LOS 7 ERRORES QUE SE DEBEN EVITAR AL SELECCIONAR UNA SOLUCIÓN SSE

Diseñar el Security Service Edge (SSE) sobre una base de Zero Trust

Por:

Sanjit Ganguli,
VP Estrategia de Transformación y CTO en Zscaler

Nathan Howe,
VP de Tecnologías Emergentes y 5G en Zscaler

Patrocinado por:

Los 7 errores que se deben evitar al seleccionar una solución SSE

Tabla de contenido

SSE. ¿Qué es y por qué debería preocuparme?

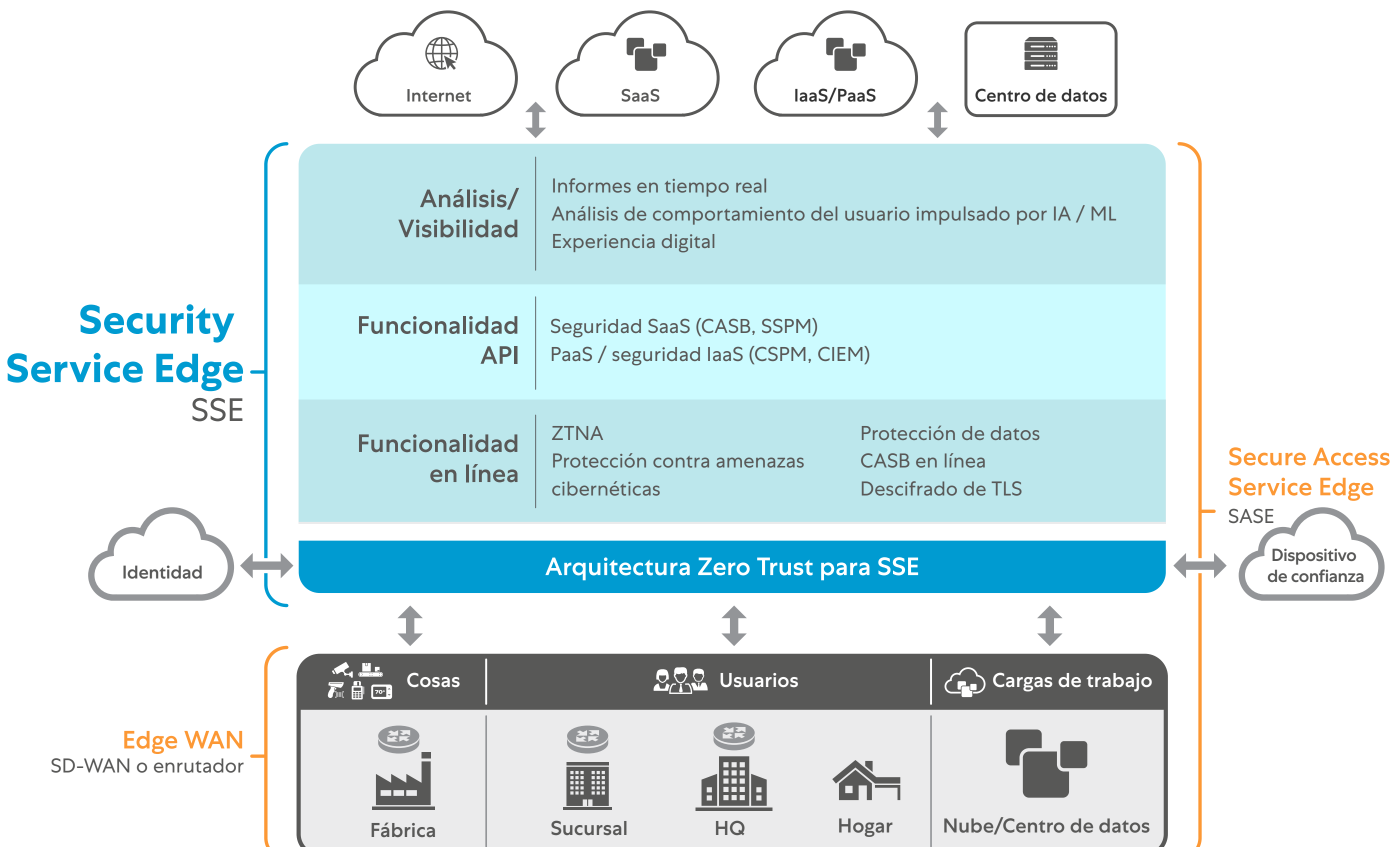

Figura 1: Secure Access Service Edge (SASE), incluye el SSE para la toma de decisiones respecto a las políticas y la aplicación de estas. El SASE requiere el uso de soluciones de conectividad dedicadas desde la entidad solicitante y el perímetro de seguridad donde se aplica la política.

El SSE es la especificación de Gartner respecto de la decisión sobre las políticas y la aplicación de estas como componentes del SASE. El SSE promete seguridad y conectividad consolidadas, simplificadas y entregadas en la nube.

La simplicidad arquitectónica es siempre un beneficio para una empresa, especialmente cuando esa simplicidad minimiza la deuda técnica y acelera el negocio. Pero en muchas organizaciones, la seguridad se considera un inconveniente, un obstáculo que crea cuellos de botella, un guardián que limita la agilidad o un impedimento para el éxito en el negocio. El SSE contrarresta esos estereotipos. Dentro de un entorno de SSE, la seguridad ofrece protección y control ofrecidos como un habilitador del progreso empresarial.

Algunos antecedentes: presentado en 2019, el marco del SASE tiene como objetivo guiar a las empresas a través de su recorrido de digitalización, un recorrido impulsado principalmente por la adopción de la nube y la movilidad. El SASE reúne el acceso a la red y la seguridad, y sirve a ambos desde el perímetro de la nube (que está altamente distribuido) **(ver Figura 1)**. De esa manera, el SASE garantiza que la seguridad ya no sea centralizada y que las conexiones seguras se puedan realizar desde y hacia cualquier lugar.

Considere cómo se conecta un teléfono móvil a varias redes celulares e inalámbricas. No existe una solución de enrutamiento de red dedicada, pero el usuario requiere controles de seguridad para el tráfico entre la fuente y el destino. De manera análoga, el perímetro, la red o la ubicación a los que se conecta el usuario no deberían importar cuando se protege el tráfico empresarial. Esto es lo que ofrece el SSE

Las empresas de ciberseguridad rápidamente se subieron al tren del SASE. Algunos especialistas en marketing se apropiaron cínicamente del término para beneficiar su marca, insinuando que el "Acceso" en SASE los hacía SASE-compliant (o a la competencia non-compliant): "Tengo una función de red, por lo tanto soy SASE; no estás construyendo rutas de red, por lo que no eres SASE".

Figura 2: Ofrezca acceso de entidad a entidad validado y basado en políticas en el perímetro para un mundo móvil y en la nube. SSE le permite ofrecer seguridad al usuario en el perímetro sin comprometer el rendimiento y, al mismo tiempo, anular todos sus firewalls y VPNs.

SSE se refiere al conjunto de servicios de SASE utilizados para proteger el tráfico empresarial. El SSE garantiza que el usuario correcto (o la tarea correcta) reciba acceso, de manera segura y bajo el control de TI de la empresa, a las aplicaciones y servicios correctos. Esos servicios pueden ser tareas en una IaaS o PaaS, aplicaciones SaaS o servicios de Internet como LinkedIn o YouTube. El acceso al servicio debe otorgarse siguiendo los controles de Zero Trust Access (ZTA), detallados con mucha más profundidad en el [segundo error que se debe evitar](#).

Para cumplir con estos objetivos ambiciosos, un proveedor de soluciones SSE debe proporcionar una solución global, altamente disponible, escalable e independiente de la red que ofrezca una política consistente, acceso a Zero Trust y una experiencia digital rápida.

Sin esta funcionalidad y disponibilidad, las soluciones de SSE no pueden ofrecer protección y disponibilidad extendidas **(ver Figura 2).** A diferencia del SASE, el SSE no prescribe ninguna conexión ni método de acceso. Se presupone que el SSE funcionará en cualquier red y proporcionará controles a cualquier servicio autorizado, en cualquier lugar donde ese servicio pueda estar.

El ideal de SASE es fusionar conectividad y protección, pero en un entorno empresarial, ese emparejamiento solo funcionará si es transparente para los empleados que son usuarios finales. La conectividad es directa, ya sea de usuario a aplicación, de aplicación a aplicación, de tarea a tarea, de lo que sea a lo que sea. Los usuarios nunca deben pensar esto: "Oh, tengo que conectarme a la red antes de poder trabajar". En su lugar, su enfoque debería ser e "Voy a hacer mi trabajo ahora".

Este ideal integrado simplemente no se puede lograr en entornos empresariales que dependen de una infraestructura heredada de red y seguridad. En ese modelo de arquitectura antiguo, la seguridad estaba centralizada y el tráfico de datos, independientemente de la ubicación (por ejemplo, remota o en una sucursal), independientemente de la fuente (por ejemplo, el usuario, la aplicación o la tarea), e independientemente del destino (por ejemplo, Internet, la nube, el centro de datos), primero tenían que conectarse y enrutarse a través de la red corporativa a (y a través de) la ubicación física de los controles de seguridad basados en dispositivos de hardware.

El verdadero valor empresarial de la transformación digital impulsada por SSE

La adopción de SSE puede requerir una transformación digital empresarial significativa. Pero aceptar ese cambio puede generar un impacto tangible:

Control:

El SSE comienza con zero. El SSE valida a cada persona, máquina, tarea, red y perímetro. Sin una identificación correcta junto con el contexto proporcionado por el análisis conductual, no hay acceso, lo que permite que una empresa controle por completo qué o quién accede a cualquier servicio dentro de la empresa.

Conectividad directa:

La aplicación de la política de SSE se hace entre la entidad de origen y el servicio de destino. Las decisiones de acceso se toman por aplicación, no a nivel de red.

Seguridad impulsada por el negocio:

Las políticas sobre qué entidades pueden conectarse con qué servicios se definen utilizando un privilegio mínimo. Los usuarios, máquinas, tareas, etc., solo pueden conectarse a lo que tienen permitido y nada más. No hay otra conectividad disponible y todos los demás accesos están bloqueados.

Aplicación global:

El SSE debe tener una aplicación global para que cualquier entidad pueda tener controles aplicados en la ruta de acceso según el contexto proporcionado por la política, los motores de conocimiento y los aprendizajes externos (monitoreo de amenazas, engaño, etc.). Esta aplicación global debe adaptarse a los requisitos de su empresa.

Servicio integral:

El SSE proporciona una evaluación completa en línea para inspeccionar el tráfico a escala y a profundidad. El SSE brinda protección contra amenazas avanzadas, defiende los activos corporativos (la nube y más), evita la pérdida de datos y garantiza el control en línea. Cuando se requiere, la solución proporciona el control del contenido almacenado en los servicios en la nube.

Oscuridad:

El SSE evita el acceso no deseado y la exposición de los activos de la empresa eliminando la superficie de ataque. No es posible atacar lo que no es accesible.

Desde cualquier lugar:

El SSE ofrece esta conectividad para todas las partes de la empresa desde cualquier lugar. El SSE protege y conecta una base de usuarios flexible a la vez que garantiza que las tareas, las cosas y las máquinas puedan moverse, reubicarse y transformarse sin perder el control.

El SSE puede ser un catalizador del cambio en una organización con solo asegurar el negocio de una manera muy integral. Pero no todas las soluciones son iguales. Los líderes de TI que buscan adoptar SSE deben evaluar y seleccionar la solución correcta, una que permita que su organización simplifique la seguridad.

Hay siete errores que se deben evitar en el recorrido de transformación digital empresarial hacia el SSE. Evitar estos pasos erróneos permitirá que esos líderes de TI seleccionen el conjunto correcto de servicios, arquitectura y funciones para cumplir con la propuesta de valor del SSE. Este recorrido no debe atravesar el camino de las "viejas maneras de trabajar", como anclarse a las redes o permitir el acceso general a los servicios, lo que limita la capacidad de transformarse y satisfacer las necesidades del negocio.

Error n.° 1:
Elegir una solución SSE que carece de un historial comprobado de operar una plataforma global en la nube que escale tanto en rendimiento como en disponibilidad

Error n.° 2:
Elegir una solución SSE que no se base en una Arquitectura Zero Trust

Error n.°3:
Elegir una solución SSE que prometa una protección avanzada contra amenazas y prevención de pérdida de datos (DLP) avanzada, pero que no pueda inspeccionar el tráfico cifrado a escala

Error n.° 4:
Elegir una solución SSE que sea "one-size-fits-all" y no soportan opciones de implementación y administración flexibles, escalables y diversas

Error n.° 5:
Elegir una solución SSE que proporcione una experiencia de usuario mediocre al no optimizar la conectividad a las aplicaciones ni diagnosticar las las caídas UX

Error n.° 6:
Elegir una solución SSE que tenga integración y orquestación limitadas con el ecosistema de proveedores externos

Error n.° 7:
Elegir una solución SSE que no pueda mostrar valor fácilmente en un ambiente de producción piloto

¿Quién debería estar leyendo esto?

Migrar a SSE no se trata solo de la transformación de la seguridad e involucra más que solo **arquitectos de seguridad**. Las mejores prácticas descritas en este libro electrónico están diseñadas para **arquitectos de seguridad**, **arquitectos de red**, **arquitectos empresariales**, **arquitectos de nube** y **arquitectos de aplicaciones**.

N.º 1 Error

Elegir una solución SSE que carece de un historial comprobado de operar una plataforma global en la nube que escale tanto en rendimiento como en disponibilidad

En su lugar, considere soluciones SSE que cumplan con:

- Ofrecer un conjunto diverso y global de ventajas para la aplicación de políticas de servicio público con rendimiento, disponibilidad, capacidad y funcionamiento respaldados por SLA. La solución ejecuta la aplicación de políticas de manera local hacia las ubicaciones de los clientes.
- Haber nacido en la nube con la resiliencia, la infraestructura, la diversidad geográfica, las capacidades funcionales mejores en su clase y una óptima experiencia de usuario. Ofrezcan servicios SSE en línea en centros de datos neutrales para cualquier operador y no como un servicio que se ejecute sobre una nube administrada en destino o un proveedor de DC.
- Tener un linaje probado y transparente de escala, crecimiento y entrega, validado por referencias de clientes, informes históricos, certificaciones de terceros y repositorios externos de datos de código abierto (https://www.peeringdb.com/org/12297).

Cómo los proveedores de SSE correctos hacen que esto funcione:

Creando y corriendo una plataforma SSE para varios usuarios a fin de realizar miles de millones de transacciones implica mucho más que el nivel de cómputo y no es algo simple. **La solución SSE será responsable de la protección, conectividad y habilitación de su empresa**, y por lo tanto debe brindar el conjunto de servicios SSE de manera uniforme y oportuna a todas las partes de la organización.

La solución SSE correcta brindará servicios a su empresa a través de un servicio distribuido globalmente. Desde el punto de vista arquitectónico, la manera más eficaz de ofrecerlo es a través de un servicio basado en proxy. Al no estar anclado al estado de la red, un servicio de proxy se enfoca en brindar SSE al acceso de la aplicación, lo que permite una mayor comprensión sin descargar a plataformas adicionales para obtener información como la inspección a escala **(consulte el error n.º 3)**.

Tenga en cuenta que la verdadera arquitectura proxy requiere un esfuerzo significativo de I+D y muchos años de refinamiento para lograr los requisitos de adaptación de la empresa moderna. La solución SSE correcta tendrá una serie de ejemplos de grandes implementaciones donde se demostró que la arquitectura proxy escaló.

Este servicio debe brindarse a través de un conjunto uniforme de perímetros de políticas donde todas las funciones de transmisión de datos de su empresa están protegidas y no solo debe ser el número de nodos, sino el número de sitios garantizados por SLA que ofrecen los servicios necesarios para el cliente. El proveedor de SSE no debe proporcionar PoP públicos si no puede garantizar el SLA en esa región debido a una mala interconexión u otros motivos.

Adoptar SSE significa que consolidará, fortalecerá y compartirá la responsabilidad de la seguridad, la conectividad y el control de su empresa con un proveedor de seguridad de confianza. Este modelo compartido simplificará los medios por los cuales brinda protección y conectividad para sus usuarios, tareas, servicios y sucursales, entre otros. El proveedor de SSE debe ofrecer un conjunto de SLA definidos y probados para garantizar el funcionamiento de su empresa y, al mismo tiempo, brindar protección.

Cuando su servicio empresarial se conecta, necesita una ruta efectiva para consumir la función de destino. Esto solo se puede lograr a través de una solución SSE con interconexión altamente efectiva haciendo sinergia con centros de datos carreer-neutral. Por lo tanto, los controles deben aplicarse en línea, entre el origen y el destino, independientemente de la ubicación de un origen o destino.

Las soluciones que alojan el servicio de seguridad dentro del cómputo central de las nubes, a menudo dentro de hiperescaladores y con puertas de enlace de entrada, como se muestra en la Figura 3 (generalmente denominadas on-wrap services), dependen de los perímetros de entrada distribuidos, pero procesan el control y la aplicación de políticas de manera central, lo que genera latencia no deseada y da lugar a malas experiencias de usuario.

Los proveedores de SSE deben tener una plataforma en la nube demostrada, completa, masiva y escalable. Más allá de los SLAs, la plataforma SSE también debe proporcionar evidencia de escalabilidad, estabilidad, disponibilidad y despliegue geográfico, etc. Para validar esta revisión, consulte los datos históricos proporcionados públicamente y hable con los clientes existentes para comprender sus experiencias.

Aplicación de políticas de perímetro uniforme

El conjunto de perímetros de servicio de un proveedor de SSE debe ofrecer la aplicación de políticas. No pueden ser perímetros de conectividad a una red más grande, basada en la nube, solo para enrutar o "poner en vía de acceso" su tráfico con la infraestructura de aplicación central. Dichos esquemas no cumplen con el propósito de proporcionar servicios de alta eficacia y baja latencia

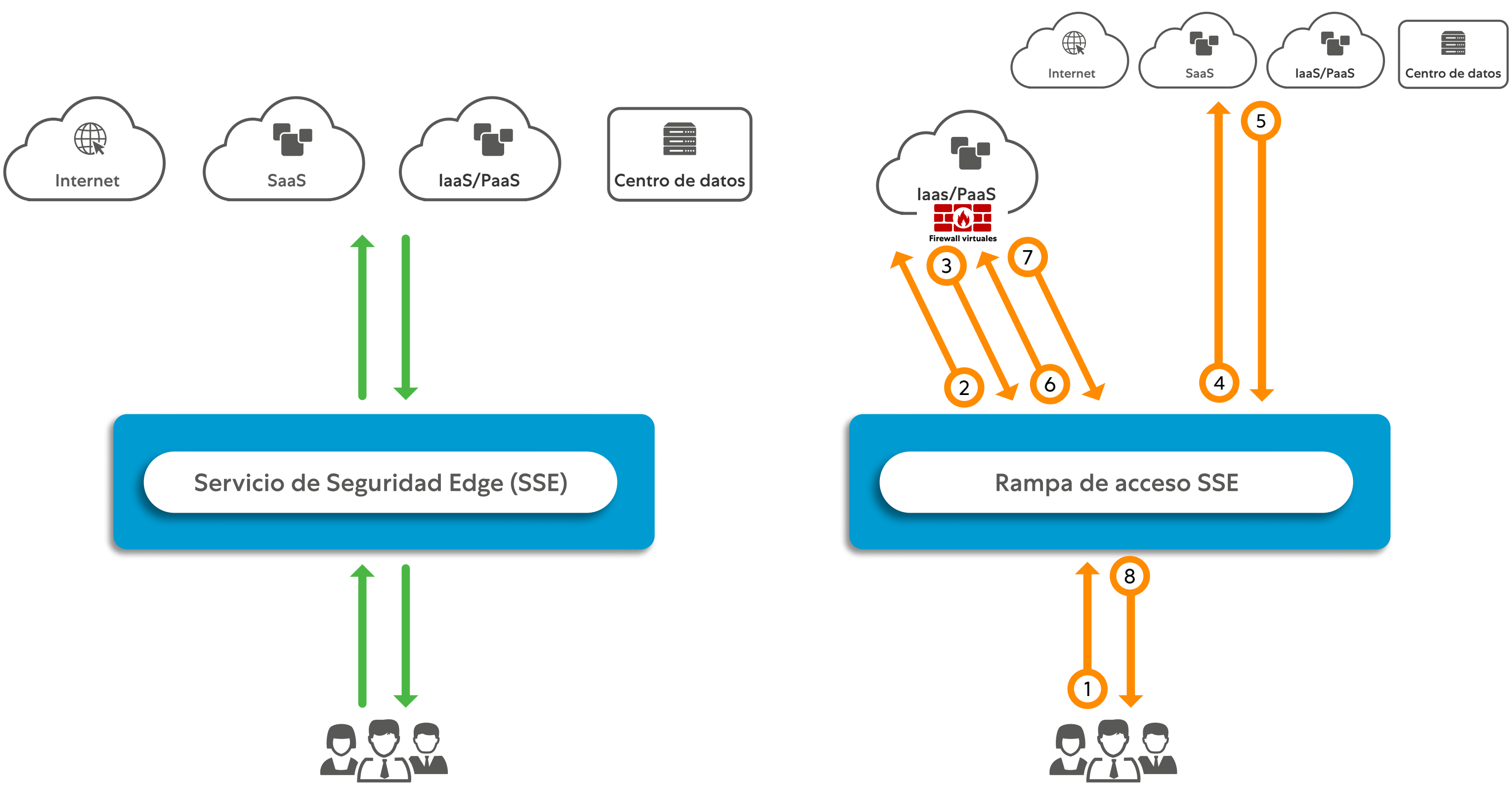

Figura 3: Los servicios SSE en línea (izquierda) aplican controles de seguridad al tráfico en línea. Los controles de seguridad en la vía de acceso (derecha) proporcionan puertas de enlace de ingreso en el perímetro solo para hacer el reenvío a un control central alojado en la nube, lo que aumenta la latencia, genera ineficiencia y brinda una experiencia de usuario deficiente.

El proveedor debe tener las siguientes consideraciones con respecto al diseño, asegurándose de que los perímetros cumplan con lo siguiente:

- Deben estar alojados en ubicaciones vitales de interconexión dentro de centros datos carrier-neutral. lo que garantiza una latencia mínima entre el origen y el destino. Cuando evalúe a un proveedor de SSE, revise las estadísticas de las referencias públicas como PeeringDB y las implementaciones de socios (**consulte el error n.° 6 para obtener detalles sobre la integración de socios**).
- Deben ser soportadas por un SLA válido. Esto asegurará la estabilidad de las funciones empresariales e indicará que el proveedor de SSE está trabajando en las regiones para garantizar los SLAs.
- Deben implementarse de manera privada “por cliente” en ubicaciones donde las condiciones locales requieran implementaciones más matizadas, como en un sitio on-prem o de un nodo de cómputo perimetral. (**el error n.°4 contiene más detalles**).
- Deben demostrar una trayectoria histórica de crecimiento del rendimiento.
- Deben ofrecer tolerancia a fallas implementada en modo activo-activo para garantizar la disponibilidad y la redundancia. (El proveedor supervisa y mantiene sus perímetros de servicio público para garantizar una disponibilidad continua).
- Deben promover la privacidad de los datos para garantizar que el tráfico de clientes no pase a ningún otro componente dentro de la infraestructura y que nunca se almacenen datos en el disco.
- Proveer controles uniformes a los recursos de la empresa en todos los servicios edge y sin tráfico "de acceso" o ruta desde los servicios edge remotos a las ubicaciones centrales.
- Deben proporcionar protección a escala global para proteger todos los servicios empresariales una vez que se detecte una amenaza.

¿Qué debo tener en cuenta?

- Perímetros públicos que no proporcionan cumplimiento. En su lugar, el tráfico de acceso va hacia centros de datos de cumplimiento más grandes donde los recursos de cómputo están disponibles.
- Reclamaciones de cientos de “edges” públicos sin compartir la función ni capacidad de cada edge.
- Perímetros sin SLAs en disponibilidad, rendimiento y resiliencia.
- Servicios perimetrales sin multi-tenance que forza el tráfico a través del acceso o la ruta hacia otras ubicaciones.
- Servicios SSE que no tienen evidencia comprobada de implementación con clientes grandes.
- Servicios sin información pública de consumo sobre la estabilidad y disponibilidad del servicio.

Resultados:

Seleccionar una solución de SSE que se adapte a su empresa es una inversión fundamental pero, más importante aún, que lo apoye a lograr sus objetivos a futuro. La escalabilidad no es simplemente el mecanismo para construir; sobre todo, esta sirve para abordar las necesidades de su empresa sin sacrificar la función, estabilidad y protección de su negocio seleccionando una solución que haga lo siguiente:

- Proporcione evidencia y transparencia de su implementación diversa y global.
- Haya documentado y valide SLAs para la pérdida o degradación de los servicios de SSE.
- Haya implementado en un gran número de clientes de tamaño y complejidad similares a los de su empresa.
- Tenga información pública que se pueda consultar para cada PoP utilizando herramientas públicas (por ejemplo, PeeringDB).
- Ofrezca todas las funciones críticas en todos los sitios sin tráfico de retorno.
- Proporcione protección en línea entre el origen y el destino.
- Esté diseñada para la infraestructura y la resiliencia operativa y funcional.
- Se pueda consumir de diferentes maneras en múltiples sitios.

N.º 2
Error

Elegir una solución SSE que no se base en una Arquitectura Zero Trust

En su lugar, considere soluciones SSE que:

- Solo permitan el acceso a identidades validadas contextualmente, independientemente de la ubicación o la red. Esta ruta menos privilegiada es para todos los servicios, no solo para los usuarios. Al conectar fuentes autorizadas a través de los controles SSE correctos a destinos válidos y nada más, las empresas eliminan el movimiento lateral, que a menudo es aprovechado por los actores que amenazan.
- Se enfoquen únicamente en conectar el acceso dinámico "por sesión". Zero trust no se entrega con firewalls, SD-WAN ni otros servicios de red. Debe ser una superposición independiente de la red.
- Nunca expongan los activos empresariales a una fuente no autorizada, lo que reduce la superficie de ataque y garantiza que se apliquen los controles correctos a todos los servicios.

Cómo los proveedores correctos de SSE hacen que esto funcione:

Zero trust significa, para todas las comunicaciones empresariales, que no se concede acceso alguno desde ninguna fuente (incluidos los usuarios, terceros, redes, etc.) a ningún destino que no cuente con permiso ni aprobación explícitos para hacerlo.

Tradicionalmente, ofrecer Zero trust dentro de una empresa había sido un desafío debido al contexto de red compartida de conectar el origen al destino, confiando en una ruta de red física o lógica para interconectar las dos entidades. La figura 4 resume estas preocupaciones físicas compartidas. No puede crear ni agregar Zero trust con SD-WANs o firewalls.

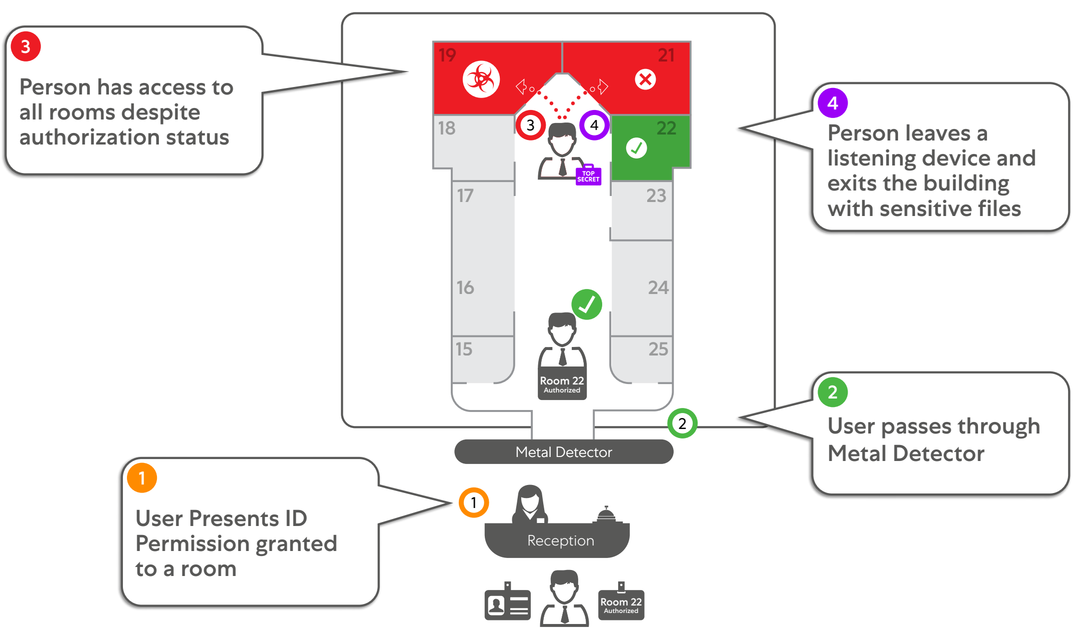

Figura 4: Cómo no habilitar el acceso: el viejo mundo de la analogía de la seguridad de redes. Conectar a los usuarios con su red corporativa es como permitir que visitantes sin escolta deambulen dentro de su sede, lo que podría causar un robo de datos confidenciales.

SSE le ayuda a dar acceso a los usuarios e implementar restricciones en toda la empresa para sus tareas. Al expandir estos controles más allá de los empleados, puede proteger a su empresa de riesgos como una superficie de ataque expuesta o un movimiento lateral de amenazas.

Entre muchas otras cosas, mediante una arquitectura de Zero trust se aplican controles granulares, lo que asegura que cada solicitante se comunique con el destino correcto por sesión, como se ilustra en la Figura 5. Dichas reglas requieren conocimiento de las entidades de origen y destino y es por ellas que la mayoría de las empresas comienzan su recorrido de Zero trust (y SSE) con su base de usuarios. A los usuarios se les suele asignar una identidad, lo que les permite diferenciarse de varios servicios. Sin embargo, como las redes son planas, expuestas y abiertas, el riesgo de que un usuario tenga acceso a más información, solo porque compartió una red, es una preocupación importante para la estabilidad de las empresas.

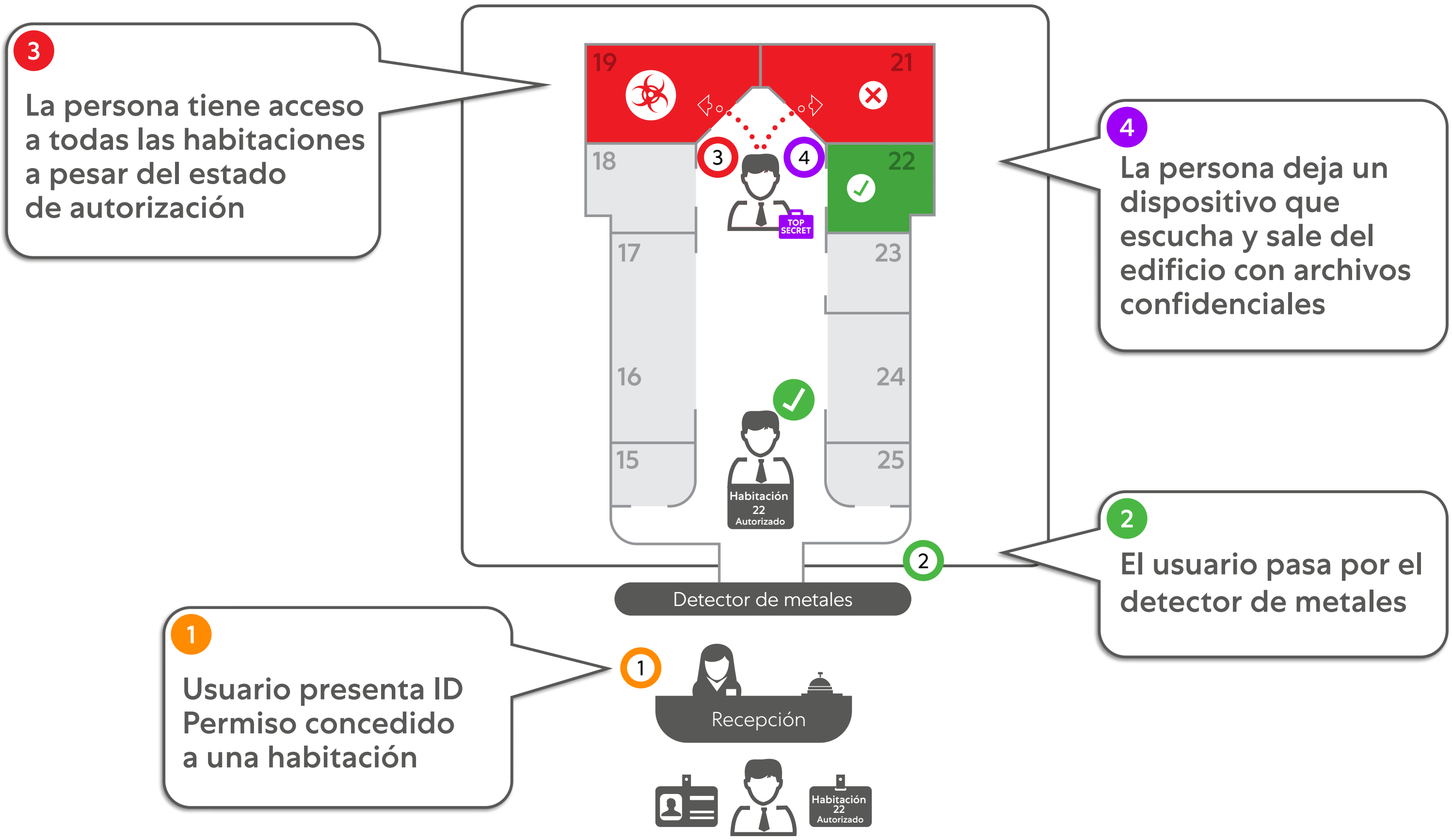

Figura 5: La manera correcta de brindar acceso es a través del control de extremo a extremo. El acceso de confianza cero es como acompañar a un visitante con los ojos vendados a una reunión en su sede y luego acompañarlo a la salida. Dicho visitante no puede deambular ni husmear.

Considere todos los casos de uso empresarial, tales como proteger a los usuarios y resguardar los activos empresariales clave, y aplique controles SSE a todo el tráfico. Establezca conexiones después de revisar dinámica y contextualmente el riesgo de los siguientes cuatro valores de conexión (consulte la Figura 6):

Iniciador de la conexión

¿Cuál es la identidad y la confianza del usuario/dispositivo/red? ¿Cómo diferencia esta identidad el acceso a esta fuente y bajo qué condiciones?

Ejemplo: Sarah de RR. HH. necesita acceso al sistema de RR. HH. alojado en la nube, así como al sistema de gastos alojados de forma interna. El acceso se otorga a través de la plataforma SSE siempre y cuando su identidad y confianza en el dispositivo tengan los derechos definidos para obtener acceso.

Control de la política

¿Qué controles se aplicarán? ¿Dónde y cómo lo harán? Los criterios de control incluyen la eficacia de la ruta, el riesgo y la confianza del iniciador, la función del destino solicitado y la política de la empresa.

Ejemplo: Pierre tiene una identidad válida para acceder a Salesforce. Sin embargo, su empresa solo quiere que vea los datos, pero no quiere que los descargue ni manipule. Por lo tanto, la solución SSE solo le permite a Pierre el acceso para ver el contenido de la aplicación y nada más.

Destino de la conexión

¿A qué servicio accede el solicitante? ¿Es SaaS público o una carga de trabajo interna? ¿Qué controles se van a aplicar? El acceso puede cambiar según el contexto de la política de identidad y control.

Ejemplo: un iniciador válido puede tener aprobación para acceder a un servicio PaaS específico en la nube y, si se trata de un servicio en la nube, el SSE inspeccionará la tarea para asegurarse de que no esté filtrando secretos corporativos. Luego, ese mismo iniciador puede hablar con un servicio interno con una confianza similar, estableciendo así solo una conexión de iniciador a servicio, sin controles adicionales.

Establecimiento de conexión

Finalmente, establezca el acceso usando los datos anteriores, la información condicional sobre las tareas, las capacidades de la red o del perímetro, la política definida por la empresa, etc. La solución SSE debe identificar variaciones como, por ejemplo, una ubicación cambiada, y dirigir el acceso a través de la mejor ruta aplicable.

Ejemplo: una vez que se validen la fuente, el control y los destinos, se hará la conexión para esa sesión y nada más. La aplicación del flujo de extremo a extremo por sesión se muestra en la Figura 6.

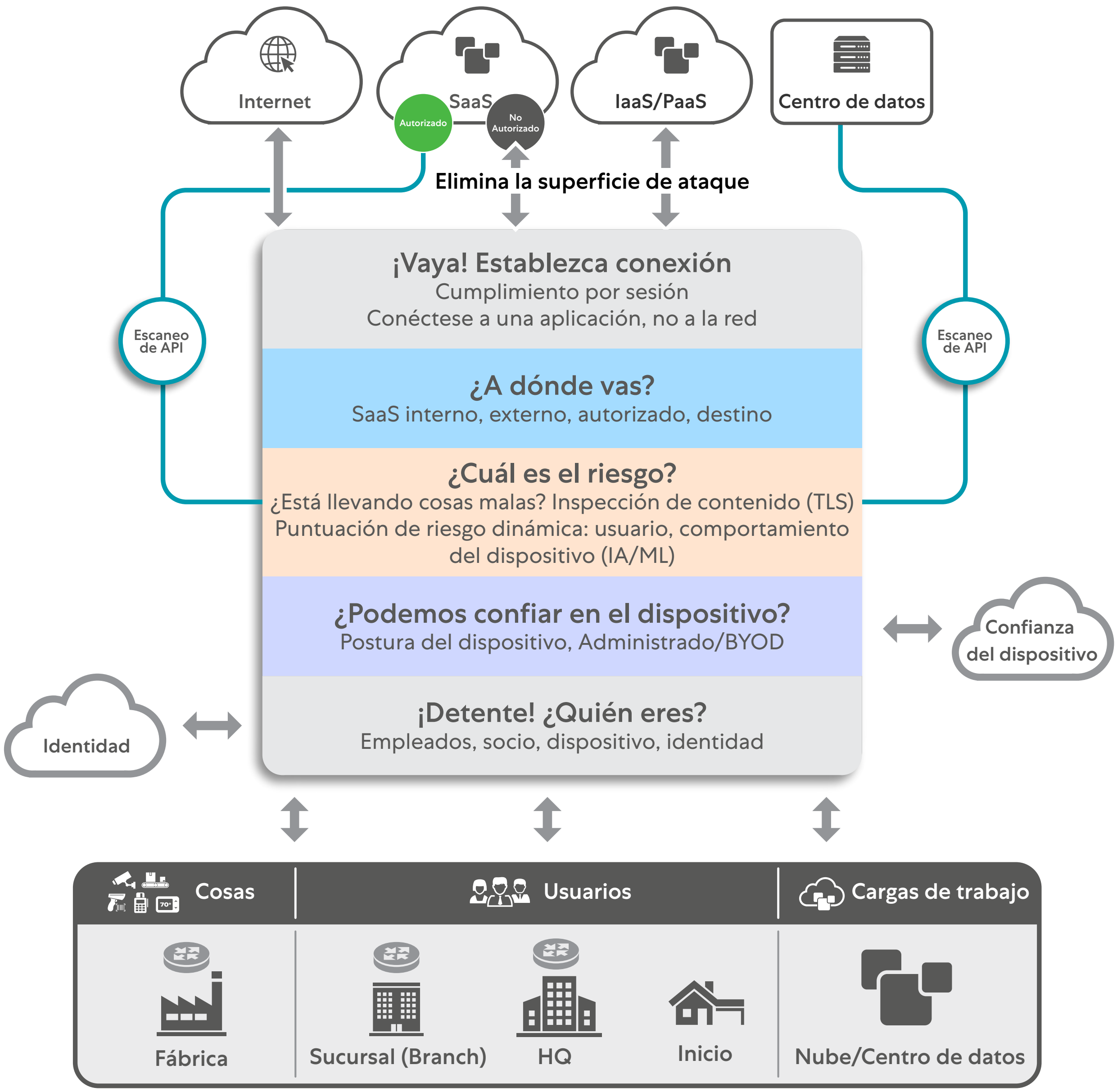

Figura 6: Pasos de una arquitectura de confianza cero; muestra el control y la aplicación de las políticas en cada paso

Definir los controles de conexión dentro de una solución SSE **garantiza que solo la fuente correcta pueda consumir el destino correcto** a través de la solución SSE correcta. Este uso de privilegios mínimos de SSE brinda múltiples beneficios a una empresa, que incluyen los siguientes:

- Aplicar los controles SSE correctos a la fuente correcta.
- Los servicios protegidos por SSE no están expuestos a fuentes no autorizadas, lo que reduce los riesgos de ciberseguridad.
- Reducción de residuos; p. ej., no permitir que un servidor Linux se conecte a un sistema de parches de Windows.
- Visibilidad granular y aprendizaje de flujos: solicitud por acceso, sin red IP a IP.
- Consolidación del acceso basado en la identidad y no en la red, lo que permite que la función (e infraestructura) de redes se racionalice.

Trayectoria por fases SSE con confianza cero:

Al seleccionar una solución SSE que brinde control en todos los siguientes casos de uso y solo el control basado en el usuario, puede extender la protección a todas sus funciones empresariales (consulte la Figura 7):

Usuario a cargas de trabajo

Habilitar el acceso de los usuarios a las tareas significa que puede eliminar el contexto de la red del acceso de los usuarios y, al mismo tiempo, obtener visibilidad de las tareas a las que acceden los usuarios. Esta acción dos en uno generalmente ofrece el valor más rápido.

Considere el control granular para los usuarios en todo el entorno de la aplicación. Por ejemplo, los servicios de Internet como YouTube pueden limitarse al equipo de relaciones públicas de una organización.

Esto permite un mayor desarrollo del inventario de los servicios empresariales y permite reglas más granulares, como el acceso a plataformas aisladas de OT e I+D, sin exponer nunca todo el ecosistema a la base de usuarios.

Acceso de terceros

La implementación del acceso de confianza cero para socios externos elimina el riesgo de la conectividad de red y la superficie de ataque expuesta que deriva del acceso de socios heredados. El control de privilegios mínimos de confianza cero le permite controlar el acceso de los socios desde dispositivos personales o que no son de confianza para que solo puedan acceder a aplicaciones designadas específicamente, y le brinda una mayor visibilidad de la información a la que se tiene acceso.

Los controles de terceros de la solución SSE deben proporcionar varios mecanismos para el control de acceso. Las opciones incluyen acceso de cliente autorizado desde múltiples proveedores de identidad, aplicaciones específicas, acceso aislado solo del navegador o aislamiento completo de acceso a una imagen renderizada que se presenta al tercero (transmisión de píxeles al dispositivo del usuario como BYOD).

De tareas a tareas

Los controles de tarea a tarea son solicitudes de acceso a aplicaciones y servicios. En general, una máquina con Windows solicitará parches de Windows, no de Linux. Por lo tanto, es fundamental que una empresa categorice qué sistemas deben tener acceso a qué.

Al igual que con los usuarios, los controles de tareas deben proporcionar una identidad válida para consumir un servicio. Si la tarea consume recursos públicos, como los servicios de IoT/OT basados en PaaS, el perímetro de seguridad debe validar y comprender su contexto y bloquear cualquier intento de uso indebido.

Por el contrario, si la tarea accede a un servicio local y privado, esto solo se puede hacer a través de controles SSE en línea, después de la aprobación de la identidad, según una validación de confianza cero.

Ubicación a Ubicación

A medida que el acceso y el control evolucionan en su empresa, considere la confianza cero para la conectividad entre sitios. Necesitaría aislar un conjunto de servicios a una red, sitio, VPC, etc. La conexión entre la ubicación y el sitio conocido no debe hacerse en una red compartida. La confianza cero permite que una ubicación válida se conecte a un conjunto válido de tareas dentro de otra ubicación. La confianza cero no utiliza el acceso de red entre enlace y capa; esta requiere conectividad entre aplicaciones de manera uniforme en cualquier sitio, VPC, VLAN, etc.

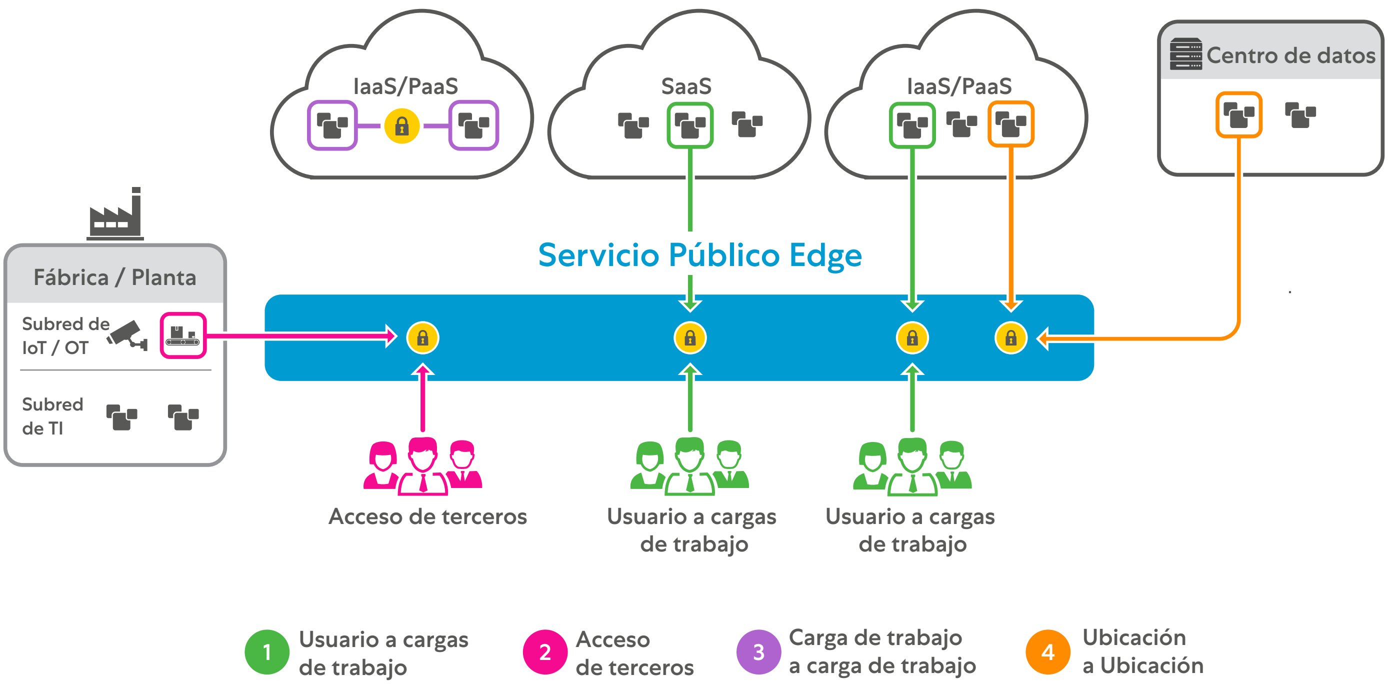

Figura 7: Un enfoque sugerido para la segmentación empresarial. Permitir un enfoque gradual de control, aprendizaje, mayor segmentación y aislamiento como parte de una implementación de confianza cero.

Como ejemplo reciente, cuando los investigadores de seguridad descubrieron la vulnerabilidad Log4j zero-day todos los clientes que ejecutaban la utilidad de registro vulnerable basada en Apache Java corrían el riesgo de una ejecución remota completa del código. Sin embargo, aquellos que adoptaran una arquitectura de zero trust hacían que sus aplicaciones internas quedaran completamente invisibles para Internet; esto implicaba que los atacantes no podrían encontrarlas ni explotarlas y que incluso las versiones susceptibles de Apache Log4j estarían protegidas de esta vulnerabilidad y de otras futuras. Esto habría sido imposible con servicios heredados y expuestos como las VPN y firewalls. **Zero Trust garantiza que solo los usuarios autorizados puedan acceder a las aplicaciones; esta evita el movimiento lateral con la microsegmentación de usuario a aplicación y entre aplicaciones, y puede inspeccionar el tráfico entrante y saliente**.

Algo similar ocurrió con el ataque a Colonial Pipeline, en el que las credenciales de VPN robadas (que no tenían MFA habilitado) dieron acceso a los hackers para moverse lateralmente a través de la red y acceder a datos confidenciales. Una arquitectura zero trust que conecta solo usuarios autorizados a las aplicaciones y no a las redes lo que evita el movimiento lateral, segmentando las comunicaciones de usuario a aplicación y entre aplicaciones.

⚠ ¿De qué debo estar al tanto?

- Evite los servicios SSE que no sigan los principios de la arquitectura Zero Trust, como la publicación especial 800-207 del NIST.
- Asegúrese de que el servicio SSE ofrezca controles Zero Trust a todos los recursos empresariales, no solo a los usuarios.
- Zero Trust no es una función de firewall o SD-WAN. Es independiente de la red y agnóstico de la red. Un SSE de un proveedor que depende de la red puede exponerlo a una deficiencia arquitectónica Zero Trust.
- Asegúrese de que los controles Zero Trust comiencen con Zero acceso; ningún activo empresarial debe ser accedido hasta ser validado.
- Aborde todos los aspectos de su empresa. No limite sus controles Zero Trust a una parte del negocio.

Resultados:

La protección de una empresa y su usuario debe enfocarse de una manera que brinde acceso según la necesidad de saber, con los mínimos privilegios. **Zero trust debe ser el control fundamental al elegir una solución SSE**, de modo que:

- El proveedor de SSE proteja todos los servicios empresariales y valide la identidad de las entidades antes de permitir el acceso; todo lo demás debe estar bloqueado.
- Las soluciones que fuercen la conectividad de red deben evitarse y el acceso debe ser independiente de la red, en todas partes.
- El servicio SSE ofrece una superficie de ataque nulo para sus servicios empresariales privados.

N.º 3
Error

Elegir una solución SSE que prometa una protección avanzada contra amenazas y DLP avanzada, pero que no pueda inspeccionar el tráfico cifrado a escala

En su lugar, considere soluciones SSE que hagan lo siguiente:

- Proporcionen inspección SSL/TLS del tráfico a escala de producción con un impacto mínimo en el rendimiento. Esto requiere una arquitectura de proxy escalable.
- Capturen y analicen conocimientos profundos obtenidos de la inspección para aplicar protección avanzada contra amenazas para el tráfico cifrado y aplicar políticas de clasificación de datos avanzadas para la prevención de pérdida de datos.
- Inspeccionen todo el tráfico, incluido el cifrado, de los usuarios, de los distintos dispositivos, las cargas de trabajo, etc.

Cómo los proveedores de SSE correctos hacen que esto funcione:

Los proveedores de SSE no pueden afirmar tener la mejor protección avanzada contra amenazas y prevención contra la pérdida de datos si no tienen la capacidad de inspeccionar todo el tráfico a escala de producción, incluido el tráfico cifrado.

Tenga cuidado con las afirmaciones de los proveedores de SSE en esta área, ya que mucho depende de la arquitectura subyacente de la solución. Aquellos proveedores de SSE que han creado cloud proxy como cloud-native desde el inicio tienen una clara ventaja en esta área.

Con la mayor parte (estimada en torno al 85 %) del tráfico de Internet encriptado los proveedores de SSE deben inspeccionar este tráfico a escala y en profundidad para obtener la protección adecuada contra amenazas y la prevención de pérdida de datos requerida frente al crecimiento exponencial de los riesgos de seguridad que plantean los canales cifrados. ¿Por qué es tan importante el descifrado SSL/TLS a escala (ver la Figura 8)?

- El cifrado SSL/TLS puede ocultar contenido dañino, como virus, spyware y otros programas maliciosos.
- Los atacantes crean sus sitios web con cifrado TLS y SSL o inyectan contenido malicioso en sitios conocidos y confiables habilitados para SSL y TLS.
- SSL/TLS puede ocultar las fugas de datos, como la transmisión de documentos financieros confidenciales de una organización.
- SSL/TLS puede ocultar la navegación de sitios web que pertenecen a clases de responsabilidad legal.
- La capacidad de controlar e inspeccionar el tráfico hacia y desde los servicios en línea mediante HTTPS se ha convertido en una parte importante de la postura de seguridad de una organización.

Figura 8: La arquitectura de transferencia empleada por algunos proveedores no proporciona la inspección del tráfico cifrado a escala, de manera similar a un puesto de control de seguridad básica que permite que un coche sin revisar la cajuela en búsqueda de carga maliciosa.

Dados estos riesgos, la arquitectura de un proveedor de SSE debe escalarse para funcionar como un proxy intermediario SSL/TLS que proporcione un análisis completo de contenido entrante y saliente y bloquee de inmediato cualquier amenaza detectada en cualquier lugar de la nube.

Los actores de amenazas siguen evolucionando sus herramientas, técnicas y procedimientos cuando su objetivo son organizaciones, incluyendo el abuso de proveedores legítimos de servicios de almacenamiento, como Dropbox, Box, OneDrive y GDrive, para alojar cargas maliciosas. Estas conexiones utilizarán certificados SSL/TLS comodín de estos reconocidos proveedores al entregar las cargas maliciosas, las que, si no se inspeccionan, provocarán un ataque exitoso. Las cargas maliciosas (ejecutables, documentos de oficina, etc.) también son de naturaleza polimórfica, ya que el objetivo es evadir las detecciones básicas de huellas digitales. La arquitectura de los proveedores de SSE debe permitir la extracción completa de cargas útiles de estas conexiones cifradas SSL/TLS y debe ser capaz de desempaquetar y desobfuscar estos archivos para una detección precisa (ver la Figura 9).

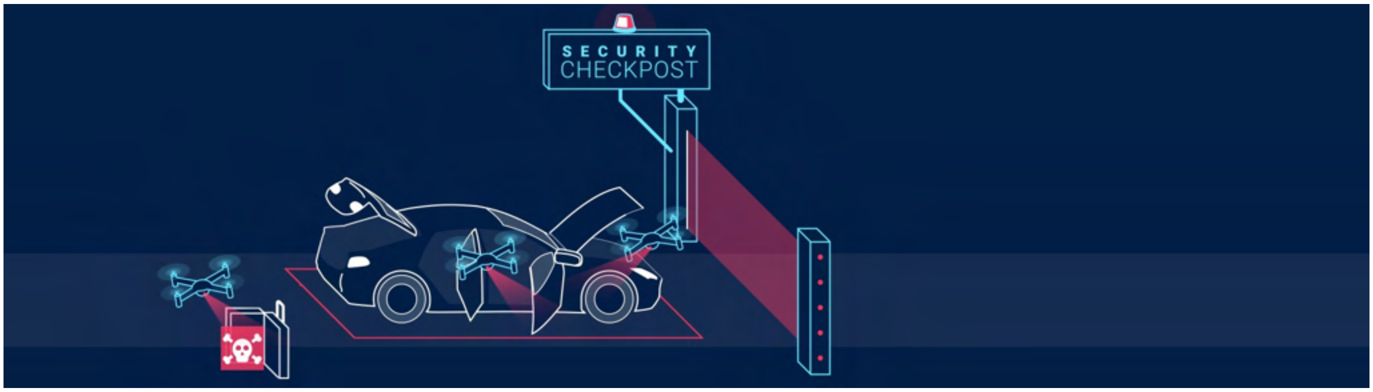

Figura 9: El proveedor de SSE adecuado proporciona una inspección SSL/TLS completa de todo el tráfico que utiliza una arquitectura de proxy, similar a un automóvil que se detiene y se inspecciona por completo antes de que se le permita pasar el puesto de control de seguridad.

Esta protección contra amenazas debería aprovechar muchas fuentes de amenazas de la industria en fuentes de código abierto, comerciales y privadas, así como tener actualizaciones de seguridad frecuentes.

Además de bloquear amenazas, la inspección a escala permite la prevención avanzada de la pérdida de datos. **Los proveedores de SSE deben ser evaluados en función de sus capacidades de clasificación de datos**. Estas deben incluir expresiones regulares (regex) como un mecanismo básico, pero encontrar y clasificar rápidamente datos confidenciales en todos los canales de datos en la nube es un requisito para proteger la pérdida de datos personales, de salud y confidenciales. Esta clasificación requiere inspección SSL/TLS y permite capacidades avanzadas como:

- **Coincidencia exacta de datos**. El SSE utiliza plantillas de índice para identificar un registro de una fuente de datos estructurada que coincida con criterios predefinidos.
- **Toma de huellas dactilares del documento**. El SSE utiliza un depósito de documentos para identificar total o parcialmente los documentos que coinciden al evaluar el tráfico saliente.
- **OCR (reconocimiento óptico de caracteres)**. El SSE detecta datos confidenciales dentro de un archivo de imagen, imágenes incrustadas, capturas de pantalla y textos escritos a mano y cierra todos los canales de exfiltración de datos basados en la nube.
- **Aprendizaje automático.** Los algoritmos preentrenados toman decisiones sobre la sensibilidad de los datos.

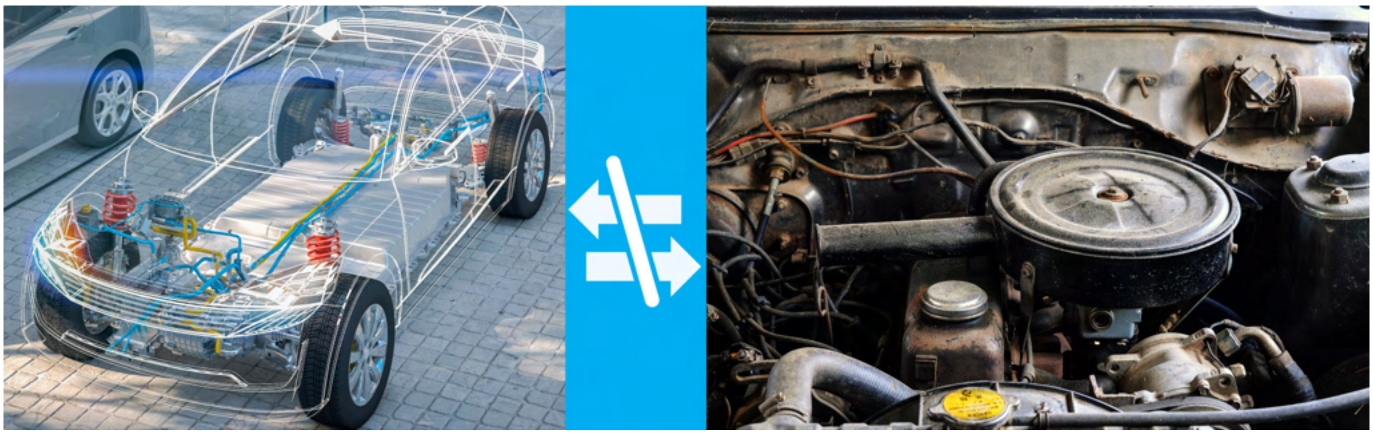

Figura 10: Al igual que un motor de combustión interna no se puede adaptar para que funcione como un vehículo eléctrico, desconfíe de los proveedores que agregan capacidades como la inspección a las arquitecturas heredadas.

SSE incluye la funcionalidad de agente de seguridad de acceso a la nube (CASB) para monitorear y hacer cumplir las políticas entre los usuarios del servicio en la nube y las aplicaciones, y poder inspeccionar el tráfico cifrado en línea tiene una serie de ventajas en este contexto. La inspección puede ser "fuera de banda", lo que significa escanear las API de los proveedores de SaaS para proteger los datos en reposo, o "en línea", el escaneo de los datos en movimiento. Preste especial atención a este último, ya que la inspección en línea evita que los datos se carguen en aplicaciones no autorizadas, que los datos se descarguen en dispositivos no autorizados y que el contenido malicioso se cargue o descargue. El proveedor de SSE también debe permitir un control de acceso granular basado en un amplio conjunto de definiciones de aplicaciones en la nube, controles de tipo de archivo y atributos de riesgo.

Con la adopción de cientos y miles de aplicaciones en la nube, los datos confidenciales de las organizaciones se distribuyen ampliamente en la actualidad. Los dos canales principales de exfiltración de datos son el escritorio en la nube y las aplicaciones de correo electrónico personal. Un buen proveedor de SSE debe brindar visibilidad contextual completa y cumplimiento cuando los usuarios deshonestos cargan datos confidenciales en su Box personal, Dropbox y otros escritorios en la nube. También deben detener la exfiltración de datos en servicios de correo web personales y no autorizados, como Gmail y Hotmail.

Donde la diferenciación entre los proveedores de SSE se hace evidente es qué tan bien su capacidad para descifrar e inspeccionar el tráfico SSL/TLS escala elásticamente según las demandas del tráfico, y que este nivel de inspección se entregue sin preocuparse por el rendimiento. Esto solo se puede lograr con una solución SSE basada en proxy construida con escala desde el principio (ver la Figura 10).

Es importante profundizar en cómo el proveedor de SSE logra esto. Para mantener una latencia mínima para cada inspección de paquetes, el proveedor debe emplear una arquitectura de paso único donde el paquete se coloca en la memoria una vez y los servicios de inspección, cada uno con recursos de CPU dedicados, y que puedan realizar sus escaneos simultáneamente. Los proveedores que atienden estas inspecciones con aplicaciones físicas y virtuales serializadas incurren en una penalización de procesamiento en cada salto, y corren el riesgo de un exceso de latencia aplicada a cada paquete.

Estas ventajas arquitectónicas deben aplicarse a estándares más recientes como TLS 1.3, donde una verdadera arquitectura proxy tiene la ventaja de estar en línea con dos conexiones separadas al cliente y al servidor. Puesto que esto permite volver a montar y escanear todo el objeto, se pueden aplicar protección avanzada contra amenazas, DLP y sandboxing. Asegúrese de que las versiones TLS y las actualizaciones de cifrado sean manejadas sin problemas por el proveedor dentro de su nube; ciertos proveedores basados en hardware pueden forzar las actualizaciones de dispositivos para manejar la carga adicional para el nuevo soporte de cifrado.

También se debe considerar la administración de certificados, dada la complejidad potencial que se puede presentar. Los proveedores de SSE deben permitir la capacidad de usar sus certificados o traer los suyos propios, y permitir la rotación entre los dos a través de la API. Los certificados se deben replicar automáticamente entre los distintos perímetros de servicio.

> Tenga cuidado con los proveedores de SSE que pueden agregar capacidades de inspección de SSL/TLS a los NGFW existentes, que tienen desafíos de escala inherentes. Esto afecta incluso a aquellos proveedores que elevan y cambian NGFW con capacidades de inspección en instancias virtuales en nodos de cómputo de CSP.

¿De qué debo estar al tanto?

Al evaluar la capacidad de un proveedor de SSE para inspeccionar SSL/TLS, asegúrese de validar que la latencia incurrida sea aceptable. Lamentablemente, las arquitecturas sin origen en la nube pueden inducir caídas de rendimiento significativas, especialmente cuando se utiliza TLS 1.2 o versiones anteriores. **La privacidad de los datos también puede ser un problema, por lo que debe comprender las restricciones regulatorias y cómo las maneja el proveedor**. Los proveedores de SSE deben permitir la exclusión fácil de ciertos tipos de datos para mantenerse dentro de las restricciones de privacidad. Los proveedores de SSE nunca deben almacenar datos de usuarios en la nube.

Tenga cuidado con los proveedores de SSE que pueden agregar capacidades de inspección de SSL/TLS a los NGFW existentes, que tienen desafíos de escala inherentes. Esto afecta incluso a aquellos proveedores que elevan y cambian NGFW con capacidades de inspección en instancias virtuales en nodos de cómputo de CSP. Además, tenga cuidado con los proveedores que combinan capacidades CASB fuera de banda con una inspección limitada del tráfico en línea. Proteger los datos en reposo y los datos en movimiento es fundamental.

Evalúe cómo el proveedor de SSE administra los certificados y tenga en cuenta que la fijación de certificados puede ser un problema.

Implementar la inspección SSL/TLS ha sido históricamente un desafío para el negocio por varias razones. **El proveedor SSE debe ser un experto de confianza y debe proporcionar orientación, comprensión e implementación al habilitar la inspección SSL/TLS. La inspección SSL/TLS** no es negociable en el mundo SSE, ya que no debería haber sacrificio de la velocidad sobre la seguridad.

Resultados:

La inspección SSL/TLS a escala con una latencia mínima aumenta significativamente la capacidad de bloquear amenazas al aprovechar el poder de la nube para identificar y proteger los datos confidenciales. Solo los proveedores de SSE con la arquitectura adecuada con origen en la nube ofrecerán:

- Inspección SSL/TLS de todo el tráfico a escala de producción con un impacto mínimo en el rendimiento para la protección de datos y amenazas más profundas.
- Una única arquitectura de análisis de memoria para obtener ventajas de escalabilidad únicas para el descifrado a escala.
- La experiencia para guiar a los clientes a través de los pasos y desafíos para lograr la inspección SSL/TLS.

N.° 4
Error

Elegir una solución SSE que sea "one-size-fits-all" y no soportan opciones de implementación y administración flexibles, escalables y diversas

En su lugar, considere soluciones SSE que:

- Ofrezcan modelos de implementación flexibles para proteger a los usuarios y las aplicaciones dondequiera que se aloje la aplicación, incluidos el centro de datos, la nube pública, la nube privada, el nodo de cómputo perimetral y las instalaciones.
- Proporcionen protección a los usuarios que acceden a aplicaciones en dispositivos de usuarios finales administrados y no administrados.
- Extiendan esas mismas amenazas cibernéticas y protecciones de datos para proteger todas las demás comunicaciones de carga de trabajo a carga de trabajo dentro de las mismas nubes o en múltiples nubes.

Cómo los proveedores de SSE correctos hacen que esto funcione:

Los evaluadores de soluciones SSE deben evaluar la preparación de su entorno para comprender la mejor manera de aplicar las protecciones SSE. Para dar soporte a la variedad de escenarios de implementación, los proveedores de SSE deben permitir servicios Edge tanto públicos como privados.

Cómo los proveedores de SSE correctos hacen que esto funcione:

Los evaluadores de soluciones SSE deben evaluar la preparación de su entorno para comprender la mejor manera de aplicar las protecciones SSE. Para dar soporte a la variedad de escenarios de implementación, los proveedores de SSE deben permitir servicios Edge tanto públicos como privados.

La mayoría de los usuarios se conectarán al SSE a través del servicio Edge público de un proveedor. Estos incluyen puertas de enlace de Internet seguras y agentes de aplicaciones privadas con todas las funciones que proporcionan seguridad integrada. Inspeccionan todo el tráfico bidireccionalmente en busca de malware y aplican políticas de seguridad, cumplimiento y firewall, y necesitan manejar cientos de miles de usuarios simultáneos con millones de sesiones simultáneas. Debido a esto, independientemente de dónde se encuentren sus usuarios, pueden acceder desde cualquier dispositivo:

- Internet y sus servicios Edge públicos que protegen el tráfico y aplican sus políticas corporativas.
- Aplicaciones internas con políticas de acceso y reautenticación aplicadas basadas en las mejores prácticas corporativas de su organización.

Figura 11: Un proveedor de SSE debe ofrecer servicios Edge tanto públicos como privados, que también deben funcionar en armonía entre sí con una gestión centralizada

Es importante garantizar que los servicios Edge públicos tengan capacidades significativas de tolerancia a fallas y que se implementen en modo activo-activo para garantizar la disponibilidad y redundancia. El proveedor debe monitorear y mantener sus servicios públicos Edge para garantizar una disponibilidad continua. Para garantizar la privacidad de los datos, el tráfico de clientes no debe pasar a ningún otro componente dentro de la infraestructura y nunca se deben almacenar datos en el disco.

Sin embargo, pueden surgir situaciones en las que el servicio público Edge no cumpla con los requisitos y, por lo tanto, el proveedor de SSE debe ofrecer opciones de servicio Edge privado (ver la Figura 11). Esta opción extiende la arquitectura y las capacidades del servicio Edge público a las instalaciones de una organización o a la ubicación privada y aprovecha la misma política controlada centralmente que los servicio públicos Edge.

Para un acceso seguro a Internet, los servicios privados Edge se pueden instalar en el centro de datos de una organización y están dedicados a su tráfico, pero deben ser administrados y mantenidos por el proveedor de SSE, con una intervención de la organización casi nula. Este modo de implementación suele beneficiar a organizaciones que tienen ciertos requisitos geopolíticos o utilizan aplicaciones que requieren la dirección IP de esa organización como la dirección IP de origen.

Para el acceso a aplicaciones internas, el servicio privado Edge proporciona una administración similar de las conexiones entre el usuario y la aplicación, y aplica las mismas políticas que el servicio público Edge, alojado en el sitio o en la nube pública, pero nuevamente administrado por el proveedor de SSE. Gracias a este modelo se permite implementar Zero Trust, ya que resulta útil reducir la latencia de la aplicación cuando una aplicación y un usuario se encuentran en la misma ubicación (e ir al servicio público Edge agregaría latencia adicional). Esta opción también proporciona una capa de sustento si se pierde la conexión a Internet. El proveedor de SSE debe distribuir imágenes para su implementación en centros de datos empresariales y entornos de nube privada local.

Para brindar protección Zero Trust a las aplicaciones internas, los proveedores de SSE deben ofrecer una manera de crear una interfaz segura y autenticada entre sus servidores de aplicaciones y los servicios Edge tanto públicos como privados para proteger las aplicaciones internas. **Este mecanismo debe estar disponible en varios formatos**: una imagen de máquina virtual (VM) estándar o una implementación en contenedores en centros de datos empresariales, entornos de nube privada local como VMware o entornos de nube pública como Amazon Web Services (AWS) EC2 y paquetes que se puede instalar en distribuciones de Linux compatibles.

Figura 12: el proveedor de SSE debe admitir una serie de modos de implementación y administración, teniendo en cuenta los usuarios remotos, los usuarios en las sucursales, los usuarios en la sede central, las cargas de trabajo que se comunican con las cargas de trabajo, etc., a través de agentes y máquinas virtuales.

Una vez que se establezca desde dónde se administrarán y aplicarán las políticas de SSE, considere cómo se ofrecerá esta protección a los usuarios y las cargas de trabajo. Es importante considerar varios escenarios (ver la Figura 12):

Para usuarios remotos en dispositivos administrados , el proveedor de SSE debe ofrecer un único agente unificado que reenvíe el tráfico al servicio Edge para un acceso seguro a Internet. El agente también debe proporcionar acceso granular basado en políticas a los recursos internos. Todo esto debería ser automático utilizando la inteligencia integrada en el agente. También debe proteger el tráfico móvil de sus usuarios en Wi-Fi o redes celulares. El agente reenvía el tráfico de usuarios al servicio SSE, que aplica las políticas de seguridad y acceso de su organización dondequiera que los usuarios accedan a Internet y establece un transporte seguro para acceder a aplicaciones y servicios empresariales. Asegúrese de que este agente pueda detectar cuándo un usuario se conecta a una red confiable y, si se detecta una red confiable, si el agente debe deshabilitar su servicio, según lo determine la política. Asegúrese de que estos agentes admitan una amplia gama de sistemas operativos, incluidos Windows, MacOS, Linux, iOS y Android.

Para los usuarios en una sucursal, un método común para reenviar tráfico al servicio Edge es a través de un túnel GRE o IPSec. Sin embargo, el proveedor de SSE debe ofrecer un enfoque alternativo. Una máquina virtual instalada en la sucursal puede simplificar la complejidad y la administración continua de estos túneles y eliminar el movimiento lateral de amenazas eliminando la red enrutable administrada por el cliente. La implementación debe automatizarse e incluir políticas flexibles de direccionamiento de tráfico al servicio Edge con monitoreo de SLA y conmutación por error integrados. Esta opción funciona bien para sucursales medianas, grandes y aquellas que ofrecen servicios locales.

La opción anterior de tratar a cada usuario como un usuario remoto debe considerarse para ramas más pequeñas donde no se ofrecen servicios locales (piense en un modelo de cafetería). Dado que los acontecimientos recientes han cambiado la importancia de la sucursal, esta opción es deseable, ya que no permite a nadie en la red corporativa y evita la posibilidad de movimiento lateral.

Para los usuarios/cosas en dispositivos no gestionados o acceso de terceros a aplicaciones web internas, los proveedores de SSE deben proporcionar una protección SSE similar sin la necesidad de instalar un agente. Dichos usuarios deben aprovechar un navegador web para la autenticación de usuarios que, a continuación, proporcione una protección Zero Trust mediante la publicación de un CNAME específico de la aplicación en su zona DNS para que el navegador web pueda redirigir automáticamente esas solicitudes. O bien, el proveedor de SSE también debe tener una capacidad integrada de aislamiento de navegador en la nube (CBI) para la seguridad sin agente de cualquier dispositivo no gestionado en cualquier lugar. Como beneficio secundario, esto evita por completo la necesidad de un proxy inverso frágil.

Con el CBI, los administradores configurarían la opción SSO de un recurso en la nube autorizado para redirigir al proveedor de SSE. Después de eso, cuando los usuarios intentan acceder a dicho recurso en la nube desde un punto final personal o de un tercero, su tráfico se envía al CBI automáticamente y sin ninguna instalación de software. Reproduce el contenido en píxeles enviados a los dispositivos del usuario, evitando la descarga, copia, pegado e impresión. De esta manera, los usuarios pueden realizar sus tareas laborales desde puntos finales no gestionados sin el riesgo de fugas de datos y cargas de malware, todo ello respetando los requisitos de cumplimiento.

Para cargas de trabajo que se conectan a cargas de trabajo dentro de la misma nube privada virtual (VPC) o centro de datos, la respuesta era la segmentación de red tradicional. Si bien esto tenía sentido en papel, lograr la segmentación de la red en la práctica fue un desafío. Como tal, los proveedores de SSE deben extender sus protecciones de usuario a aplicación a las comunicaciones de carga de trabajo a carga de trabajo. Con la instalación de un agente en la propia carga de trabajo, el proveedor de SSE debe determinar el riesgo y aplicar protección basada en la identidad a sus cargas de trabajo, sin cambios en la red, y debe tener políticas que se adapten automáticamente a los cambios del entorno.

Para las cargas de trabajo que se conectan a cargas de trabajo a través de VPC o CSP o a Internet, los proveedores de SSE también deben extender a estas cargas de trabajo una protección SSE similar a la ofrecida a los usuarios. Como tal, los proveedores de SSE deben ofrecer un mecanismo, generalmente a través de una máquina virtual (disponible en nubes públicas o hipervisores locales), que simplifique el reenvío de tráfico al servicio Edge. El resultado es una amenaza cibernética y una protección de datos para las cargas de trabajo que llegan a Internet, así como una protección Zero Trust para las cargas de trabajo en una nube que accede a las cargas de trabajo en otra nube. Con este enfoque, los proveedores de SSE pueden consolidar múltiples productos (por ejemplo, proxies web, firewalls, puertas de enlace NAT, filtrado de URL, etc.) en una única solución.

Para proteger los datos en reposo en entornos IaaS y SaaS, el proveedor de SSE también debe proporcionar soluciones en el espacio CASB, gestión de derechos de infraestructura en la nube (CIEM) y gestión de postura de seguridad en la nube (CSPM), de modo que puede producirse un escaneo basado en API con aplicaciones IaaS y SaaS. Hacerlo permite identificar y corregir errores de configuración y permisos inadecuados dentro de los entornos de nube, junto con auditorías y escaneos de plataformas SaaS e IaaS para protección de datos y amenazas. Un proveedor de SSE debe ofrecer estas capacidades fuera de banda en estrecha alineación con sus capacidades en línea para aplicar políticas coherentes a los datos en reposo y en movimiento.

La ventaja de que un solo proveedor de SSE proporcione esta amplia capa de protección es que se puede administrar desde un plano de control central con políticas corporativas aplicadas de manera uniforme y dinámica en todos los usuarios/cosa a aplicación y comunicaciones de carga a carga de trabajo.

¿De qué debo estar al tanto?

La implementación de la tecnología SSE depende en gran medida de la complejidad del entorno de la organización. **Por lo tanto, comprender la ubicación, el comportamiento y los requisitos de acceso de los usuarios, así como los requisitos de la aplicación, es muy importante**. Además, ciertos países como China presentan desafíos únicos con el rendimiento debido a los controles de Internet que ni siquiera los modelos de implementación flexibles pueden superar. El proveedor de SSE debe ofrecer soluciones innovadoras para enfrentar estos desafíos.

Resultados:

Implementadas correctamente, estas opciones flexibles, diversas y escalables brindarán a su organización todos los beneficios del servicio de seguridad Edge, independientemente de dónde se encuentre el usuario, o dónde esté alojada la aplicación, e incluso extenderá dicha protección dentro de la aplicación en sí:

- La ventaja de que un solo proveedor de SSE proporcione esta amplia capa de protección es que se puede administrar desde un plano de control central con políticas corporativas aplicadas de manera uniforme y dinámica en todos los usuarios/cosa a aplicación y comunicaciones de carga a carga de trabajo.
- Extender la misma protección para dispositivos administrados a BYOD no administrado y acceso de terceros permite una mayor flexibilidad para contratistas y empleados.
- La seguridad de carga de trabajo permite a los ingenieros de DevOps y CloudOps las mismas protecciones Zero Trust para sus aplicaciones que acceden a otras cargas de trabajo, otras nubes o

N.º 5 Error

Elegir una solución SSE que proporcione una experiencia de usuario mediocre al no optimizar la conectividad a las aplicaciones ni diagnosticar las caídas UX

En su lugar, considere a los proveedores de SSE que:

- Sean transparentes, fáciles de autenticar y siempre activos, lo que garantiza que los usuarios finales de su plataforma SSE tengan una excelente experiencia de usuario utilizando medidas objetivas.
- Correlacionen la mala experiencia del usuario final con las causas subyacentes, ya sea el punto final, la red, la aplicación o la pila de seguridad.
- Aprovechen los partnerships con proveedores de SaaS más populares, como Microsoft 365, para minimizar la latencia entre el servicio privado Edge y la red del proveedor de aplicaciones.

Cómo los proveedores de SSE correctos hacen que esto funcione:

Los puntos de presencia del proveedor de SSE en todo el mundo y las relaciones de intercambio de interconexión de Internet con los proveedores y los comerciantes de aplicaciones proporcionan una alternativa poderosa al “backhauling” y el “hairpinning” requeridos por la seguridad heredada.

Más allá de estos beneficios arquitectónicos, los proveedores de SSE están en una posición única para medir y diagnosticar la experiencia del usuario final en función de su presencia en los puntos finales del usuario y en la ruta de datos de la aplicación. Estas ventajas permiten a los proveedores de SSE comprender la experiencia del usuario desde la perspectiva del punto final del usuario y proporcionar diagnósticos y escalas más profundos al aprovechar la infraestructura del servicio público Edge.

Céntrese en los proveedores de SSE que han integrado una solución de monitoreo (comúnmente llamada **Digital Experience Monitoring** o DEM) en sus agentes existentes y en la infraestructura de la nube. Aquellos proveedores que ofrecen soluciones que requieren agentes adicionales o que están externamente integrados no proporcionarán el mismo nivel de visibilidad y diagnóstico.

La solución DEM que ofrecen los proveedores de SSE debe ser amplia, proporcionando visibilidad de extremo a extremo y solución de problemas de rendimiento del usuario final para cualquier usuario o aplicación, independientemente de su ubicación. Además, debe permitir el monitoreo continuo para los equipos de red, seguridad, escritorio y servicio de asistencia con información sobre los problemas de rendimiento de la aplicación, la red y el dispositivo del usuario final. Por último, debería permitir flujos de trabajo reactivos que ayuden a cerrar los tickets de problemas informados por los empleados y flujos de trabajo proactivos que ayuden a identificar problemas macro (como interrupciones del ISP regional o tiempo de inactividad de la aplicación global) antes de que los usuarios se den cuenta. **Esto debe habilitarse con algoritmos de puntuación basados en el aprendizaje automático, rastreando la experiencia normal frente a la anormal del usuario, la aplicación, la oficina o la geolocalización**.

Este monitoreo debe realizarse en varios niveles, incluida la capa 7 para brindar información estratégica sobre los tiempos de respuesta de la aplicación web y la capa 3 para comprender el comportamiento de la red, incluida la información estratégica continua sobre la ruta, la latencia y la pérdida de paquetes. Este análisis también debe incluir el autodiagnóstico de la nube del proveedor de SSE para identificar si y cuando el salto de SSE está induciendo un retraso anómalo. Finalmente, la solución debe brindar información estratégica sobre el estado del dispositivo del punto final del usuario e identificar los eventos del dispositivo que contribuyen a las caídas de puntuación (**ver la Figura 13**).

Los proveedores de SSE tienen una posición única para medir y diagnosticar la experiencia del usuario final en función de su presencia en los puntos finales del usuario y en la ruta de datos de la aplicación.

Monitoreo y solución de problemas del rendimiento de calidad de Microsoft Teams y Zoom

Al convertirse Teams y Zoom en la principal plataforma de colaboración y comunicación para muchas organizaciones, medir y diagnosticar problemas de calidad de audio/video se vuelve aún más apremiante. Las soluciones DEM proporcionadas por el proveedor de SSE deberían poder interactuar con aplicaciones UCaaS populares como Zoom y Microsoft Teams para ingerir métricas de calidad de audio y video y unirlas con análisis de red profundos, salto por salto y análisis de dispositivos de punto final. Al combinar estos conjuntos de datos, la solución DEM debe identificar a aquellos que tienen problemas de calidad, así como proporcionar una causa raíz para el problema.

Además, el DEM debe aprovechar la escala de la nube del proveedor de SSE, usándola para pruebas de telemetría proxy y caché, de modo que se puedan recopilar datos granulares de cada usuario final, cada pocos minutos, con un impacto mínimo en las aplicaciones.

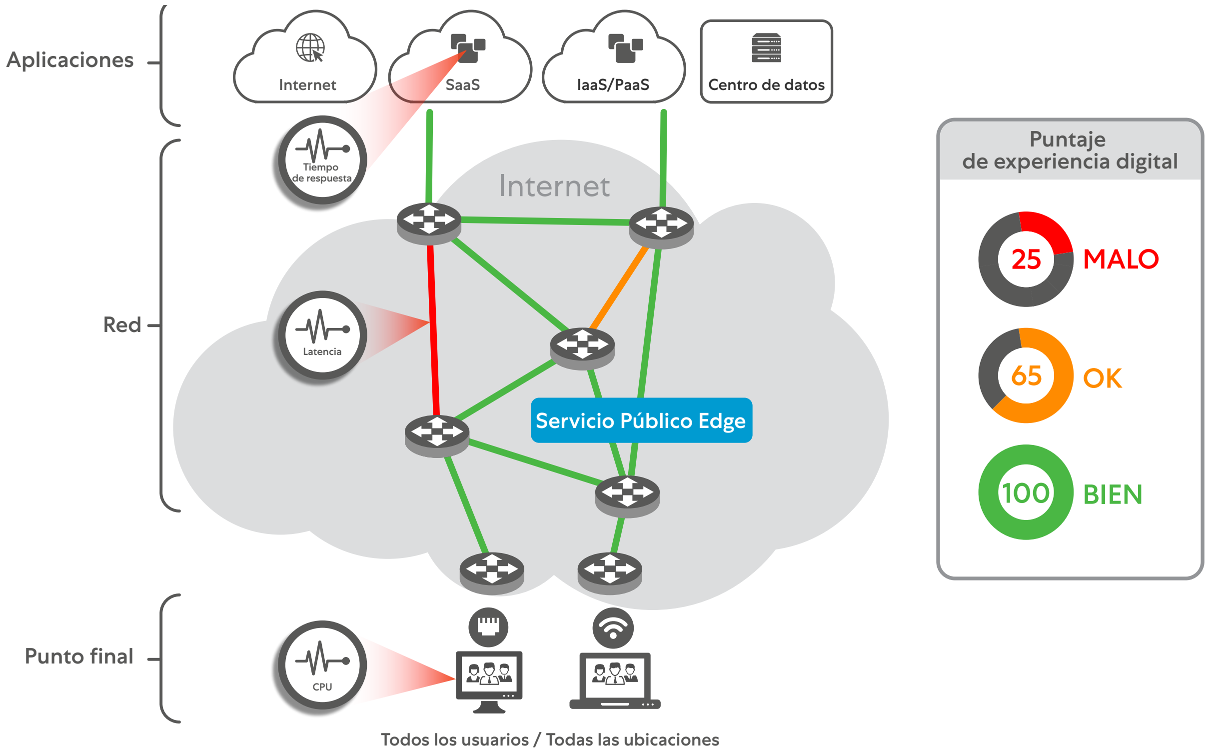

Figura 13: Una solución DEM integrada como parte de la plataforma SSE debe proporcionar una visibilidad única de la calidad de la experiencia del usuario desde la perspectiva del usuario final, prestando atención a los problemas de punto final, red y aplicación.

Tenga cuidado con las herramientas de monitoreo heredadas que adoptan un enfoque en el centro de datos para monitorear y recopilar métricas desde ubicaciones fijas en lugar de directamente desde el dispositivo del usuario. Este enfoque no proporciona una visión unificada del rendimiento basada en el dispositivo del usuario, la ruta de red o la aplicación, y ofrece poca visibilidad cuando los usuarios y las aplicaciones no están en el centro de datos o en la red corporativa. Estas herramientas crean silos de información y no comparten ningún contexto, lo que lleva a una visibilidad fragmentada de la experiencia del usuario y un tiempo de solución de problemas prolongado. Las herramientas de monitoreo de puntos optimizadas para los centros de datos dejan brechas de visibilidad que permiten detectar, solucionar problemas y diagnosticar problemas de rendimiento del usuario final en Internet, mientras que una solución DEM moderna integrada en una plataforma SSE proporciona la gama más amplia de datos para el análisis de causa raíz (ver la Figura 14).

La solución DEM debe identificar a aquellos que tienen problemas de calidad y proporcionar una causa raíz del problema.

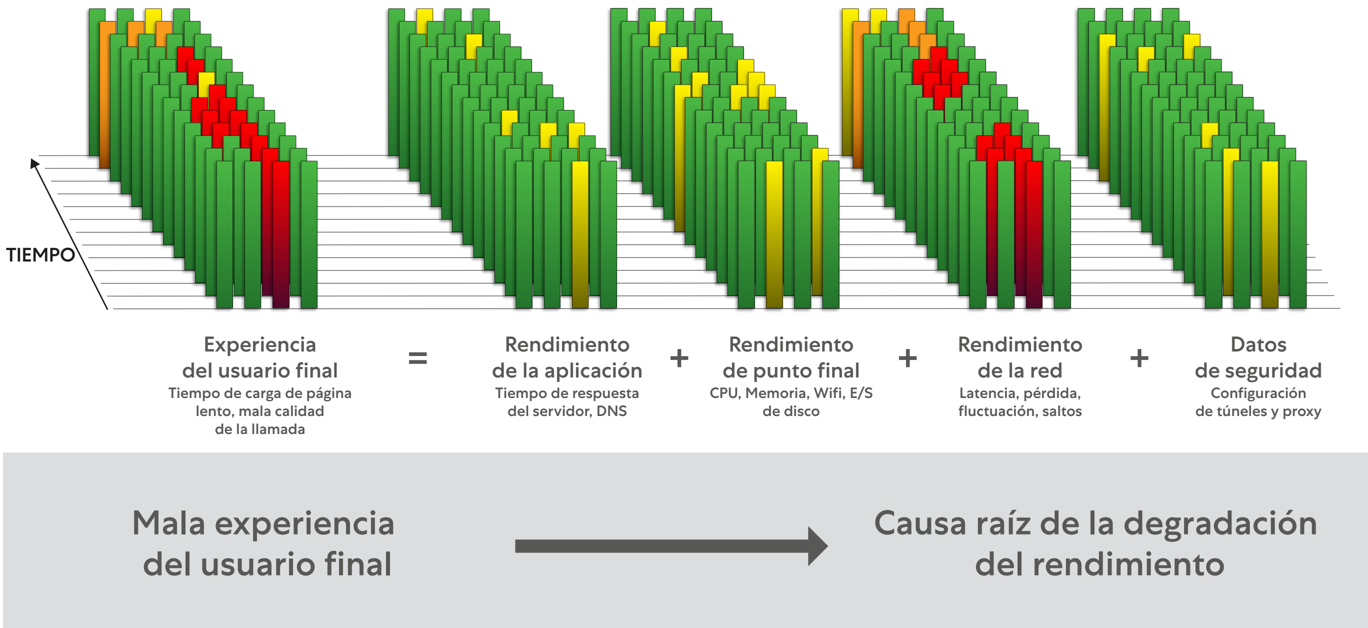

Figura 14: Una solución DEM integrada como parte de la plataforma SSE debe proporcionar una visibilidad única de la calidad de la experiencia del usuario desde la perspectiva del usuario final, arrojando luz sobre los problemas de punto final, red y aplicación.

Optimización de la experiencia del usuario de M365

Un SSE integral puede ir más allá de medir y diagnosticar la experiencia del usuario final para optimizar el rendimiento de aplicaciones SaaS populares como Microsoft 365. El desafío es que muchas empresas enrutan el tráfico de forma centralizada a través de redes radiales y ExpressRoute. Además, el tráfico de usuarios de M365 aumenta la utilización de la red en un 40% y las infraestructuras de salida de Internet de la mayoría de las empresas simplemente no están a la altura de la tarea y la experiencia del usuario. Microsoft recomienda conexiones directas a Internet y arquitectura de proveedores SSE, lo que permite que las salidas directas locales a Internet ofrezcan un rendimiento y un costo óptimos.

Figura 15: Microsoft recomienda una conexión directa a Internet como el método óptimo para el rendimiento y el costo, alineándose con los principios de SSE (fuente: microsoft.com).

Pero la arquitectura importa. Los puntos de presencia del proveedor de SSE en todo el mundo y las relaciones de interconexión con los proveedores y los comerciantes de aplicaciones deben acercar Edge a los usuarios para una conectividad rápida y un acceso de baja latencia. Busque proveedores SSE que se conecten con fibra directa a Microsoft 365 en la mayoría de los intercambios principales para reducir la latencia a aproximadamente 1-2 ms de tiempo de ida y vuelta, escalar para manejar el alto número de conexiones de larga duración, permitir descargas rápidas de archivos y proporcionar una resolución de DNS rápida con menos saltos. (ver la Figura 15).

Es especialmente importante proteger las transacciones de M365 con su solución SSE, ya que la inspección de aplicaciones como OneDrive y SharePoint es ventajosa para la prevención de la pérdida de datos confidenciales. Esto también proporciona una pista de auditoría completa de cada comunicación hacia y desde las aplicaciones M365. Sin embargo, tenga en cuenta que es posible que algunas aplicaciones M365 como Teams no necesiten ser inspeccionadas, dado que gran parte de este tráfico es de voz/video a través de UDP.

¿De qué debo estar al tanto?

Dado nuestro mundo de trabajo desde cualquier lugar (WFA), hay muchos eslabones débiles a lo largo de la cadena de entrega de un buen rendimiento de las aplicaciones en la malla global de redes cableadas e inalámbricas. Optimizar la experiencia del usuario es difícil incluso con una arquitectura superior y conjuntos de herramientas dedicados que miden y diagnostican problemas de UX. Es esencial establecer expectativas razonables con los usuarios finales sobre lo que constituye una experiencia de usuario aceptable de aplicaciones críticas. Entonces es vital usar estas expectativas para construir líneas base para supervisar y administrar.

El diagnóstico de problemas de experiencia del usuario es más un arte que una ciencia. Requiere herramientas y arquitectura excelentes, pero también depende de tener los conjuntos de habilidades adecuados para interpretar y actuar sobre los datos. Si bien las herramientas de DEM ofrecidas por los proveedores de SSE destacarán la mayoría de las causas de problemas (problemas de Wi-Fi, ISP, red troncal, punto final o DNS), un subconjunto requerirá escalamiento y conjuntos de datos adicionales. Por ejemplo, se pueden requerir registros y pistas de paquetes para llegar a la causa raíz. Y también habrá un subconjunto de problemas que no se resuelven en absoluto, lo cual es absolutamente normal.

Tenga cuidado con los proveedores que retornan el tráfico. Todos los centros de datos de un proveedor de SSE deben tener capacidad de computación e inspección, lo que permite una experiencia de usuario más rápida y mejor. La arquitectura con origen en la nube no debe retornar el tráfico a unas pocas ubicaciones centralizadas para la inspección del tráfico. Por ejemplo, si un usuario aparece en Melbourne, su inspección de tráfico debe realizarse localmente con servicios de prevención de amenazas y protección de datos y no debe ser redirigido a otras regiones como Sydney o Singapur. Los proveedores de SSE que ejecutan su nube en hiperescaladores a menudo terminan retornando el tráfico de usuarios. Un hiperescalador puede tener 120 edge points, pero es probable que el 80 % de ellos sean rampas de acceso para llevar el tráfico a una cantidad menor de centros de datos hiperescaladores donde se puede aplicar el control de la política de SSE. Es importante comprender cuántos centros de datos son rampas de acceso y cuántos centros de datos pueden realmente hacer cumplir la política.

Resultados:

El éxito de cualquier transformación, ya sea digital, de red o de seguridad, depende de cómo la experimente el usuario final. El objetivo final de cualquier proyecto de SSE es mejorar la experiencia del usuario final mientras se reduce la exposición a amenazas y se protegen los datos confidenciales. Por lo tanto, el resultado ideal es que la capacidad de un proveedor de SSE para mejorar la experiencia de usuario se puede medir con la capacidad de DEM; esto debería ser una tarea fácil, ya que alejarse del retorno del tráfico a un centro de datos o alejarse de las VPN son formas bien aceptadas de mejorar la experiencia del usuario:

- La solución SSE debe modernizar la experiencia del usuario y actualizar la experiencia de servicio de asistencia. Al aprovechar un enfoque proactivo de la experiencia del usuario, el servicio de asistencia puede reaccionar antes de que los usuarios se quejen.
- La solución SSE debe proporcionar información sobre el rendimiento de audio y video en tiempo real para plataformas de colaboración como Teams y Zoom.
- La solución SSE debe recopilar métricas de las capas de aplicación, puntos finales y red para encontrar anomalías y proporcionar determinación de causa raíz.
- El proveedor de SSE debe proporcionar saltos mínimos entre su nube y destinos populares como Microsoft 365.

N.º 6
Error

Elegir una solución SSE que tenga integración y orquestación limitadas con el ecosistema de proveedores externos

En su lugar, considere a los proveedores de SSE que:

- Integren a través de API sólidas con otros participantes del ecosistema de primera linea (como CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) para garantizar una protección y una experiencia de usuario óptimas.
- Aprovechen estas integraciones para habilitar la automatización, la orquestación y reduzcan la complejidad operativa y los gastos generales.
- No aumenten la deuda técnica improvisando una cartera de soluciones con integración limitada tanto dentro del portafolio como con terceros.

Cómo los proveedores de SSE correctos hacen que esto funcione:

La mayoría de las organizaciones que tienen dificultades con la deuda técnica se dan cuenta de que gran parte de ella se debe a la adquisición de tecnologías de proveedores a lo largo de los años que no logran interoperar.

Peor aún es la llamada "plataforma" ofrecida por un solo proveedor que no está realmente integrada, sino una colección de productos puntuales adquiridos que no tienen una integración real más allá de un tablero. A menudo, estas tecnologías de proveedores requieren habilidades especializadas para operar y mantener una coexistencia frágil con las tecnologías que las acompañan. SSE puede eliminar gran parte de esta deuda técnica con una plataforma de seguridad unificada en la nube proporcionada por un solo proveedor. Dada esta visión, SSE aún vive en un ecosistema de tecnologías complementarias, y los proveedores deben considerar la interoperabilidad con este ecosistema como un objetivo principal **(ver la Figura 16)**. Este ecosistema consta en general de otras soluciones de seguridad, red y nube.

Figura 16: No se quede atrás con un proveedor que no tenga un rico ecosistema de integraciones de terceros, ya que esto genera deuda técnica, interoperabilidad limitada y una pila de seguridad frágil (no ágil).

Para garantizar una implementación e integración rápidas, sencillas y seguras, el proveedor de SSE debe proporcionar integraciones con los líderes en:

- Proveedores de servicios en la nube (CSP), tanto IaaS/PaaS como SaaS
- Detección y respuesta de punto final (EDR)
- SD-WAN
- Gestión de accesos e identidades (IAM)
- Gestión de eventos e información de seguridad (SIEM)/orquestación, automatización y respuesta de seguridad (SOAR)
- Herramientas de orquestación

Estas integraciones deben permitir la orquestación entre el proveedor de SSE y los proveedores adyacentes para reducir la complejidad, el costo total de propiedad (TCO) y mejorar la postura de seguridad (ver la Figura 17).

Proveedores de servicios en la nube (IaaS/PaaS y SaaS)

Para las aplicaciones internas que cambian a la nube o se construyen desde su origen en la nube, el proveedor de SSE debe integrar los principales proveedores de IaaS/PaaS como AWS, GCP y Azure para proporcionar conectividad de acceso remoto seguro Zero Trust a dichas aplicaciones. Hacerlo garantiza que estas aplicaciones nunca se expongan a Internet, lo que las hace completamente invisibles para los usuarios no autorizados, ya que se conectan a través de conectividad de adentro hacia afuera, basada en políticas en oposición a que la red se extienda hacia ellas.

Este enfoque garantiza el acceso directo a la nube sin conectarse a través de una VPN de acceso remoto, con la capacidad de aprovechar las ventajas de escala del proveedor de nube sin agregar ninguna complejidad de segmentación de red. No depende de ningún dispositivo virtual o físico, y aporta las ventajas de Zero Trust para eliminar la superficie de ataque.

Para las aplicaciones SaaS populares, los proveedores de SSE deben proporcionar integraciones con un solo clic. En el caso de Microsoft 365, la integración del proveedor de SSE debe asignar todos los rangos de IP y dominios de Microsoft para las aplicaciones de M365 enumeradas, lo que permite el reenvío transparente del tráfico del usuario final a su nube. Además, la interconexión con Microsoft 365 reduce el tiempo de ida y vuelta, mejora la escala y permite descargas de archivos más rápidas y resolución de DNS.

La integración de SSE con otros proveedores de SaaS como ServiceNow puede mejorar la protección de datos. Al escanear los datos nuevos y existentes de ServiceNow, el proveedor de SSE debe identificar los datos confidenciales en función de las políticas de DLP y bloquear la carga saliente de archivos de datos confidenciales. La integración con ServiceNow Security Incident Response puede organizar acciones de respuesta, incluida la actualización de listas de bloqueo personalizadas. Las IP, dominios y URL de riesgo pueden bloquearse sin intervención manual, mientras que las configuraciones incorrectas en la nube pueden cerrarse para ayudar a reducir el riesgo de una violación.

Detección y respuesta de punto final

El proveedor de SSE debe integrarse con varios socios de seguridad de punto final para compartir telemetría, mejorar la visibilidad mutua y orquestar respuestas. Dicha integración permite que la defensa en profundidad implemente Zero Trust de manera eficaz y eficiente.

Esta integración debe brindar la capacidad de evaluar la identidad, la ubicación y la postura del dispositivo del usuario para implementar automáticamente políticas de acceso condicional apropiadas. Además, la correlación y el flujo de trabajo entre plataformas pueden acelerar la investigación y la respuesta. Esto implica:

- Evaluar el estado del dispositivo e implementar automáticamente las políticas de acceso adecuadas.
- Identificar amenazas de día cero y correlacionarse con la telemetría de puntos finales para identificar los dispositivos afectados a fin de obtener respuestas rápidas con un flujo de trabajo de cuarentena entre plataformas.
- Investigar amenazas con el contexto de punto final y de red para una detección y toma de decisiones efectivas.

SD-WAN

El proveedor de SSE debe integrarse con los proveedores de SD-WAN para simplificar el enrutamiento del tráfico desde la rama y facilitar la establecimiento de salidas directas locales y seguras a Internet.

Una solución conjunta de SSE/SD-WAN puede permitir un acceso a Internet seguro y basado en políticas así como a las aplicaciones críticas de la empresa, y brindar una protección idéntica para todos los usuarios, donde sea y cuando sea que se conecten a las aplicaciones en la nube y a Internet abierto. Las soluciones SD-WAN se pueden integrar con SSE a través de la integración de API. Con esta solución combinada, las sucursales empresariales pueden administrar el aumento del tráfico en la nube y de Internet sin red de retorno a la DMZ centralizada en el centro de datos, utilizando una arquitectura WAN híbrida para la transformación de la red junto con una seguridad sólida.

Cabe señalar que cualquier proveedor de SSE debe ser independiente de la red y no estar vinculado exclusivamente con ninguna solución subyacente de red. De hecho, muchos de los beneficios de SD-WAN provienen de sus capacidades "definidas por software", pero no necesariamente de la WAN, que extiende inherentemente la red corporativa y permite el movimiento lateral de las amenazas. Los responsables de la toma de decisiones de SSE deben evaluar cuidadosamente las razones para continuar extendiendo la red corporativa a la sucursal y considerar enfoques alternativos (como solo Internet) que sean más seguros.

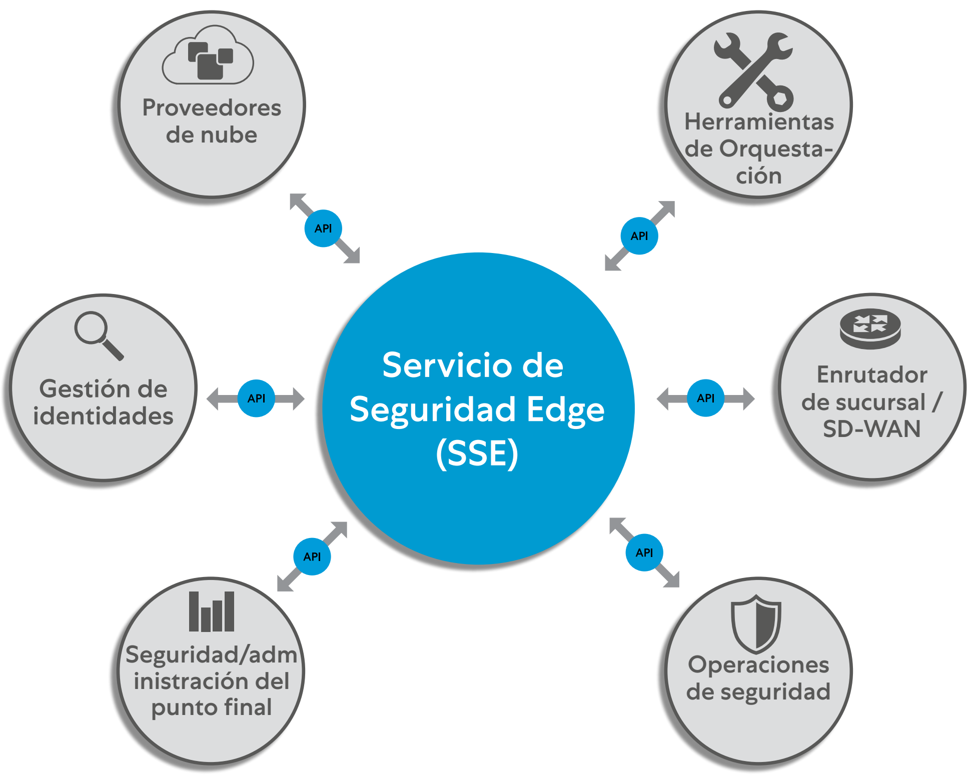

Figura 17: Los proveedores de SSE deben integrarse con los mejores participantes de su clase en varias funciones.

Gestión de accesos e identidades

Los proveedores de SSE deben proporcionar integraciones con IAM para hacer cumplir el acceso Zero Trust basado en la postura del dispositivo y una protección contra amenazas más efectiva en toda la empresa.

Utilizando estándares como Security Assertion Markup Language (SAML), desplegar la integración debería ser fácil. Los usuarios deben poder autenticar y proteger el acceso a Internet y a las aplicaciones internas. La IAM administra el acceso del usuario final a las aplicaciones mediante una combinación de SSO y MFA, mientras que el proveedor de SSE protege la conexión. La compatibilidad con el protocolo System for Cross-domain Identity Management (SCIM) permite que toda la información del usuario se mantenga sincronizada entre los dos sistemas, incluidos los cambios de roles de trabajo o grupos de usuarios y las eliminaciones de cuentas para instancias de usuarios que se mudan de la empresa.

SIEM y SOAR

Los proveedores de SSE deben incluir integraciones con los proveedores de SIEM y SOAR para permitir una gestión eficaz y eficiente del riesgo y el cumplimiento con el enriquecimiento y la automatización de la información.

Los proveedores de SSE deben tener la capacidad de enviar datos de registro casi en tiempo real a soluciones SIEM/SOAR locales y basadas en la nube para facilitar la correlación de registros de múltiples fuentes, lo que permite a las organizaciones analizar los patrones de tráfico en todas sus redes. Además, las organizaciones deben poder aprovechar los datos de registro en SIEM para realizar análisis históricos extendidos (>6 meses). Esto garantiza el cumplimiento de los mandatos normativos a través del archivo de registros locales.

Herramientas de orquestación

Como la infraestructura con código (IaC) y DevSecOps obliga a los equipos de seguridad a "Shift-left", los proveedores de SSE deben proporcionar las API para la orquestación. Aquí, el enfoque está en las aplicaciones internas donde la creación de instancias de acceso Zero Trust es parte del ciclo de vida de entrega de la aplicación, habilitado por secuencias de comandos de orquestación (como Ansible o Terraform), particularmente para configuraciones de segmentación de usuario a aplicación o de carga a carga de trabajo. Dicha orquestación permite alinear las capacidades Zero Trust con los métodos ágiles utilizados por los desarrolladores de software.

Dado que la infraestructura como código (IaC) y DevSecOps obligan a los equipos de seguridad a "Shift-left", los proveedores de SSE deben proporcionar las APIs para la orquestación.

¿De qué debo estar al tanto?

Los responsables de la toma de decisiones de SSE deben evaluar la profundidad de las integraciones de las APIs, la frecuencia de actualización y monitorear los cambios en el mercado que pueden impedir futuras integraciones (es decir, un proveedor adquirido que se convierte en un competidor). Tenga en cuenta la escasez de habilidades en su organización, ya que implementar estas integraciones, especialmente con las herramientas heredadas, requerirá habilidades especializadas

Resultados:

Los proveedores SSE que ofrecen integraciones de terceros ricas y basadas en APIs, proporcionan eficiencias operativas derivadas de la capacidad de orquestar las mejores soluciones de su clase y reducir las posibilidades de bloqueo de proveedores:

- Los proveedores de SSE que se integran con los principales participantes del ecosistema (como CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) preparan su tecnología para el futuro y reducen la deuda técnica.
- Un ecosistema orquestado de proveedores integrados reduce la complejidad operativa, los gastos generales y pueden disminuir los errores de los operadores.
- Los proveedores de SSE que improvisan una cartera de soluciones a través de la adquisición tienden a quedarse atrás en la innovación de productos y, a menudo, carecen de interoperabilidad con terceros.

N.º 7
Error

Elegir una solución SSE que no pueda mostrar valor fácilmente en un ambiente de producción piloto

En su lugar, considere a los proveedores de SSE que:

- Realicen eficientemente una prueba piloto de su solución con un sólo agente unificado, accedan a un conjunto global de servicios Edge (cerca del usuario), con una interfaz centralizada en el usuario y fácil de usar.
- Realicen una prueba piloto de los diferentes aspectos de la plataforma SSE con requisitos de implementaciones mínimos.
- Proporcionen la confianza de que su solución funcionará según lo previsto en la implementación completa con un esfuerzo de mínimo de post-venta.

Figura 18: Asegúrese de que la prueba del proveedor de SSE sea con el producto real y no con una réplica de juguete. Solo una prueba piloto ejecutada en un entorno de producción puede demostrar el valor de la solución del proveedor de SSE.

Cómo los proveedores de SSE correctos hacen que esto funcione:

La adopción de una plataforma SSE requiere repensar su arquitectura de seguridad, por lo que la elección de un proveedor SSE no debe tomarse a la ligera.
La capacidad de comprender la verdadera capacidad del proveedor SSE para trabajar en su entorno de producción es, por lo tanto, crítica. La facilidad con la que se hace esto es representativa de la arquitectura de la plataforma.

Al considerar proveedores de SSE, comprenda los pasos necesarios para ejecutar una prueba piloto. Para los proveedores de SSE correctos, el proceso debería ser encontrar una manera de reenviar el tráfico al servicio Edge. Debe haber pasos mínimos que debe seguir el administrador de SSE, además de establecer un mecanismo de reenvío, configurar políticas básicas, autenticación e informes. Por supuesto, las configuraciones avanzadas de políticas tardarán más tiempo.

La prueba piloto debería abordar un conjunto de resultados comerciales e involucrar a miembros de varios equipos, incluidos la seguridad, la red y el escritorio (por ejemplo, para la instalación de los agentes de punto final). Sin embargo, la participación activa de estos equipos debería ser mínima; después de todo, buscan adquirir una solución SaaS. Los proveedores de SSE que requieran una profunda participación, particularmente de los equipos de redes para manejar escenarios de enrutamiento complejos en una prueba piloto, deben ser un signo de advertencia.

Adopte un enfoque secuencial que refleje sus objetivos comerciales al planificar una prueba piloto de la solución de SSE integral:

1. Revise la postura de seguridad existente, las políticas existentes, la infraestructura de red y los requisitos de las aplicaciones, la tecnología de autenticación, las opciones de reenvío de tráfico y la capacidad.
2. Identifique un conjunto de usuarios/servicios de origen y un conjunto de aplicaciones de destino en las que ejecutar la prueba piloto.
3. Habilite el reenvío de tráfico para esos usuarios, con mayor frecuencia con un solo agente, pero también se pueden crear túneles desde una ubicación de sucursal; implemente máquinas virtuales frente a las aplicaciones privadas elegidas.
4. Configure la autenticación de usuario mediante el aprovisionamiento de la integración del proveedor de identidad.
5. Configure la prevención de amenazas y pérdida de datos utilizando plantillas estándar, que incluyan protección contra amenazas, políticas de sandbox, políticas de control del navegador, política de URL, política de aplicaciones en la nube, control de tipo de archivo e integración de API para SaaS y políticas de firewall.
6. Configure el descubrimiento del servidor para aplicaciones privadas y la política de acceso para esas aplicaciones. Esta puede ser una política *.* para los propósitos de la prueba piloto.
7. Configure la inspección SSL/TLS, políticas avanzadas y capacidades adicionales como CBI, DEM o CSPM.

Todos los pasos anteriores deben ser sencillos y realizables por el proveedor de SSE en un corto plazo (probablemente días) y sin grandes revisiones de configuración o enrutamiento. Si bien la implementación completa real requerirá pasos adicionales, configuraciones de políticas avanzadas, manejo de varios tipos de aplicaciones y puntos finales, e integraciones y coexistencia con otros agentes/tecnologías, el proveedor de SSE debe poder mostrar el valor de la plataforma a través de una prueba piloto sencilla pero bien ejecutada.

Durante la prueba piloto, el proveedor de SSE debe poder demostrar lo siguiente, en consonancia con las seis prácticas anteriores detalladas en este documento:

- **Infraestructura global en la nube con una latencia mínima para el segundo usuario que opere con alta disponibilidad y rendimiento.** El proveedor debe demostrar su capacidad para operar esta nube a escala y demostrar el efecto de la conmutación por error.
- **Zero trust para cada sesión de usuario**, desde la protección de aplicaciones privadas, aplicaciones públicas e incluso comunicaciones de carga de trabajo a carga de trabajo (si la prueba piloto lo requiere).
- **Protección avanzada contra amenazas y DLP avanzada mediante la interconexión del tráfico cifrado**. La gestión de certificados puede requerir algunos pasos adicionales en la prueba piloto, pero demostrar la capacidad del proveedor para realizar una inspección SSL/TLS con una latencia mínima agregada es una excelente manera de diferenciar un proveedor de SSE de otro.
- **Opciones de implementación flexibles**. Aunque esto puede no ser parte de la prueba piloto, el proveedor de SSE debe proporcionar un plan para proteger a todos los usuarios, independientemente de la ubicación o la aplicación. Puede requerir una comprensión de la implementación del servicio privado Edge o CBI para los contratistas. El punto clave para verificar es que el proveedor de SSE puede cumplir con los requisitos de una fuerza laboral distribuida y aplicaciones con sus modelos de implementación.

- **Experiencia de usuario óptima**. Esta métrica abarca desde la facilidad de uso (cómo interactúa el usuario final con su agente, por ejemplo) hasta la experiencia general del usuario al acceder a aplicaciones públicas y privadas a través de su plataforma SSE. El proveedor debe poder medir y diagnosticar un amplio conjunto de problemas de rendimiento del usuario final (Wi-Fi, ISP, CPU, etc.). Esta capacidad de medir/diagnosticar debe integrarse directamente en la plataforma SSE sin necesidad de implementar nuevos agentes.
- **Integración de proveedores externos**. Aunque esto también puede no ser parte de la prueba piloto, el proveedor debe suministrar métodos para integrar los datos de registro en una herramienta externa de SIEM o integración con una herramienta de EDR implementada. El proveedor de SSE debe analizar el ecosistema de herramientas implementado y proporcionar recomendaciones para la integración una vez que comience la implementación real.

Dé preferencia a los proveedores de SSE que requieran la menor cantidad de gastos generales, dadas las habilidades y la escasez de personal que enfrenta la industria.

El beneficio de contratar un proveedor de seguridad de SaaS es confiarle al proveedor de SSE que maneje las tareas que normalmente realiza el personal interno; la prueba piloto debe proporcionar una indicación clara de cuánto esfuerzo requerirá implementar, administrar y actualizar la solución de SSE.

¿De qué debo estar al tanto?

- Las pruebas piloto no pueden probar todas las posibilidades y pueden surgir problemas imprevisibles durante un despliegue real.
- Verifique que el proveedor de SSE esté centrado en el cliente y muestre el deseo de superar cualquier problema de implementación que surja.
- Recuerde que es probable que no vea la escala en una prueba piloto y que no vea cómo se rompen las cosas. Los proveedores de SSE pueden evitar problemas de red molestos o problemas de enrutamiento durante la prueba piloto que solo pueden quedar expuestos durante la implementación. El proveedor de SSE correcto debe ser el que no dependa de ninguna ruta de red para funcionar.
- Calcule la sobrecarga de administración: ¿qué le pertenecerá frente a lo que poseerá el proveedor de SSE? Averigüe el esfuerzo requerido para una implementación de producción, además del mantenimiento continuo de la solución.
- Es posible que algunos proveedores de SSE no sean verdaderos SaaS. Asegúrese de que administrar la solución SSE tenga el costo total de propiedad más bajo, lo que es especialmente importante dada la escasez de habilidades que enfrentan la mayoría de las organizaciones de TI.

Resultados:

Una prueba piloto que valga la pena demostrará que la solución SSE es fácil de implementar, funciona en su entorno de producción y logra sus objetivos.

- Los proveedores de SSE que pueden realizar eficientemente una prueba piloto de su solución son un buen augurio para implementaciones completas. Con el objetivo de un TCO bajo, un único agente unificado, acceso a un conjunto global de servicios Edge y una interfaz de usuario centralizada y fácil de usar, todo esto hace que el mantenimiento continuo de la solución sea sencillo. Cualquier implementación a gran escala requerirá tiempo y esfuerzo, pero el objetivo debe ser trabajar con el proveedor que lo minimice.
- La arquitectura y el diseño de un SSE deben facilitar la adición de características con requisitos de implementación mínimos adicionales (como agentes adicionales o máquinas virtuales). De esta manera, los compradores pueden adoptar un enfoque por fases de SSE, sabiendo que moverse entre fases no requerirá grandes esfuerzos.
- En última instancia, el objetivo es tener la confianza de que el proveedor de SSE realizará una implementación sin problemas en un entorno de producción y estará a su lado cuando ocurran problemas inevitables. Los proveedores centrados en el cliente con arquitectura demostrada son sus mejores pistas para que su inversión en seguridad y transformación de red tenga éxito.

No tome nuestra palabra por hecho

Los momentos "Big Bang" que permiten a las empresas invertir exitosamente en un nuevo camino son muy inusuales. Como tal, las empresas deben considerar un enfoque medido para brindar SSE. El alcance de SSE empresarial (como se comparte públicamente a través de https://trust.zscaler.com), abordar a todos los usuarios, servidores, dispositivos, etc. posibles, se describe en el Error n.° 2. A continuación se muestra cómo sus contemporáneos han abordado la adopción de SSE:

Referencia A:

El cliente implementó la plataforma SSE de Zscaler para el control Zero Trust de:

- Acceso granular del usuario final a los servicios privados
- Seguridad de Internet para usuarios finales, incluida la inspección en línea y la protección de datos
- Transformación de red con usuarios completamente eliminados de la red
- Protección de cargas de trabajo, Internet y acceso privado
- Control de acceso de terceros limitado

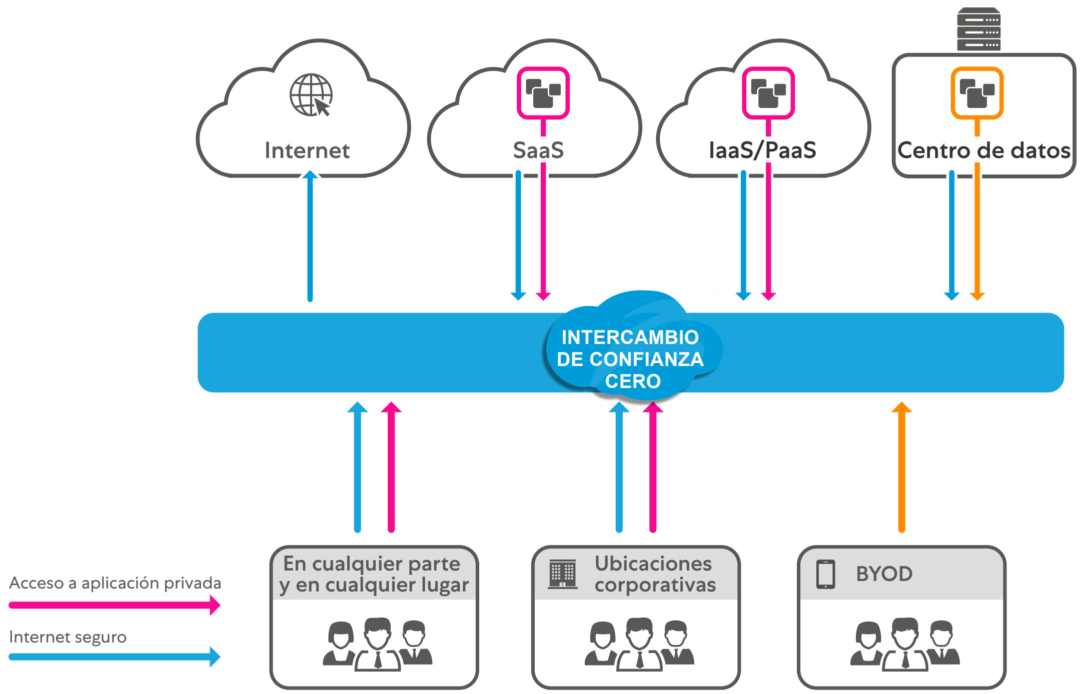

Figura 19: Representación de alto nivel de conectividad implementada por la empresa con Zscaler

"En menos de cinco días, hicimos la transición de 20,000 empleados a WFA de manera fluida, segura y rentable al reemplazar las VPNs con la solución de acceso a la red Zero Trust de Zscaler".

Michael Alvmarken, director de servicios de ciberseguridad y tecnología, Sandvik Group.

"Aprovechar la infraestructura en la nube de Zscaler y las integraciones nativas con ZIA y ZPA nos brindó la mejor información sobre los datos de nuestros usuarios finales".

John Dawes, director de arquitectura empresarial, Reckitt Benckiser.

"Al no tener red de retorno de nuestro tráfico, sino usar directamente Internet, podremos reducir los costos en un 70 %".

Frederik Janssen, vicepresidente de cartera de infraestructura de TI global, Siemens.

Referencia B:

- El cliente implementó la plataforma Zscaler SSE para:
- Visibilidad completa del acceso a todos los servicios de Internet (nube y más allá)
- Control completo en línea para restringir la pérdida de propiedad intelectual corporativa
- Monitoreo de la experiencia digital del acceso de los usuarios durante el trabajo desde casa

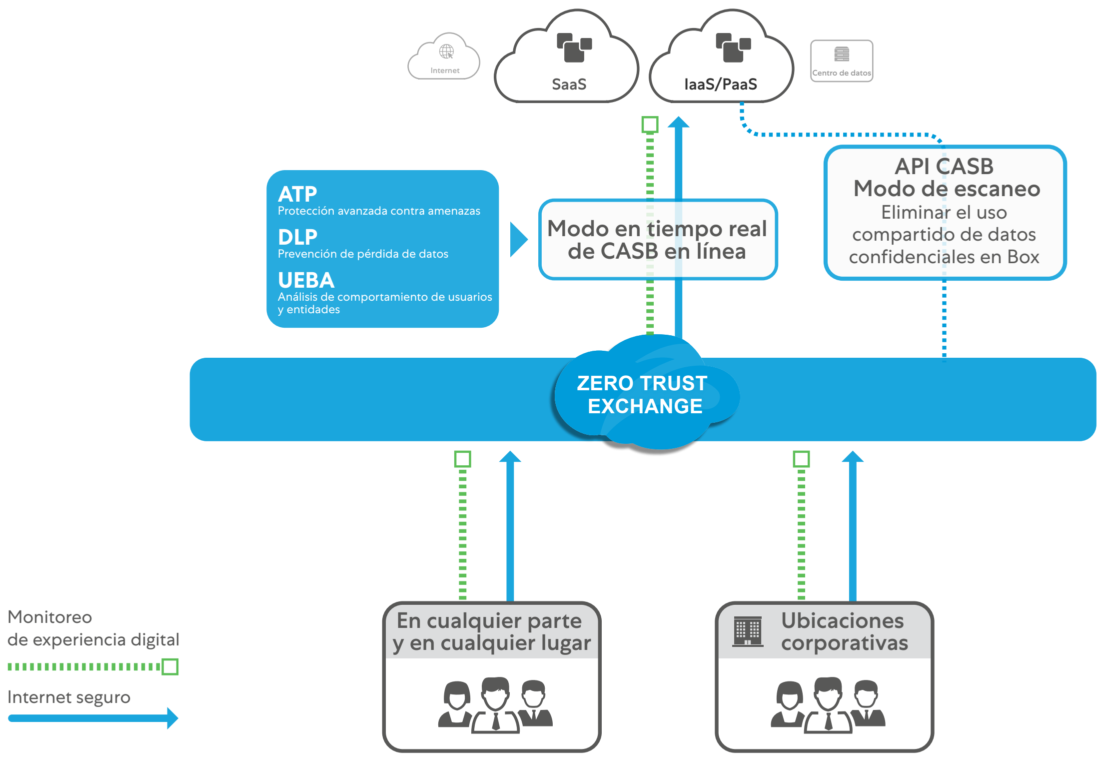

Figura 20: Ejemplo de inspección en línea y supervisión de la experiencia con Zscaler.

"Vemos a Zscaler Digital Experience como un servicio crítico para permitir una experiencia productiva de trabajo desde cualquier lugar. Tuvimos la suerte de resolver el 25 % de los problemas de los usuarios en el pasado. Ahora ZDX es el punto de partida para resolver todos nuestros problemas de experiencia de usuario y podemos identificar la causa principal el 95 % de las veces".

Ed DeGrange, arquitecto principal de seguridad, Ciena.

"Ya sea un comercio o un problema de fraude, algo en el sitio web o fraude interno, todo tiene un impacto financiero y es por eso que la seguridad debe ser parte de él"."

Frederik Janssen, vicepresidente de cartera de infraestructura de TI global, Siemens.

"Con Advanced Cloud Sandbox de Zscaler, no existen grandes esfuerzos para TI, lo cual es fundamental, ya que el mercado actual de talentos es tan limitado que la contratación es extremadamente desafiante."

Mark Ferguson, CISO, Bombardier.

Referencia C:

El cliente entregó protección granular de servicios que no son de TI utilizando la plataforma Zscaler:

- Zero Trust hacia Operation Technology (OT), tanto de empleados como de terceros
- OT hacia cargas de trabajo
- Nube hacia carga de trabajo

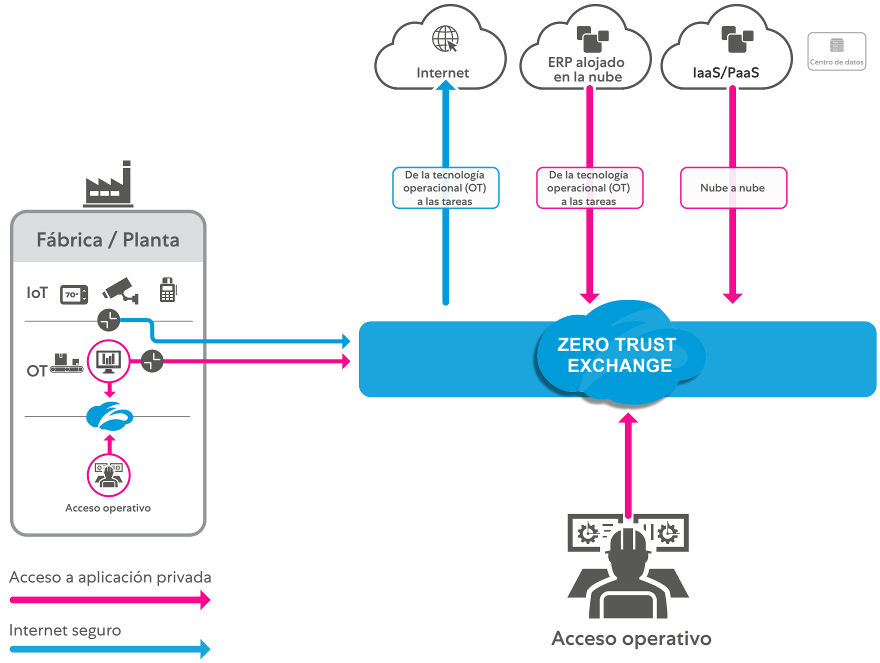

Figura 20: Ejemplo de inspección en línea y monitoreo de la experiencia con Zscaler.

Principales conclusiones

El proveedor de SSE debe ofrecer un SLA documentado basado en la pérdida o degradación del servicio.

La solución SSE debe ofrecer cumplimiento en todos los sitios, en línea, a nivel mundial y dentro de los puntos de interconexión neutrales del operador, lo que garantiza el camino más eficaz hacia los clientes.

El proveedor de SSE debe ofrecer controles Zero Trust para todos los usuarios empresariales, cargas de trabajo y dispositivos autorizados a través de cualquier protocolo.

La solución SSE debe brindar un servicio de manera independiente en cualquier red.

El proveedor de SSE debe proporcionar su inspección en línea a través de una arquitectura de nube proxy que garantice una latencia mínima y permita una visibilidad completa de todo el tráfico web (hasta TLS 1.3 inclusive).

La solución SSE debe proporcionar múltiples controles de seguridad a través de una arquitectura de escaneo simple de memoria para obtener ventajas de escalabilidad únicas para el descifrado a escala.

El proveedor de SSE debe proporcionar su solución administrada de manera centralizada e implementable en múltiples formas para abordar la ubicación del cliente, la región, la localidad y la personalización de funciones.

La solución SSE debe ampliarse para brindar protección para BYOD no administrado, acceso de terceros y socios con el mismo nivel de control granular que los empleados.

El proveedor de SSE debe optimizar la experiencia del usuario al monitorear y diagnosticar problemas de rendimiento para los servicios empresariales (Teams, Zoom, etc.).

La solución SSE debe recopilar métricas de rutas de aplicaciones, puntos finales y capas de red para identificar anomalías y proporcionar información para apoyar a los equipos.

El proveedor de SSE debe integrarse con los participantes del ecosistema mejores de su clase (como CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.), lo que aporta un control y seguridad completos en profundidad a todo el entorno empresarial.

La solución SSE debe integrarse con estos proveedores para proporcionar orquestación a fin de minimizar la sobrecarga operativa.

Los proveedores de SSE deben poder realizar eficientemente una prueba piloto de las funciones y ubicaciones que necesita la empresa en producción.

La solución SSE debe ser simplemente expandible sin necesidad de hardware o agentes adicionales, lo que permita a las empresas hacer crecer su uso de SSE a través de un enfoque por fases.

Para obtener más información sobre SSE, visite Zscaler SSE 2022

Acerca de los autores

Sanjit Ganguli (vicepresidente de estrategia de transformación/CTO de campo) y Nathan Howe (vicepresidente de tecnología emergente y 5G) con carreras en todo el mundo y empresas como Gartner, Nestlé, Riverbed y Verizon, aportan un liderazgo y una visión innovadora sobre la nube y la seguridad, la transformación y las tecnologías emergentes.