad de la seguridad como parte de una arquitectura SASE totalmente funcional.

No implantes antiguas reglas

La gente suele tener miedo a los *firewalls* porque han acumulado capas de reglas creadas por persona que ya se han ido. Lo mismo puede pasar con otras tecnologías de seguridad que requieren reglas y ajustes de configuración complejos para conseguir los resultados deseados. SSE es diferente. Aunque siguen existiendo reglas y configuración, una gran parte del trabajo se consigue con la definición de políticas que describen los resultados. Cuando se implementa de forma eficaz, SSE gestiona los pormenores de las interacciones entre reglas por su cuenta. Así que no te preocupes por la configuración de tu antigua tecnología. En lugar de ello, céntrate en los resultados de seguridad que deseas y utiliza SSE para conseguirlos.

La mayoría de los productos SSE ofrecen también una gestión de la posición de seguridad en la nube y una gestión de la posición de seguridad en SaaS que te ayudarán a hacerlo bien y que siga funcionando correctamente.

No odies el centro de datos

Ahora que vas a adoptar SASE y SSE, es fácil pensar que el centro de datos tradicional no es importante. Siempre tendremos centros de datos de alguna manera; al fin y al cabo, la nube no es más que una colección de centros de datos con acceso a través de interfaces de programación de aplicaciones (API). El nuevo objetivo del centro de datos es ser un lugar para las aplicaciones y cargas de trabajo de procesamiento importantes. El centro de datos ya no desempeñla el papel principal en la infraestructura de seguridad, pero todavía tiene un papel secundario importante.

No temas al cambio

No dejes que el miedo a SASE y SSE te detengan. Sí es cierto que hay un cambio en la arquitectura y nuevos productos que tendrás que aprender a dominar, una tarea difícil porque los productos interactúan con todas las personas de la empresa. Una implementación de SSE te enseñará muchas cosas sobre tus compañeros, tus datos, tus aplicaciones y sobre los sitios y aplicaciones de terceros. Estos conocimientos abrirán después la puerta a una mayor automatización para encontrar errores y poner en marcha respuestas eficaces. En comparación con tu posición de seguridad actual, vivir en el nuevo mundo será como alcanzar el nirvana.

SSE es la pila de seguridad con la que conseguirás una arquitectura SASE eficaz. En este libro te decimos qué debes hacer para que SSE sea realidad hoy.

En el viaje a SASE deben acompañarte socios de confianza con plataformas realmente integradas y no proveedores que vendan humo y solo escriban «SASE» y «SSE» con letras grandes en su publicidad. Este libro es una guía práctica para implementar SASE y SSE, que explica por qué ambos conceptos son fundamentales para conseguir una seguridad centrada en la nube y las arquitecturas de red del futuro, además de cómo invertir y diseñar un servicio de seguridad en el borde (SSE) hoy en día.

Dentro encontrarás...

- La definición de SASE y SSE
- Explicación del papel crítico de Zero Trust
- Cómo proteger los datos empresariales críticos en la nube
- Cómo acelerar el rendimiento de tus trabajadores remotos
- Cómo evitar errores de diseño para SSE y SASE

Los líderes de Netskope, **Jason Clark** (responsable de Seguridad y director de Marketing) y **Steve Riley** (director de Tecnología) cuentan con gran reconocimiento en el campo de la tecnología informática en la nube, ciberseguridad y redes, y tienen décadas de experiencia en organizaciones de todo el mundo, incluidas Gartner, Optiv, Riverbed y Websense.

Visita Dummies.com®
para ver vídeos, fotografías paso a paso, artículos con instrucciones o comprar productos.

ISBN: 978-1-119-89738-5

para dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.