LOS SIETE ERRORES QUE HAY QUE EVITAR AL SELECCIONAR UNA SOLUCIÓN SSE

Construyendo el perímetro de servicio de seguridad (SSE) sobre una base de confianza cero

Por:

Sanjit Ganguli
Vicepresidente de Estrategia de Transformación / CTO de campo de Zscaler

Nathan Howe
Vicepresidente de Tecnología Emergente y 5G de Zscaler

Patrocinado por:

zscaler™

Los siete errores que hay que evitar al seleccionar una solución SSE

Índice

SSE. ¿Qué es y por qué debería importarme?

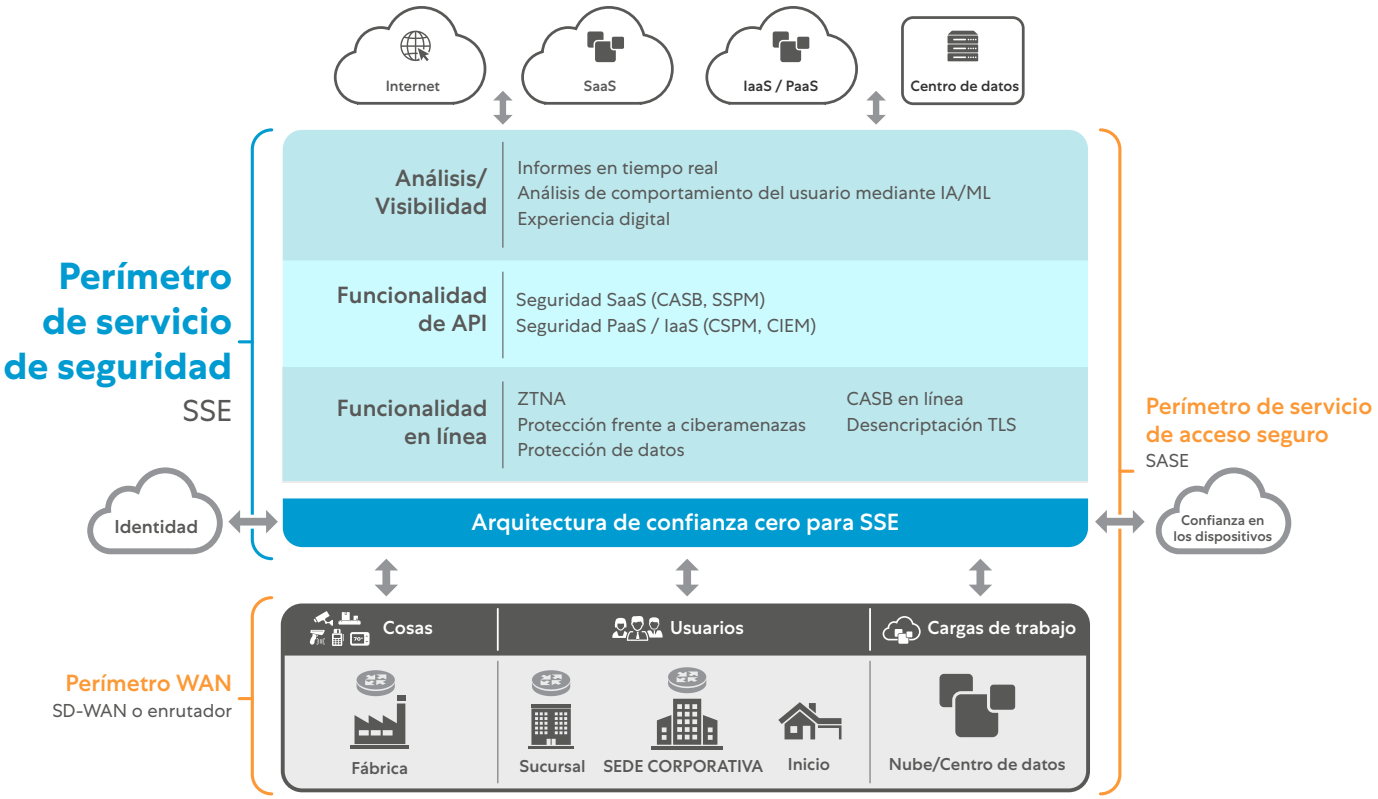

Figura 1: El marco del perímetro de servicio de acceso seguro (Secure Access Service Edge o SASE) incluye SSE para la decisión y aplicación de políticas. SASE requiere el uso de soluciones de conectividad dedicadas desde la entidad solicitante y el perímetro de seguridad donde se aplica la política.

El perímetro de servicio de seguridad (SSE) es la especificación de Gartner de la decisión y aplicación de políticas como componentes del marco del perímetro de servicio de acceso seguro (SASE). SSE promete seguridad y conectividad consolidadas, simplificadas y entregadas en la nube.

La sencillez arquitectónica es siempre una ventaja para una empresa, especialmente cuando esa sencillez 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 obstáculo para el éxito del negocio. SSE contrarresta esos estereotipos. Dentro de un entorno SSE, la seguridad ofrece protección y control entregados como habilitadores del progreso empresarial.

Algunos antecedentes: presentado en 2019, el marco SASE tiene como objetivo guiar a las empresas a través del proceso de digitalización, un proceso impulsado principalmente por la adopción de la nube y la movilidad.
SASE hace converger el acceso a la red y la seguridad, y sirve a ambos desde el perímetro de la nube (altamente distribuido) **(véase la figura 1)**. De este modo, SASE garantiza que la seguridad ya no está centralizada y que se pueden entablar conexiones seguras desde y hacia cualquier lugar.

©2022 Zscaler, Inc. Todos los derechos reservados.

Piense en cómo se conecta un teléfono móvil a varias redes móviles e inalámbricas. No existe una solución de enrutamiento de red específica, pero el usuario exige controles de seguridad para el tráfico entre el origen y el destino. Del mismo modo, el perímetro, la red o la ubicación a la que se conecta el usuario no deben importar a la hora de proteger el tráfico empresarial. Esto es lo que ofrece SSE.

Las empresas de ciberseguridad rápidamente aprovecharon la oportunidad SASE. Algunos vendedores se apropiaron del término de una forma un tanto cínica en beneficio de la marca, pretendiendo que el "acceso" en SASE los convertía en cumplidores de SASE (o que la competencia no lo era): "Tengo una función de red, por tanto soy SASE; tú no estás construyendo rutas de red, por tanto, no eres SASE".

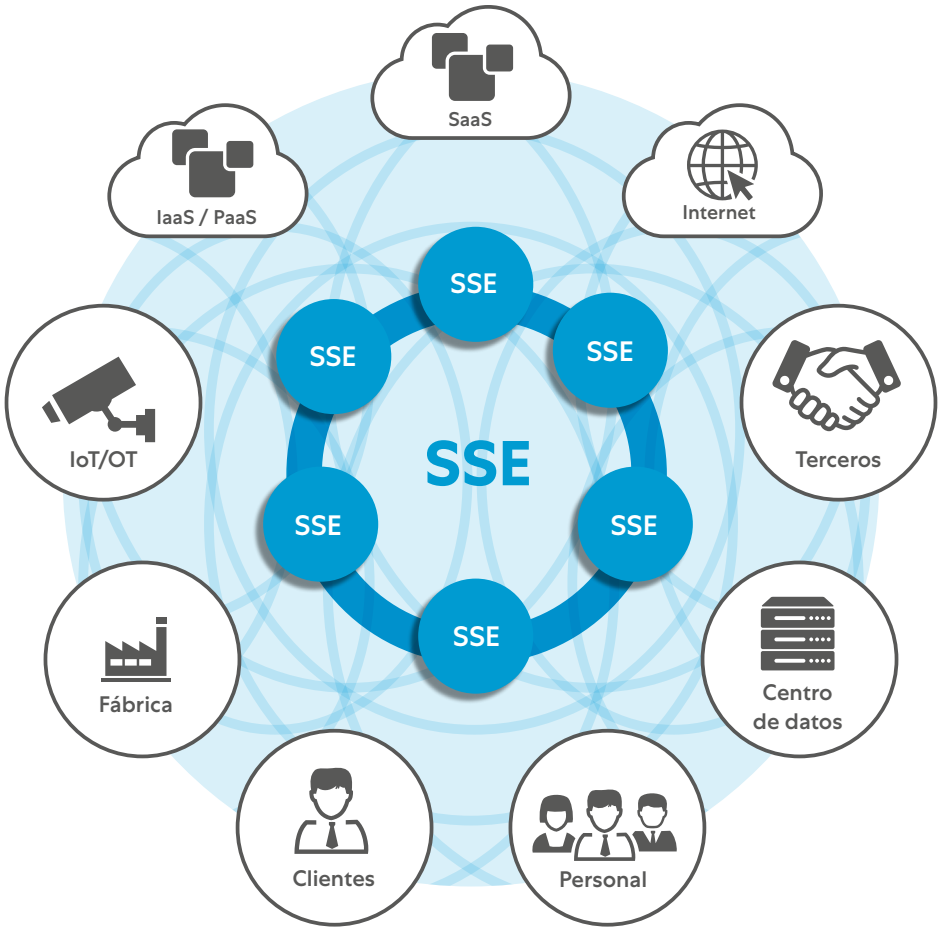

Figura 2: Ofrezca un acceso basado en políticas y validado de entidad a entidad en el perímetro para un mundo móvil y en la nube. SSE le permite llevar la seguridad al usuario en el perímetro, sin comprometer el rendimiento, mientras anula todos sus cortafuegos y VPN

SSE se refiere al conjunto de servicios de SASE utilizados para proteger el tráfico empresarial. SSE garantiza que el usuario (o la carga de trabajo) correcto tenga acceso, de forma segura y bajo el control de TI empresarial, a las aplicaciones y servicios correctos. Esos servicios pueden ser cargas de trabajo en un IaaS o PaaS, aplicaciones SaaS o servicios de Internet como LinkedIn o YouTube. El acceso al servicio debe otorgarse siguiendo los controles de acceso de confianza cero (ZTA), descritos con mucha mayor profundidad en el **segundo error que evitar**.

©2022 Zscaler, Inc. Todos los derechos reservados.

Para cumplir estos altos objetivos, un proveedor de soluciones SSE debe proporcionar una solución global, de alta disponibilidad, escalable e independiente de la red que ofrezca una política coherente, un acceso de confianza cero y una experiencia digital rápida.

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

El SASE ideal es fusionar conectividad y protección, pero en un entorno empresarial, esa fusión solo funcionará si es transparente para los empleados del usuario final. La conectividad es directa, ya sea de usuario a aplicación, de aplicación a aplicación, de carga de trabajo a carga de trabajo, lo que sea. Los usuarios nunca deben pensar: "Vaya, tengo que conectarme a la red antes de poder trabajar". Lo que deben pensar es: "Voy a hacer mi trabajo ahora".

Este ideal integrado sencillamente no se puede lograr en los entornos empresariales que dependen de la infraestructura de red y seguridad heredada. En ese antiguo modelo arquitectónico, la seguridad estaba centralizada, y el tráfico de datos, independientemente de su ubicación (por ejemplo, remota o sucursal), independientemente de su origen (por ejemplo, usuario, aplicación o carga de trabajo) e independientemente de su destino (por ejemplo, Internet, nube, centro de datos), tenía que conectarse y enrutarse primero a través de la red corporativa hasta (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 importante transformación digital de la empresa. Pero adoptar ese cambio puede generar un impacto tangible:

Control:

SSE empieza desde cero. SSE valida cada persona, máquina, carga de trabajo, red y perímetro. Sin una identificación correcta, combinada además con el contexto proporcionado por el análisis del comportamiento, no hay acceso, lo que permite a una empresa controlar completamente qué o quién accede a cualquier servicio dentro de la empresa.

Conectividad directa:

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

Seguridad orientada al negocio:

Las políticas sobre qué entidades pueden conectarse a qué servicios se definen utilizando el privilegio mínimo. Los usuarios, las máquinas, las cargas de trabajo, etc., solo pueden conectarse a lo que se les permite y nada más. No hay ninguna otra conectividad disponible y todos los demás accesos están bloqueados.

Ejecución global:

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

Integral:

SSE proporciona una evaluación completa en línea para inspeccionar el tráfico a escala y en profundidad. SSE brinda protección frente a amenazas avanzadas, defiende los activos corporativos (en la nube y fuera de ella), evita la pérdida de datos y garantiza el control en línea. Cuando sea necesario, la solución debe proporcionar control de los contenidos almacenados en los servicios en la nube.

Oculto:

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

Desde cualquier lugar:

SSE ofrece esta conectividad para todas las partes de la empresa desde cualquier lugar. SSE protege y conecta una base de usuarios flexible al tiempo que garantiza que las cargas de trabajo, los objetos y las máquinas puedan moverse, reubicarse y transformarse sin perder el control.

©2022 Zscaler, Inc. Todos los derechos reservados.

SSE puede ser un catalizador del cambio en una organización sencillamente asegurando el negocio de una manera notablemente 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 a su organización simplificar la seguridad.

Hay siete errores que debe evitar en el recorrido de transformación digital empresarial hacia 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 SSE. Este recorrido debe ser una alternativa a las "viejas formas de trabajar", como aferrarse a las redes o permitir el acceso general a los servicios, lo que limita la capacidad de transformar y satisfacer las necesidades del negocio.

Error n.º1:
Elegir una solución SSE que carezca de un historial probado de funcionamiento en una plataforma de nube global que se adapte al rendimiento y la disponibilidad

Error n.º 2:
Elegir una solución SSE que no esté basada en una arquitectura de confianza cero

Error n.º 3:
Elegir una solución SSE que prometa protección contra amenazas avanzadas y DLP avanzada, pero que no pueda inspeccionar el tráfico cifrado a escala

Error n.º 4:
Elegir una solución SSE que sea "única para todo" y no admita opciones de despliegue y gestión flexibles, escalables y diversas

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

Error n.º 6:
Elegir una solución SSE limitada en cuanto a la integración y orquestación con un ecosistema de proveedores ajenos

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

¿Quién debería leer esto?

El paso a SSE no se limita a la transformación de la seguridad e implica a más personas que a los **arquitectos de seguridad**. Las mejores prácticas descritas en este libro electrónico están destinadas a **los arquitectos de seguridad**, **los arquitectos de redes**, **los arquitectos empresariales**, **los arquitectos de la nube** y **los arquitectos de aplicaciones**.

N.º 1
Error

Elegir una solución SSE que carezca de un historial probado de funcionamiento en una plataforma de nube global que se adapte al rendimiento y la disponibilidad

En su lugar, considere soluciones SSE que:

- Ofrezcan un conjunto diverso y global de perímetros de aplicación de políticas de servicio público con rendimiento, disponibilidad, rendimiento y función respaldados por SLA. La solución ejecuta la aplicación de políticas de forma local en las ubicaciones de los clientes.
- Hayan nacido en la nube con la mejor capacidad de recuperación, infraestructura, diversidad geográfica, capacidades funcionales y una experiencia de usuario óptima. Ofrezcan servicios SSE en línea en centros de datos sin importar el operador y no como un servicio ejecutado sobre una nube administrada de destino o un proveedor de centros de datos.
- Tengan un historial probado y transparente de adaptabilidad, 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 adecuados hacen que esto funcione:

Crear y ejecutar una plataforma SSE multiusuario para miles de millones de transacciones implica mucho más que el nivel de cómputo y no es algo sencillo. **Se confiará a la solución SSE 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 prestará servicios a su empresa a través de un servicio distribuido globalmente. Arquitectónicamente, la forma de entrega más eficaz es a través de un servicio basado en proxy. Al no estar sujeto al estado de la red, un servicio proxy se centra en entregar SSE al acceso a la aplicación, lo que permite una mayor comprensión sin descargar plataformas adicionales para obtener información estratégica, como la inspección a escala **(consulte el error n.º 3)**.

Tenga en cuenta que una verdadera arquitectura proxy requiere un esfuerzo significativo de I+D y muchos años de refinamiento para lograr los requisitos de escala de la empresa moderna. La solución SSE adecuada tendrá decenas de ejemplos de grandes despliegues en los que se ha demostrado que la arquitectura proxy es escalable.

Este servicio debe prestarse a través de un conjunto uniforme de perímetros de política en el que se protejan todas y cada una de las funciones de transmisión de datos de su empresa y no debe ser solamente el número de nodos, sino más bien el número de sitios con garantía de SLA que ofrecen los servicios que necesita 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 otras razones.

Adoptar SSE significa que consolidará, vigorizará y compartirá la responsabilidad de su seguridad, conectividad y control empresarial con un proveedor de seguridad de confianza. Este modelo compartido simplificará los medios por los que ofrece protección y conectividad a sus usuarios, cargas de trabajo, servicios y sucursales, entre otros. El proveedor de SSE debe cumplir con un conjunto de SLA definidos y comprobados para garantizar la actividad de su empresa y, al mismo tiempo, ofrecer protección.

©2022 Zscaler, Inc. Todos los derechos reservados.

Cuando su servicio empresarial se conecta, necesita una ruta eficaz para consumir la función de destino. Esto solo se puede lograr a través de una solución SSE con interconexión altamente eficaz en los centros de datos neutrales para el operador. Por lo tanto, los controles se deben aplicar en línea, entre el origen y el destino, independientemente de la ubicación de un origen y/o destino.

Las soluciones que alojan el servicio de seguridad dentro de nubes de computación centrales, a menudo dentro de hiperescaladores y tienen puertas de entrada, como se muestra en Figura 3 (suelen ser denominados servicios de rampa de entrada) se basan en perímetros de entrada distribuidos, pero procesan el control de las políticas y la aplicación de forma centralizada, introduciendo así una latencia no deseada y dando lugar a malas experiencias de usuario.

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

Aplicación de la política de perímetro uniforme

El conjunto de perímetros de servicio de un proveedor de SSE debe cumplir con las políticas. No pueden ser perímetros de conectividad a una red más grande y basada en la nube, cuyo único fin sea el de enrutar o encauzar su tráfico a la infraestructura de cumplimiento central. Dichos esquemas anulan el objetivo de proporcionar servicios de alta eficacia y baja latencia

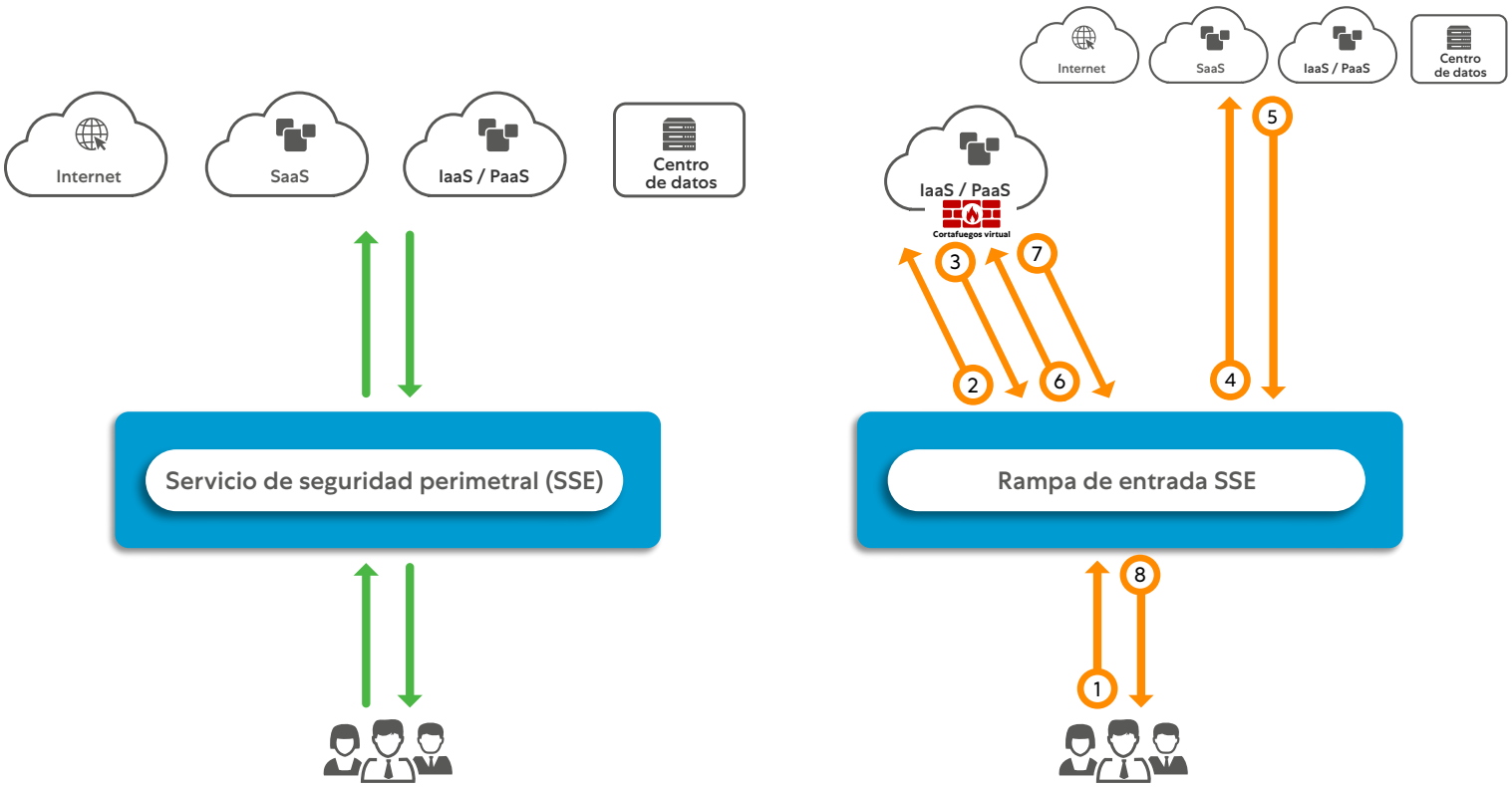

Figura 3: Los servicios de SSE en línea (izquierda) aplican controles de seguridad al tráfico en línea. Los controles de seguridad de rampa (derecha) proporcionan puertas de enlace de entrada en el perímetro, con el único fin de reenviar a un control central alojado en el cómputo en la nube, lo que produce latencia, ineficiencia y una mala experiencia de usuario.

©2022 Zscaler, Inc. Todos los derechos reservados.

El proveedor debe tener en cuenta las siguientes consideraciones de diseño y asegurarse de que los perímetros:

- Estén alojados en ubicaciones de interconexión vitales dentro de centros de datos neutrales para el operador, lo que garantiza una latencia mínima entre la fuente y el destino. Al evaluar a un proveedor de SSE, revise las estadísticas de referencias públicas como PeeringDB y las implementaciones de socios **(consulte el error n.º 6 para obtener detalles sobre la integración de socios)**.
- Estén respaldados por un SLA válido. Esto garantizará la estabilidad de las funciones comerciales e indicará que el proveedor de SSE está trabajando en las regiones para garantizar los SLA.
- Se implementen de forma privada por cliente en ubicaciones donde las condiciones locales requieran implementaciones más matizadas, como en las instalaciones del cliente o dentro de un nodo de cómputo perimetral **(el error n.º 4 contiene más detalles)**.
- Demuestren un recorrido histórico de crecimiento del rendimiento.
- Ofrezcan tolerancia a errores implementada en modo activo-activo para garantizar la disponibilidad y redundancia (el proveedor supervisa y mantiene sus perímetros de servicio público para garantizar una disponibilidad continua).
- Promuevan la privacidad de los datos para garantizar que el tráfico del cliente no pase a ningún otro componente dentro de la infraestructura y que ningún dato se almacene en el disco.
- Proporcionen controles uniformes para los recursos de la empresa en todos los perímetros y no encaminen o encaucen el tráfico desde los perímetros remotos a las ubicaciones centrales.
- Apliquen una protección a escala global para proteger todos los servicios de la empresa una vez que se detecta una amenaza.

⚠ ¿Qué debo tener en cuenta?

- Perímetros públicos que no proporcionan ejecución. En su lugar, encauzan el tráfico a grandes centros de datos de cumplimiento donde hay recursos informáticos disponibles.
- Aseguran tener cientos de perímetros públicos sin compartir la función y la capacidad de cada perímetro
- Perímetros sin SLA sobre disponibilidad, rendimiento y resiliencia.
- Derivan al perímetro los servicios sin multitenencia y fuerzan el tráfico a través de un cauce / ruta a otros lugares.
- Servicios SSE que no tienen evidencia comprobada de implementación con grandes clientes.
- Servicios sin información pública sobre la estabilidad y disponibilidad del servicio

Resultados:

Seleccionar una solución SSE que se adapte a su empresa en la actualidad y, lo que es más importante, a sus objetivos futuros, es una inversión fundamental. La escalabilidad no es simplemente el mecanismo para ampliar, sino lo que es más importante, para abordar las necesidades de su empresa sin sacrificar la función, la estabilidad y la protección de su negocio. Seleccione una solución que:

- Proporcione evidencia y transparencia de su implementación global y diversa.
- Haya documentado y validado los SLA para la pérdida o degradación de los servicios SSE.
- Haya implementado en un gran número de clientes de tamaño y complejidad similares a los de su empresa.
- Tenga información pública y revisable para cada PoP utilizando herramientas públicas (por ejemplo, PeeringDB).
- Ofrezca todas las funciones críticas en todos los sitios sin tráfico de bucles invertidos.
- Proporcione protección en línea entre el origen y el destino.
- Esté diseñada para la infraestructura y la resiliencia operativa y funcional.
- Sea consumible en múltiples formas en múltiples sitios.

N.º 2
Error

Elegir una solución SSE que no esté basada en una arquitectura de confianza cero

En su lugar, considere soluciones SSE que:

- Permitan exclusivamente el acceso a identidades validadas contextualmente, independientemente de la ubicación/red. Esta ruta con menos privilegios es para todos los servicios, no solo para los usuarios. Al conectar fuentes autorizadas a través de los controles correctos de SSE a destinos válidos exclusivamente, las empresas eliminan el movimiento lateral, del que a menudo se aprovechan los actores de amenazas.
- Se centren únicamente en la conexión del acceso dinámico y por sesión. La confianza cero no se entrega con cortafuegos, SD-WAN y otros servicios de red. Debe ser una superposición independiente de la red.
- Nunca expongan los activos empresariales a una fuente no autorizada, reduciendo con ello la superficie de ataque y garantizando que se apliquen los controles correctos a todos los servicios.

Cómo los proveedores de SSE adecuados hacen que esto funcione:

La confianza cero para todas las comunicaciones de la empresa significa que no se concede acceso desde ninguna fuente (incluidos los usuarios, terceros, redes, etc.) a ningún destino sin el permiso y la aprobación explícitos para hacerlo.

Ofrecer confianza cero dentro de una empresa ha sido tradicionalmente un reto debido al contexto de red compartida de conectar el origen con el destino, confiando en una ruta de red física o lógica para interconectar las dos entidades. La figura 4 detalla estas preocupaciones físicas compartidas. No se puede construir o añadir confianza cero con las SD-WAN o los cortafuegos.

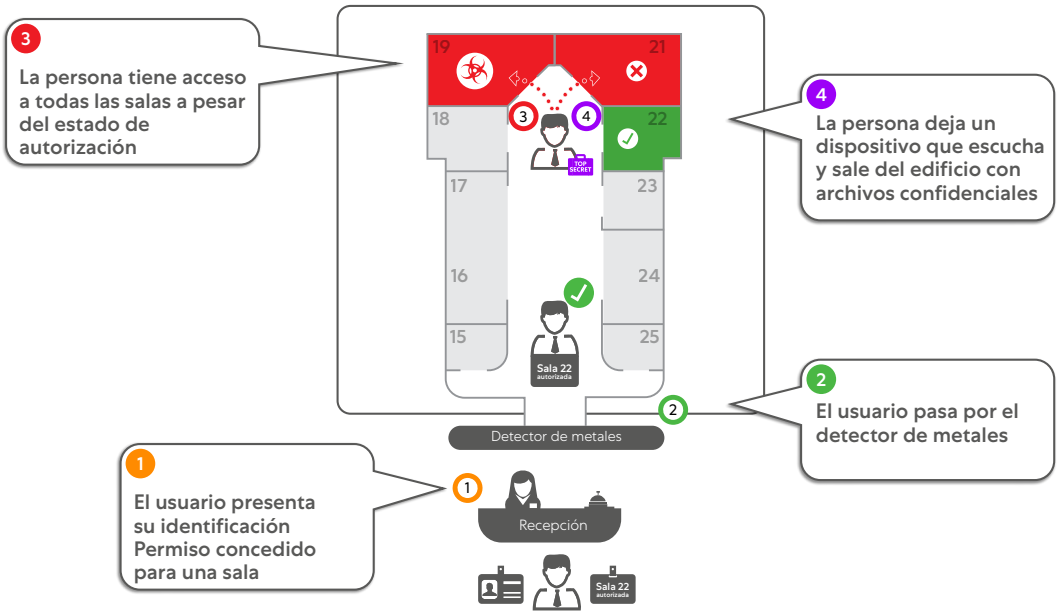

Figura 4: Cómo no habilitar el acceso: el antiguo mundo de la analogía de la seguridad de la red. Conectar a los usuarios a su red corporativa es como permitir que visitantes no escoltados paseen dentro de sus instalaciones y potencialmente roben datos confidenciales.

©2022 Zscaler, Inc. Todos los derechos reservados.

SSE puede ayudarle a reforzar el acceso de los usuarios en toda la empresa y las restricciones para sus cargas de trabajo. Al ampliar 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 otras muchas cosas, la arquitectura de confianza cero impone controles granulares, garantizando que cada solicitante se comunique con el destino correcto en cada sesión, como ilustra la Figura 5. Estas reglas requieren el conocimiento de las entidades de origen y de destino, y son la razón por la que la mayoría de las empresas comienzan su viaje de confianza cero (y SSE) con su base de usuarios. A los usuarios se les suele asignar una identidad, lo que les permite diferenciarlos de los distintos servicios. Sin embargo, dado que las redes son planas y están expuestas y abiertas, el riesgo de que un usuario tenga acceso a más información solo por haber compartido una red es una preocupación importante para la estabilidad de las empresas.

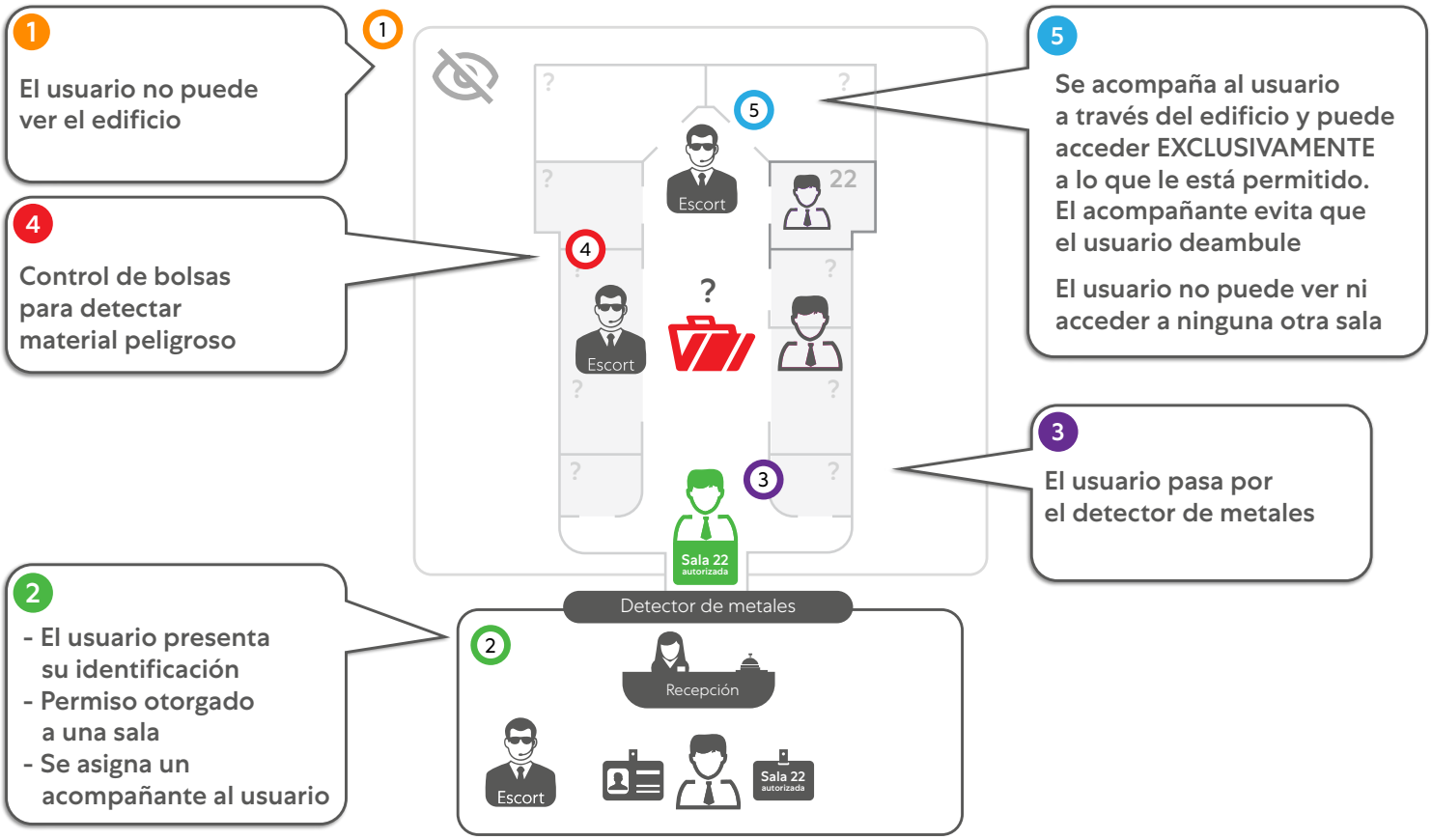

Figura 5: La forma correcta de proporcionar acceso es mediante el control de extremo a extremo. El acceso de confianza cero es como acompañar a un visitante con los ojos vendados a una reunión en sus instalaciones y luego acompañarlo a la salida. El visitante no puede deambular ni husmear.

Considere todos los casos de uso empresarial, como la protección de los usuarios y los activos empresariales clave, y aplique los controles de SSE a todo el tráfico. Establezca conexiones después de revisar dinámica y contextualmente el riesgo de los siguientes cuatro valores de conexión (véase 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 en qué condiciones?

Ejemplo: Sarah, de Recursos Humanos, necesita acceder al sistema de recursos humanos alojado en la nube, así como al sistema interno de gastos. El acceso se concede a través de la plataforma SSE siempre que su identidad y la confianza del dispositivo tengan los derechos definidos para obtener dicho acceso.

Control de política

¿Dónde, cómo y qué controles se aplicarán? 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, pero su empresa solo quiere que vea, no que descargue o manipule datos. Por tanto, la solución SSE únicamente permite a Pierre acceder 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 hay que aplicar? El acceso puede cambiar en función del contexto de la política de identidad y control.

Ejemplo: un iniciador válido puede tener aprobación para acceder a un servicio PaaS en la nube específico y, si se trata de un servicio en la nube, SSE inspeccionará la carga de trabajo para asegurarse de que no está filtrando secretos corporativos. Ese mismo iniciador puede entonces hablar con un servicio interno con una confianza similar, estableciendo así simplemente una conexión iniciador-servicio, sin controles adicionales.

Establecimiento de la conexión

Por último, tomando las entradas anteriores, las perspectivas condicionales sobre cargas de trabajo, capacidades de red o perímetro, políticas definidas por la empresa, etc., se establece el acceso. La solución SSE debe identificar variaciones, por ejemplo, una ubicación cambiada, y encauzar el acceso a través de la mejor ruta aplicable.

Ejemplo: una vez validados el origen, el control y los destinos, se construirá la conexión para esa sesión y nada más. El flujo de extremo a extremo de la aplicación de políticas por sesión se describe en la Figura 6.

©2022 Zscaler, Inc. Todos los derechos reservados.

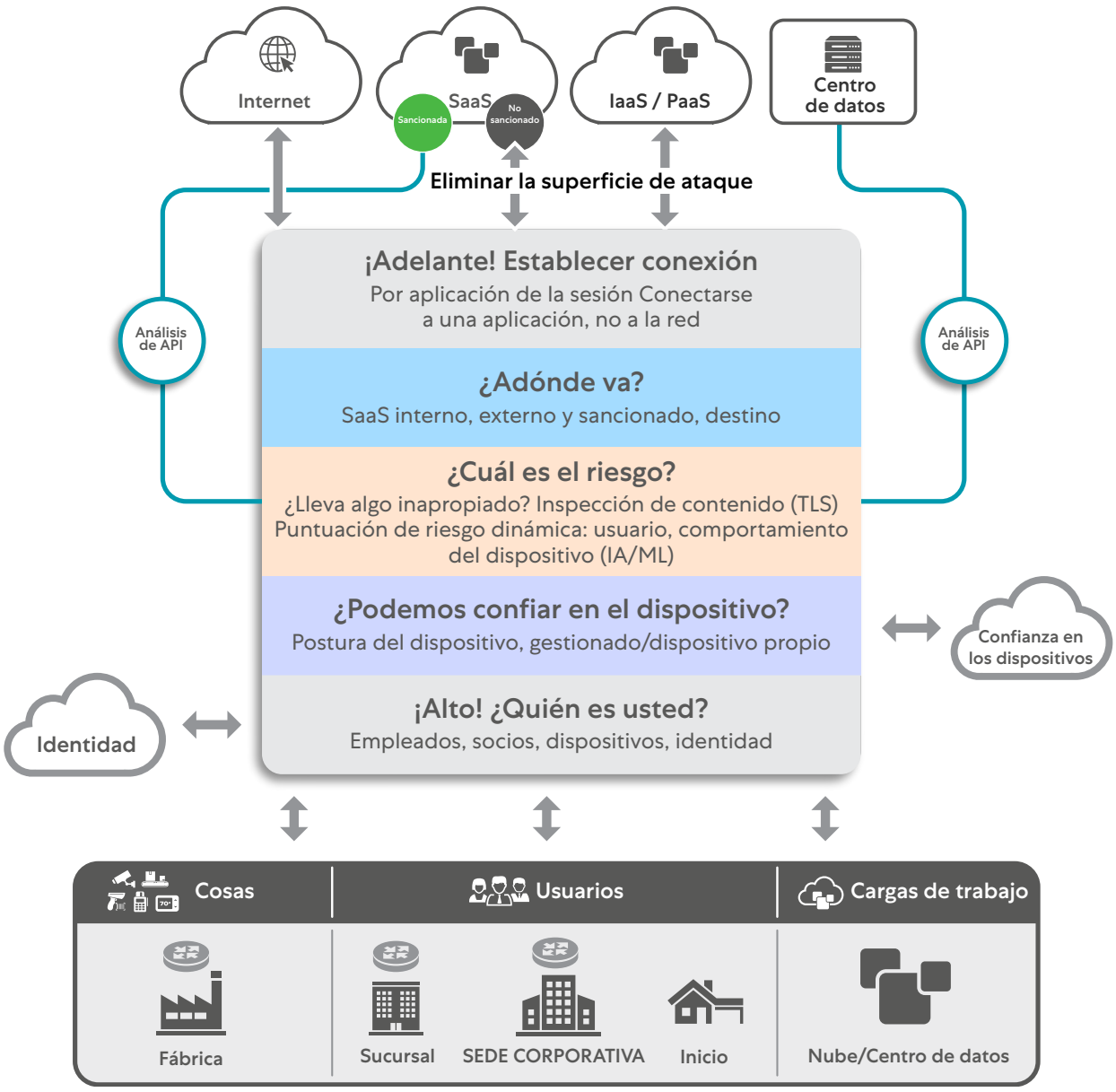

Figura 6: Pasos que se dan en una arquitectura de confianza cero, que muestran el control y la aplicación de políticas en cada paso

La definición de los controles de conexión dentro de una solución SSE **garantiza que solo el origen correcto puede acceder al destino adecuado**, a través de la solución SSE correcta. Este uso de SSE con menos privilegios ofrece múltiples beneficios a una empresa, entre los que se incluyen:

- Aplicación de 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, por ejemplo, no permitir que un servidor Linux se conecte a un sistema de parches de Windows.
- Visibilidad granular y aprendizaje de los flujos, por solicitud de acceso, no IP de red a IP
- Consolidación del acceso basado en la identidad y no en la red, lo que permite racionalizar la función de las redes (y la infraestructura)

©2022 Zscaler, Inc. Todos los derechos reservados.

Viaje escalonado hacia el SSE con confianza cero:

Al seleccionar una solución SSE que ofrece el control en todos los siguientes casos de uso (y el control basado exclusivamente en el usuario), puede ampliar la protección en todas las funciones empresariales (véase la Figura 7):

Usuario a cargas de trabajo

Habilitar el acceso de los usuarios a las cargas de trabajo significa que puede eliminar el contexto de la red del acceso de los usuarios, al tiempo que obtiene visibilidad de las cargas de trabajo a las que acceden los usuarios. Esta combinación suele ser la más rentable.

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

Permita un mayor desarrollo de la totalidad de los servicios empresariales, así como reglas más granulares, como el acceso a plataformas aisladas de OT e I+D, sin exponer nunca la totalidad del ecosistema a la base de usuarios.

Acceso de terceros

Implementar el acceso de confianza cero para socios externos elimina el riesgo de conectividad de red y la superficie de ataque expuesta que acompaña al acceso de socios heredado. El control de privilegios mínimos de confianza cero le permite controlar el acceso de los socios desde dispositivos personales o no confiables hasta aplicaciones específicamente designadas, a la vez que brinda mayor visibilidad de aquello a lo que se accede.

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

Cargas de trabajo a cargas de trabajo

Los controles de carga de trabajo a carga de trabajo son solicitudes de acceso a aplicaciones y servicios. Por lo general, una máquina Windows solicitará revisiones de Windows, no de Linux. Por consiguiente, es fundamental que una empresa determine qué sistemas deben tener acceso a qué.

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

Por el contrario, si la carga de trabajo accede a un servicio local y privado, esto únicamente puede hacerse a través de controles SSE en línea, tras la aprobación de la identidad, mediante una validación de confianza cero.

Ubicación a ubicación

A medida que el acceso y el control evolucionan en su empresa, considere el uso de la confianza cero para la conectividad entre sitios. Debería aislar un conjunto de servicios a una red, sitio, VPC, etc. La conexión entre la ubicación y el sitio conocido no debe realizarse a través de una red compartida. La confianza cero permite que una ubicación válida se conecte a un conjunto válido de cargas de trabajo dentro de otra ubicación. La confianza cero no utiliza el acceso a la capa de enlace de la red; exige una conectividad de aplicación a aplicación de manera uniforme en cualquier sitio, VPC, VLAN, etc.

©2022 Zscaler, Inc. Todos los derechos reservados.

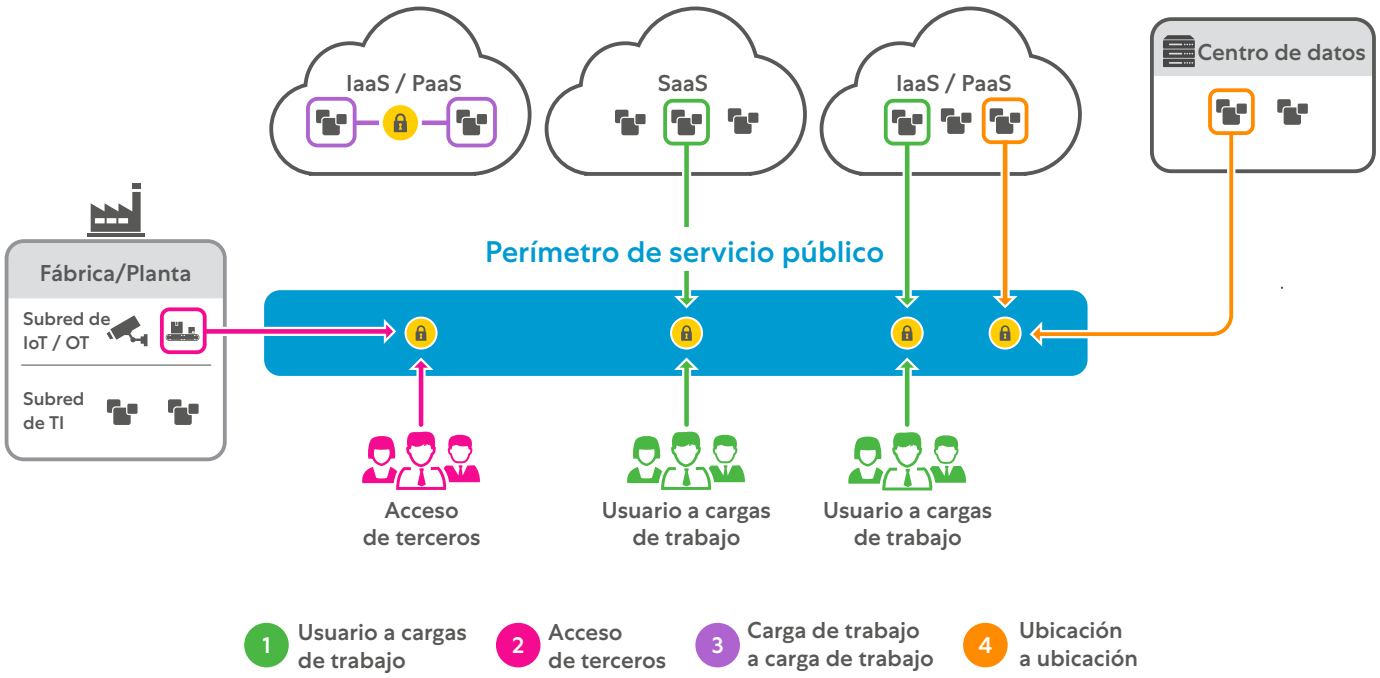

Figura 7: Un enfoque sugerido para la segmentación empresarial. Permitir un enfoque de control, aprendizaje, segmentación y aislamiento por fases, como parte de una implementación de confianza cero

Un ejemplo reciente: cuando los investigadores de seguridad descubrieron la vulnerabilidad de día cero de Log4j, todos los clientes que ejecutaban la utilidad de registro vulnerable basada en Java de Apache corrían el riesgo de una ejecución remota completa de código. Sin embargo, aquellos que adoptaran una arquitectura de confianza cero tendrían sus aplicaciones internas completamente invisibles a Internet, lo que significaba que los atacantes no podrían encontrarlas ni explotarlas, salvaguardando incluso las versiones susceptibles de Apache Log4j de esta y futuras vulnerabilidades. Esto habría sido imposible con servicios heredados y expuestos, como las VPN y los cortafuegos. **La confianza cero garantiza que solo los usuarios autorizados puedan acceder a las aplicaciones; evita el movimiento lateral con la microsegmentación de usuario a aplicación y de aplicación a aplicación, y puede inspeccionar tanto el tráfico entrante como el saliente**.

Lo mismo ocurrió con el ataque a Colonial Pipeline, en el que las credenciales de VPN robadas (que no tenían activado el MFA) dieron a los piratas informáticos acceso para moverse lateralmente por la red y acceder a datos confidenciales. Una arquitectura de confianza cero que conecta exclusivamente a los usuarios autorizados a las aplicaciones y no a las redes evita el movimiento lateral segmentando las comunicaciones de usuario a aplicación y de aplicación a aplicación.

⚠ ¿Qué debo tener en cuenta?

- Evite los servicios SSE que no sigan los principios de la arquitectura de confianza cero, como la publicación especial 800-207 del NIST.
- Asegúrese de que el servicio SSE ofrezca controles de confianza cero para todos los recursos empresariales, no solo para los usuarios.
- La confianza cero no hace función de cortafuegos o SD-WAN. Es independiente e indiferente de la red. Un SSE de un proveedor que depende de la red puede exponerle a una deficiencia arquitectónica de confianza cero.
- Asegúrese de que los controles de confianza cero comiencen con un acceso cero; no se debe poder acceder a los activos empresariales hasta que se validen.
- Aborde todos los aspectos de su empresa. No limite sus controles de confianza cero a una parte de la misma.

Resultados:

La protección de una empresa y sus usuarios se debe acometer de tal manera que brinde acceso en base a la necesidad de saber y de privilegios mínimos. **La confianza cero debe ser la base 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.
- Deben evitarse las soluciones que fuerzan la conectividad a la red y el acceso debe ser independiente de la red, en todas partes.
- El servicio SSE ofrece una superficie de ataque cero para sus servicios empresariales privados.

N.º 3
Error

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

En su lugar, considere soluciones SSE que:

- Proporcionen inspección SSL/TLS del tráfico a escala de producción con un impacto mínimo en el rendimiento. Esto requiere una arquitectura proxy escalable.
- Recojan y analicen información estratégica detallada obtenida de la inspección para aplicar protección frente a amenazas avanzadas para el tráfico cifrado y apliquen políticas avanzadas de clasificación de datos para la prevención de la pérdida de datos.
- Inspeccionen todo el tráfico, incluido el cifrado, de usuarios, cosas, cargas de trabajo, etc.

Cómo los proveedores de SSE adecuados hacen que esto funcione:

Los proveedores de SSE no pueden afirmar tener la mejor protección contra amenazas avanzadas y prevención de 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 proveedores de SSE en este sentido, ya que muchas cosas dependen de la arquitectura subyacente de la solución. Aquellos proveedores de SSE que han construido su proxy en la nube como nativo de la nube desde cero tienen una ventaja clara en esta área.

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

- El cifrado SSL/TLS puede ocultar contenido nocivo, como virus, spyware y otros tipos de malware.
- Los atacantes crean sus sitios web con cifrado TLS y SSL, o inyectan contenido malicioso en sitios conocidos y fiables habilitados para SSL y TLS.
- SSL/TLS puede ocultar fugas de datos, como la transmisión de documentos financieros confidenciales de una organización.
- SSL/TLS puede ocultar la navegación de sitios web de ámbitos de responsabilidad legal.
- La capacidad de controlar e inspeccionar el tráfico hacia y desde los servicios en línea utilizando HTTPS se ha convertido en una pieza importante de la postura de seguridad de una organización.

©2022 Zscaler, Inc. Todos los derechos reservados.

Figura 8: La arquitectura de paso que emplean algunos proveedores no proporciona la inspección del tráfico cifrado a escala, de forma similar a un puesto de control de seguridad básico que permite el paso de un coche sin revisar su maletero en busca de carga maliciosa

Teniendo en cuenta estos riesgos, la arquitectura de un proveedor de SSE debe escalar para funcionar como un proxy SSL/TLS central que proporcione un análisis completo del contenido entrante y saliente, y bloquee inmediatamente cualquier amenaza detectada en cualquier lugar de la nube.

Los actores de las amenazas continúan evolucionando sus herramientas, técnicas y procedimientos cuando atacan a las organizaciones, lo que incluye el abuso de proveedores legítimos de servicios de almacenamiento como Dropbox, Box, OneDrive y GDrive para alojar cargas útiles maliciosas. Estas conexiones utilizarán certificados SSL/TLS comodín de estos reputados proveedores al servir las cargas útiles maliciosas, que si no se inspeccionan darán lugar a un ataque con éxito. Las cargas útiles maliciosas (ejecutables, documentos de office, 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 la carga útil de estas conexiones cifradas SSL/TLS y debe ser capaz de desempaquetar y desofuscar estos archivos para una detección precisa (véase la Figura 9).

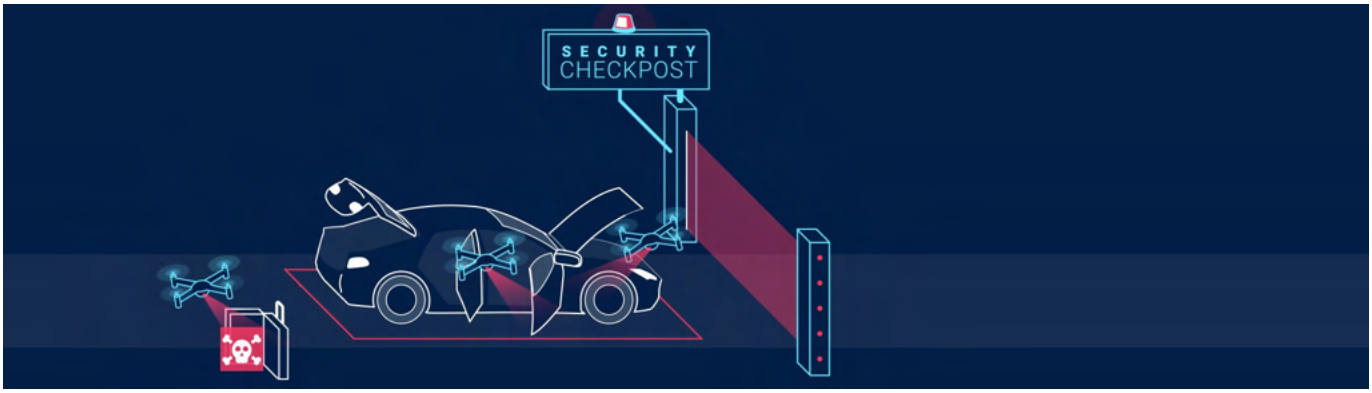

Figura 9: El proveedor de SSE adecuado proporciona inspección SSL/TLS completa de todo el tráfico mediante una arquitectura proxy, similar a un coche al que se detiene y se inspecciona completamente antes de que se le permita pasar el puesto de control de seguridad.

Esta protección frente a amenazas debe aprovechar muchas fuentes de amenazas del sector a través de fuentes de código abierto, comerciales y privadas, así como tener actualizaciones de seguridad frecuentes.

©2022 Zscaler, Inc. Todos los derechos reservados.

Además de bloquear amenazas, la inspección a escala habilita 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 de pérdidas de datos personales, de salud y confidenciales. Esta clasificación requiere inspección SSL/TLS y permite capacidades avanzadas como:

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

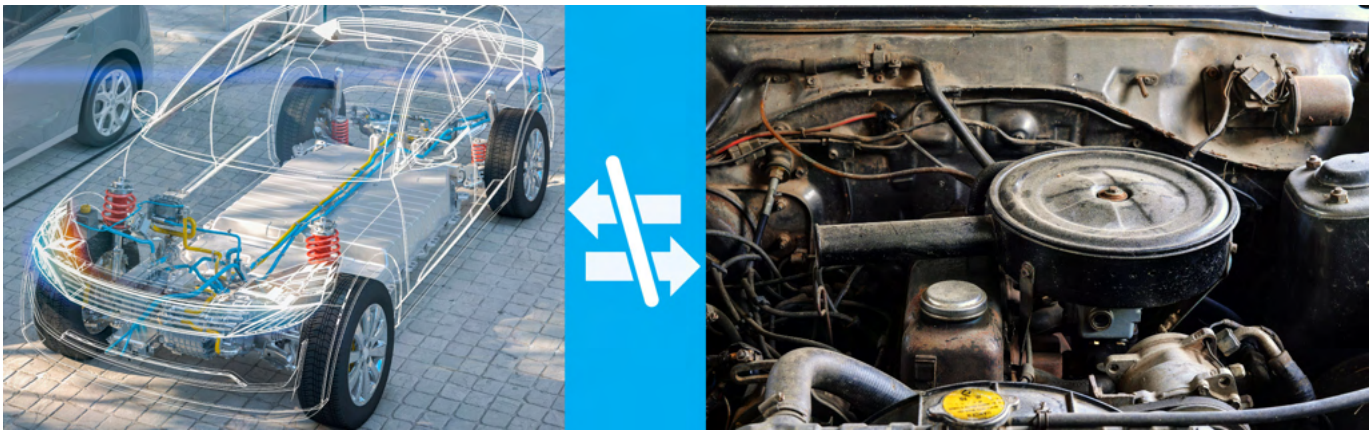

Figura 10: Al igual que un motor de combustión interna no se puede adaptar para que funcione como un vehículo eléctrico, sea cauteloso con los proveedores que vinculan capacidades como la inspección SSL/TLSa arquitecturas heredadas

SSE incluye la funcionalidad de agente de seguridad de acceso a la nube (CASB) para supervisar y aplicar las políticas entre los usuarios de los servicios 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 analizar las API de los proveedores de SaaS para proteger los datos en reposo, o "en línea", que es el análisis de los datos en movimiento. Preste especial atención a esta última, ya que la inspección en línea evita que los datos se carguen en aplicaciones no sancionadas, que se descarguen en dispositivos no autorizados y que se descargue o cargue contenido malicioso. 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, actualmente los datos confidenciales de las organizaciones tienen una gran distribución. Los dos principales canales de exfiltración de datos son el escritorio en la nube y las aplicaciones de correo electrónico personales. Un buen proveedor de SSE debe ofrecer visibilidad contextual y cumplimiento completos cuando los usuarios fraudulentos cargan datos confidenciales en su Box personal, Dropbox y otros equipos de escritorio en la nube. También debe detener la exfiltración de datos en servicios de correo web personales y no autorizados, como Gmail y Hotmail.

©2022 Zscaler, Inc. Todos los derechos reservados.

Donde la diferencia entre los proveedores de SSE se hace evidente es en hasta qué punto su capacidad de descifrar e inspeccionar el tráfico SSL/TLS se adapta de manera elástica según las demandas de tráfico, y en si este nivel de inspección se realiza sin afectar al rendimiento, todo lo cual solo se puede lograr con una solución SSE basada en proxy creada pensando en la adaptación desde el principio (véase la Figura 10).

Es importante analizar detenidamente cómo logra todo esto el proveedor de SSE. Para mantener una latencia mínima en cada inspección de paquetes, el proveedor debe emplear una arquitectura de paso único en la que el paquete se coloca en la memoria una vez y los servicios de inspección, cada uno con recursos de CPU dedicados, pueden realizar sus análisis de manera simultánea. Los proveedores que ofrecen estas inspecciones en cadena con aplicaciones físicas y virtuales en serie incurren en una penalización de procesamiento en cada salto y corren el riesgo de que se aplique un exceso de latencia 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 diferentes al cliente y al servidor. Puesto que esto permite volver a montar y analizar todo el objeto, se pueden aplicar protección frente a amenazas avanzadas, DLP y sandboxing. Asegúrese de que su proveedor maneja las versiones TLS y las actualizaciones de cifrado sin problemas 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 gestión de certificados, dada la complejidad potencial que se puede introducir. Los proveedores de SSE deben permitir el uso de sus certificados o traer los suyos, y permitir la rotación entre los dos a través de la API. Los certificados se deben replicar automáticamente entre los distintos ejes de servicio.

Tenga cuidado con los proveedores de SSE que pueden dirigir las capacidades de inspección SSL/TLS a NGFW existentes, que tienen desafíos de adaptación inherentes. Esto afecta incluso a los proveedores que trasladan los NGFW con capacidades de inspección a instancias virtuales en nodos de computación CSP

⚠ ¿Qué debo tener en cuenta?

Al evaluar la capacidad de un proveedor de SSE para inspeccionar SSL/TLS, asegúrese de comprobar que la latencia en la que se ha incurrido es aceptable. Desafortunadamente, las arquitecturas no nativas de 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 una preocupación, por lo que hay que entender las restricciones normativas 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 y nunca deben almacenar los datos del usuario en la nube.

Tenga cuidado con los proveedores de SSE que pueden dirigir las capacidades de inspección SSL/TLS a NGFW existentes, que tienen desafíos de adaptación inherentes. Esto afecta incluso a los proveedores que trasladan los NGFW con capacidades de inspección a instancias virtuales en nodos de computación CSP Tenga también cuidado con los proveedores que combinan capacidades CASB fuera de banda con una inspección limitada del tráfico en línea. La seguridad de los datos en reposo y en movimiento es fundamental.

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

La implantación de la inspección SSL/TLS ha sido históricamente complicada para las empresas por varias razones. **El proveedor de SSE debe ser el experto de confianza principal 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 se debería sacrificar la velocidad en beneficio de la seguridad en absoluto.

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 nativa de la nube adecuada lograrán:

- Inspección SSL/TLS de todo el tráfico a escala de producción con un impacto mínimo en el rendimiento para la protección más completa de los datos y frente a las amenazas.
- Una arquitectura de exploración de memoria individual 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 con el fin de lograr la inspección SSL/TLS.

N.º 4
Error

Elegir una solución SSE que sea "única para todo" y no admita opciones de despliegue y gestión flexibles, escalables y diversas

En su lugar, considere soluciones SSE que:

- Ofrezcan modelos de despliegue flexibles para proteger a los usuarios y las aplicaciones dondequiera que la aplicación esté alojada, incluidos el centro de datos, la nube pública, la nube privada, el nodo de computación perimetral y en las instalaciones.
- Ofrezcan protección a los usuarios que acceden a las aplicaciones tanto en dispositivos de usuario final gestionados como en dispositivos no gestionados.
- Extiendan esas mismas protecciones de datos y frente a amenazas para proteger todas las demás comunicaciones de carga de trabajo a carga de trabajo dentro de la misma nube o en varias.

Cómo los proveedores de SSE adecuados hacen que esto funcione:

Los evaluadores de soluciones SSE deben valorar la preparación de su entorno para comprender la mejor manera de aplicar las protecciones SSE. Para acomodarse a la variedad de escenarios de despliegue, los proveedores de SSE deben permitir tanto los perímetros de servicio público como los perímetros de servicio privado.

Cómo los proveedores de SSE adecuados hacen que esto funcione:

Los evaluadores de soluciones SSE deben valorar la preparación de su entorno para comprender la mejor manera de aplicar las protecciones SSE. Para acomodarse a la variedad de escenarios de despliegue, los proveedores de SSE deben permitir tanto los perímetros de servicio público como los perímetros de servicio privado.

La mayoría de los usuarios se conectarán a SSE a través de un perímetro de servicio público del proveedor. Se trata de pasarelas de Internet seguras y con todas las funciones, así como de agentes de aplicaciones privados que proporcionan seguridad integrada. Inspeccionan todo el tráfico bidireccional en busca de malware, aplican políticas de seguridad, cumplimiento y cortafuegos, y deben gestionar cientos de miles de usuarios simultáneos con millones de sesiones simultáneas. Por ello, independientemente de dónde se encuentren sus usuarios, pueden acceder desde cualquier dispositivo:

- Internet con los perímetros de servicio público protegiendo el tráfico y aplicando sus políticas corporativas.
- Aplicaciones internas con políticas de acceso y reautenticación impuestas basadas en las mejores prácticas corporativas de su organización.

Figura 11: Un proveedor de SSE debe ofrecer tanto opciones de perímetro de servicio público como privado, que también deben funcionar en armonía entre sí con una gestión centralizada

©2022 Zscaler, Inc. Todos los derechos reservados.

Es importante asegurarse de que estos perímetros de servicio público tengan una importante capacidad de tolerancia a los fallos y se desplieguen en modo activo-activo para garantizar la disponibilidad y la redundancia. El proveedor debe supervisar y mantener sus perímetros de servicio público para garantizar una disponibilidad continua. Para garantizar la privacidad de los datos, el tráfico de los clientes no debe pasar a ningún otro componente de la infraestructura y ningún dato debe almacenarse en el disco.

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

Para un acceso seguro a Internet, se pueden instalar perímetros de servicio privado en el centro de datos de una organización y dedicados a su tráfico, pero el proveedor de SSE debe gestionarlos y mantenerlos, con una participación prácticamente nula por parte de la organización. 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 perímetro de servicio privado proporciona una gestión similar de las conexiones entre el usuario y la aplicación y aplica las mismas políticas que el perímetro de servicio público, con el servicio alojado en el sitio o en la nube pública, pero nuevamente lo administra el proveedor de SSE. Este modelo de implementación permite la confianza cero dentro de las instalaciones propias, ya que resulta útil para reducir la latencia de la aplicación cuando una aplicación y un usuario se encuentran en la misma ubicación (y acudir al perímetro de servicio público agregaría latencia adicional). Esta opción también proporciona una capa de supervivencia si se pierde la conexión a Internet. El proveedor de SSE debe distribuir imágenes para su despliegue en los centros de datos de la empresa y en los entornos locales de nube privada.

A fin de brindar protección de confianza cero para aplicaciones internas, los proveedores de SSE deben ofrecer una manera de crear una interfaz segura y autenticada entre sus servidores de aplicaciones y los perímetros de servicio público y privado para proteger las aplicaciones internas. **Este mecanismo debe estar disponible en varios factores de forma**: una imagen de máquina virtual (VM) estándar o una implementación contenerizada en centros de datos empresariales, entornos de nube privada locales como VMware o entornos de nube pública como Amazon Web Services (AWS) EC2, y paquetes que se pueden instalar en distribuciones compatibles con Linux.

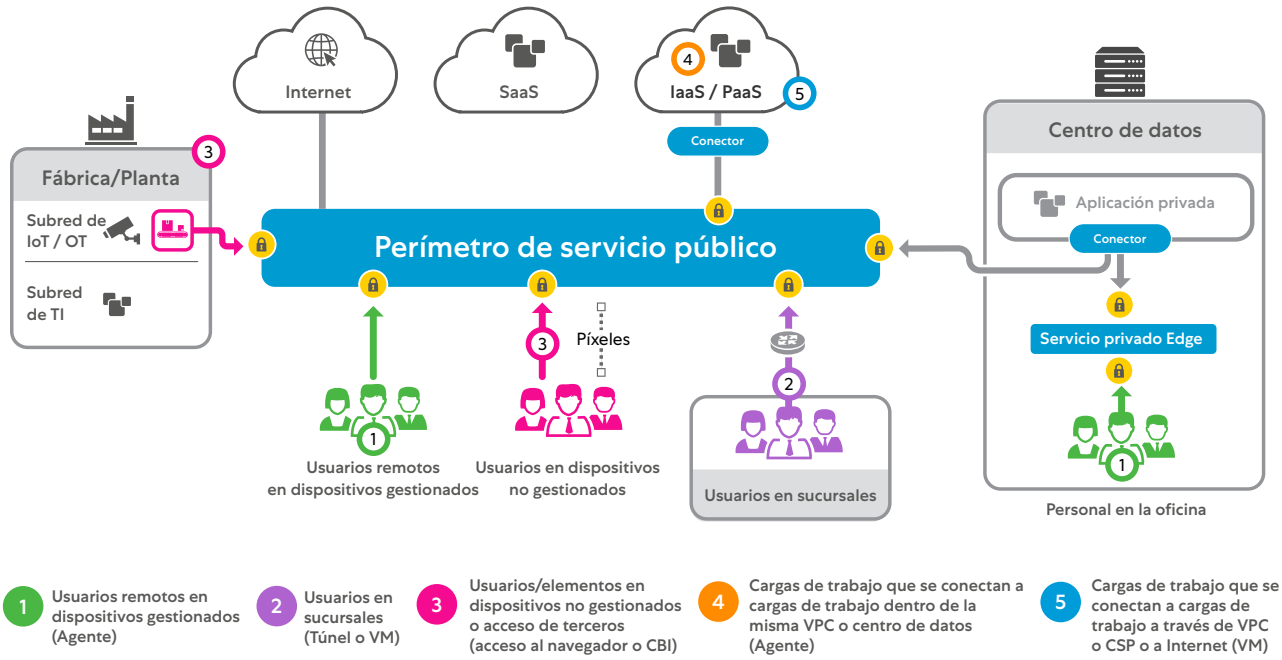

Figura 12: El proveedor de SSE debe ofrecer diversos modos de despliegue y gestión, teniendo en cuenta los usuarios remotos, los usuarios en las sucursales, los usuarios en la sede central, las cargas de trabajo que se comunican con las cargas de trabajo, etc., a través de agentes y máquinas virtuales.

©2022 Zscaler, Inc. Todos los derechos reservados.

Una vez establecido desde dónde se administrarán y aplicarán las políticas SSE, hay que considerar cómo se ofrecerá esta protección a los usuarios y a las cargas de trabajo. Es importante tener en cuenta varios escenarios (véase la Figura 12):

Para los usuarios remotos en dispositivos gestionados, el proveedor de SSE debe ofrecer un solo agente unificado que reenvíe el tráfico al perímetro del servicio para un acceso seguro a Internet. El agente también debe proporcionar acceso granular basado en políticas a los recursos internos. Todo esto debe ser automático utilizando la inteligencia incorporada en el agente. También debe proteger el tráfico móvil de los usuarios en redes wifi o móviles. El agente reenvía el tráfico de los 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 se conecta un usuario a una red confiable y, si se detecta una red fiable, si el agente debe desactivar su servicio, según lo que determine la política. Asegúrese de que estos agentes sean compatibles con 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 perímetro de servicio es a través de un túnel GRE o IPSec. No obstante, 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 acabar con el movimiento lateral de amenazas eliminando la red enrutable gestionada por el cliente. La implementación debe automatizarse e incluir políticas flexibles de direccionamiento de tráfico al perímetro de servicio con supervisión de SLA y conmutación por error integradas. Esta opción funciona bien para sucursales de tamaño medio y grande, y aquellas que ofrecen servicios locales.

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

Para los usuarios/objetos 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 de confianza cero mediante la publicación de un CNAME específico de la aplicación en su zona DNS de tal modo que el navegador web pueda redirigir automáticamente esas solicitudes. Como alternativa, el proveedor de SSE también debe tener una capacidad integrada de aislamiento del navegador en la nube (CBI) para una seguridad sin agente para cualquier dispositivo no gestionado en cualquier lugar. Como beneficio secundario, esto evita por completo la necesidad de un proxy inverso frágil.

Con CBI, los administradores configurarían los ajustes SSO de un recurso en la nube autorizado para redirigir al proveedor de SSE. Después, cuando los usuarios intentan acceder a dicho recurso en la nube desde un punto final personal o de terceros, su tráfico se envía a CBI automáticamente y sin necesidad de instalar ningún software. Representa el contenido en píxeles que se envían a los dispositivos del usuario, evitando la descarga, la copia, el pegado y la impresión. De este modo, los usuarios pueden realizar sus tareas laborales desde puntos finales no gestionados sin el riesgo de filtraciones de datos y cargas de malware, todo ello respetando los requisitos de cumplimiento.

Para las cargas de trabajo que se conectan a cargas de trabajo dentro de la misma VPC o centro de datos, la segmentación de red tradicional era la respuesta. Si bien esto tenía sentido en un plano teórico, lograr la segmentación de red en la práctica era todo 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 una instalación de agente en la carga de trabajo en sí, el proveedor de SSE debería determinar el riesgo y aplicar protección basada en identidad a sus cargas de trabajo, sin cambios en la red, y debería tener políticas que se adapten automáticamente a los cambios del entorno.

©2022 Zscaler, Inc. Todos los derechos reservados.

En el caso de las cargas de trabajo que se conectan a cargas de trabajo a través de VPC o CSP o a Internet, los proveedores de SSE deben volver a extender a estas cargas de trabajo una protección SSE similar a la ofrecida a los usuarios. Para ello, los proveedores de SSE deben ofrecer un mecanismo, normalmente a través de una máquina virtual (disponible en nubes públicas o hipervisores locales), que simplifique el reenvío de tráfico al perímetro del servicio. El resultado es la protección frente a las ciberamenazas y de los datos para las cargas de trabajo que llegan a Internet, así como protección de confianza cero para las cargas de trabajo en una nube que acceden a las cargas de trabajo en otra nube. Con este enfoque, los proveedores de SSE pueden consolidar múltiples productos (por ejemplo, proxies web, cortafuegos, pasarelas NAT, filtrado de URL, etc.) en una única solución.

Para asegurar los datos en reposo en entornos IaaS y SaaS, el proveedor de SSE también debe proporcionar soluciones en el espacio de CASB, gestión de derechos de infraestructura en la nube (CIEM) y gestión de la postura de seguridad en la nube (CSPM), de modo que pueda producirse un análisis basado en API con aplicaciones SaaS e IaaS populares. Esto permite identificar y remediar las configuraciones erróneas y los permisos inadecuados dentro de los entornos de la nube, junto con la auditoría y las exploraciones de las plataformas SaaS e IaaS para la protección de los datos y frente a amenazas. Un proveedor de SSE debe ofrecer estas capacidades fuera de banda en estrecha consonancia con sus capacidades en línea para aplicar políticas coherentes a los datos en reposo y en movimiento.

La ventaja de que un único proveedor de SSE proporcione este amplio marco de protección es que puede gestionarse desde un plano de control central con políticas corporativas aplicadas de forma uniforme y dinámica en todas las comunicaciones entre usuarios/objetos y aplicaciones y entre cargas de trabajo.

⚠ ¿Qué debo tener en cuenta?

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 tremendamente importante**. Además, ciertos países como China presentan desafíos únicos en cuanto a rendimiento debido a sus controles de Internet que ni siquiera los modelos de implementación flexibles pueden superar. El proveedor de SSE debe ofrecer soluciones innovadoras para afrontar estos desafíos.

Resultados:

Implantadas correctamente, estas opciones flexibles, diversas y escalables proporcionarán a su organización todas las ventajas del perímetro de servicio de seguridad, independientemente de dónde se encuentre el usuario o el objeto, o de dónde esté alojada la aplicación, e incluso ampliarán dicha protección dentro de la propia aplicación:

- La ventaja de que un único proveedor de SSE proporcione este amplio marco de protección es que puede gestionarse desde un plano de control central con políticas corporativas aplicadas de forma uniforme y dinámica en todas las comunicaciones entre usuarios/objetos y aplicaciones y entre cargas de trabajo.
- Extender la misma protección de los dispositivos gestionados a los dispositivos propios no gestionados y al acceso de terceros permite una mayor flexibilidad para los contratistas y los empleados.
- La seguridad de carga de trabajo a carga de trabajo ofrece a los ingenieros de DevOps y CloudOps las mismas protecciones de confianza cero para sus aplicaciones que acceden a otras cargas de trabajo, otras nubes o Internet.

N.º 5
Error

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

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

- Sean transparentes, fáciles de autenticar y estén siempre activos, para asegurar que los usuarios finales en su plataforma de SSE disfrutan de una gran experiencia de usuario utilizando medidas objetivas.
- Correlacionen la mala experiencia del usuario final con sus causas subyacentes, ya sea el punto final, la red, la aplicación o la pila de seguridad.
- Aprovechen las asociaciones con los proveedores de SaaS más populares, como Microsoft 365, para minimizar la latencia entre el perímetro de servicio público y la red del proveedor de aplicaciones

Cómo los proveedores de SSE adecuados hacen que esto funcione:

Los puntos de presencia del proveedor de SSE en todo el mundo y las relaciones de intercambio de pares de Internet con proveedores y proveedores de aplicaciones ofrecen una potente alternativa al retorno y los bucles invertidos que requieren las pilas de seguridad heredadas.

Más allá de estos beneficios arquitectónicos, los proveedores de SSE están en una posición única para medir y diagnosticar la experiencia del usuario final gracias a 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 profundas mediante el aprovechamiento de la infraestructura del perímetro de servicio público.

Céntrese en los proveedores de SSE que han integrado una solución de supervisión (**comúnmente llamada supervisión de la experiencia digital** o DEM) en sus agentes e infraestructura de nube existentes. Aquellos proveedores que ofrezcan soluciones que requieran agentes adicionales o sean adquisiciones poco integradas no proporcionarán el mismo nivel de visibilidad y diagnóstico.

La solución DEM que ofrezcan los proveedores de SSE debe ser amplia, que proporcione visibilidad de extremo a extremo y resolución de problemas de rendimiento del usuario final para cualquier usuario o aplicación, independientemente de su ubicación. Además, debe permitir la supervisión continua de los equipos de red, seguridad, escritorio y servicio de asistencia técnica con información sobre los problemas de rendimiento de los dispositivos, la red y las aplicaciones de los usuarios finales. Por último, debe permitir tanto flujos de trabajo reactivos que ayuden a cerrar los tickets de problemas comunicados por los empleados, como flujos de trabajo proactivos que ayuden a identificar macroproblemas (como cortes regionales del ISP o caídas globales de las aplicaciones) antes de que los usuarios se den cuenta. **Esto se debe habilitar mediante algoritmos de puntuación basados en el aprendizaje automático que hagan un seguimiento de la experiencia normal del usuario frente a la anormal por usuario, aplicación, oficina o localización geográfica**.

Esta supervisión debe darse a 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 el salto de SSE está induciendo un retraso anómalo y cuándo. Finalmente, la solución debe brindar información estratégica sobre el estado del dispositivo de punto final del usuario e identificar los eventos del dispositivo que contribuyen a las caídas de puntuación (**véase la Figura 13**).

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

©2022 Zscaler, Inc. Todos los derechos reservados.

Supervisión del rendimiento de la calidad y resolución de problemas de Microsoft Teams y Zoom

Ahora que Teams y Zoom se están convirtiendo en las principales plataformas de colaboración y comunicación para muchas organizaciones, la medición y el diagnóstico de los problemas de calidad del audio/vídeo son incluso más urgentes. Las soluciones de DEM que proporcione el proveedor de SSE deben ser capaces de interactuar con las aplicaciones UCaaS más populares, como Zoom y Microsoft Teams, para tomar las métricas de calidad de audio y vídeo y combinarlas con el análisis exhaustivo de la red salto a salto y de los dispositivos de punto final. Al combinar estos conjuntos de datos, la solución de DEM debe identificar a aquellos que tienen problemas de calidad, así como proporcionar una causa raíz para el problema.

Además, la DEM debe aprovechar la escala de la nube del proveedor de SSE, utilizándola para realizar pruebas de telemetría de 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.

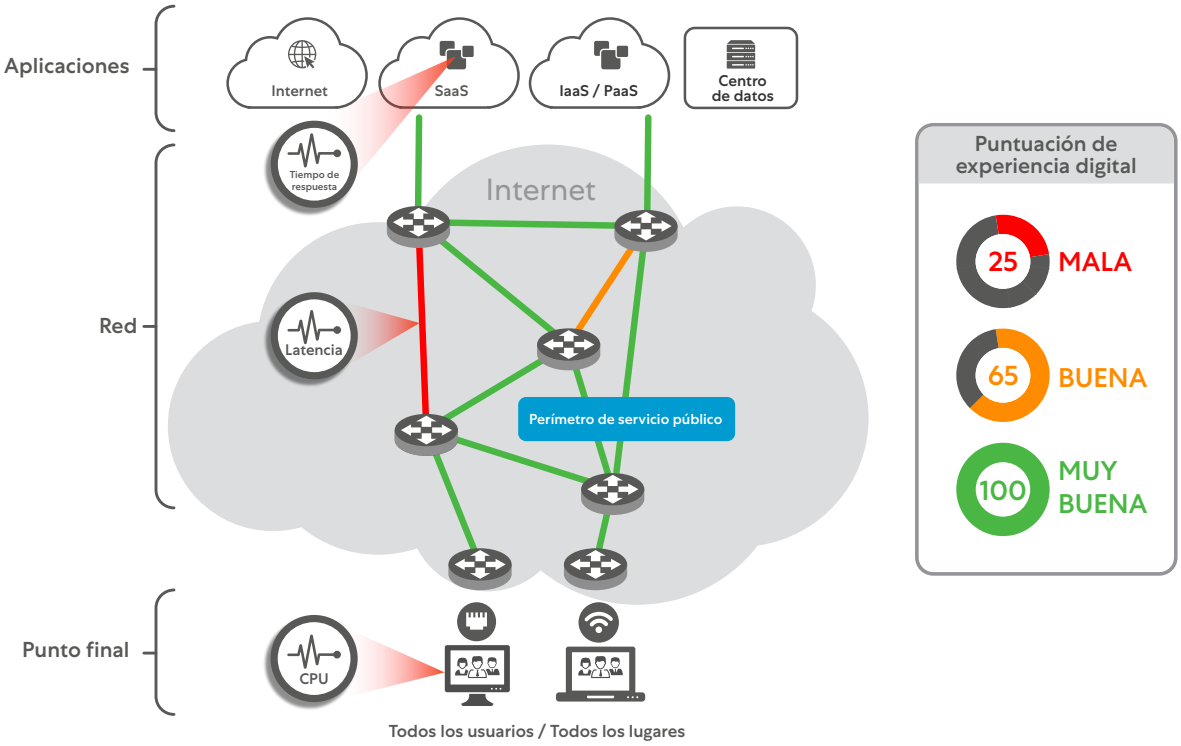

Figura 13: Una solución de DEM integrada como parte de la plataforma SSE debería proporcionar una visibilidad única de la calidad de la experiencia del usuario desde la perspectiva del usuario final, lo que arrojaría luz sobre los problemas del punto final, la red y la aplicación

Tenga cuidado con las herramientas de supervisión heredadas que adoptan un enfoque centrado en el centro de datos para supervisar 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 a un tiempo de resolución de problemas prolongado. Las herramientas de supervisión de puntos optimizadas para los centros de datos dejan brechas de visibilidad para 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 (véase la Figura 14).

La solución de DEM debe identificar a aquellos que tienen problemas de calidad, así como proporcionar una causa raíz para el problema

©2022 Zscaler, Inc. Todos los derechos reservados.

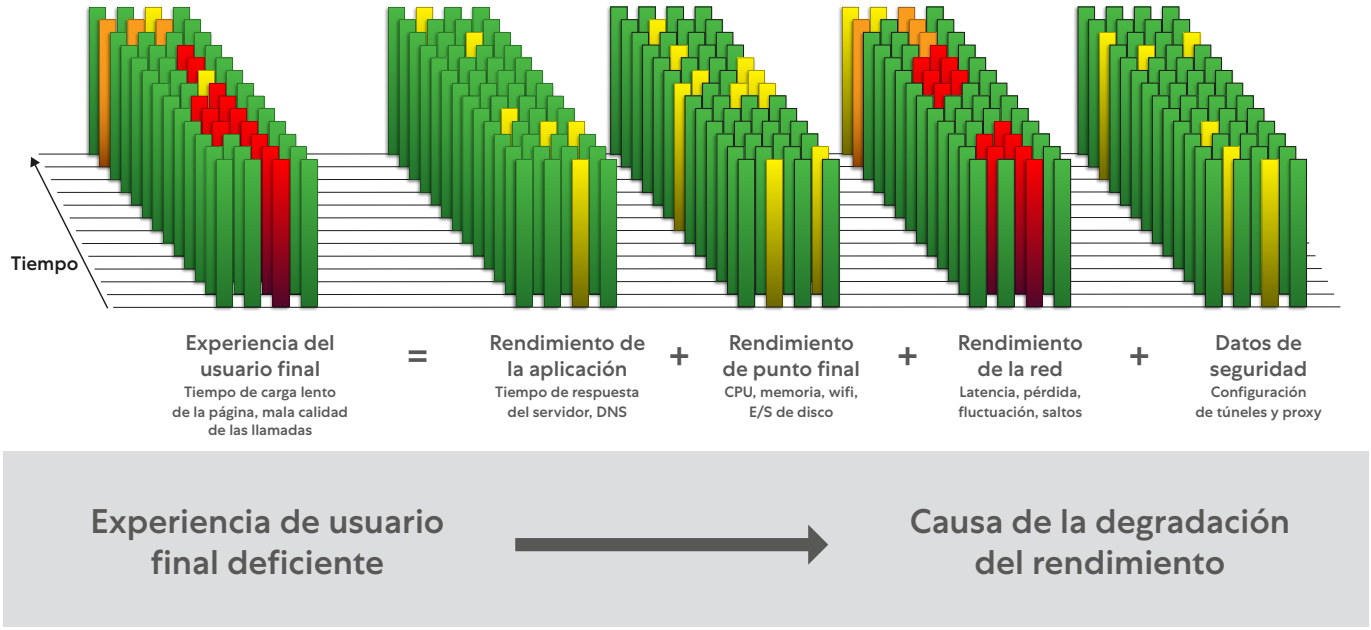

Figura 14: Una solución de DEM integrada como parte de la plataforma SSE debería proporcionar una visibilidad única de la calidad de la experiencia del usuario desde la perspectiva del usuario final, lo que arrojaría luz sobre los problemas del punto final, la red y la aplicación

Optimización de la experiencia del usuario de M365

Un SSE integral puede ir más allá de la medición y el diagnóstico de la experiencia del usuario final para optimizar el rendimiento de aplicaciones SaaS populares como Microsoft 365. El reto es que la mayoría de las empresas dirigen el tráfico centralmente 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, por lo que la experiencia del usuario se ve negativamente afectada. Microsoft recomienda las conexiones directas a Internet y la arquitectura de los proveedores de SSE que permiten los accesos locales de Internet para proporcionar un rendimiento y un coste óptimos.

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

©2022 Zscaler, Inc. Todos los derechos reservados.

Pero la arquitectura es importante. Los puntos de presencia del proveedor de SSE en todo el mundo y la relación de interrelación con proveedores y vendedores de aplicaciones deben acercar el perímetro a los usuarios para una conectividad rápida y un acceso de baja latencia. Busque proveedores de SSE que establezcan interconexiones con fibra directa a Microsoft 365 en la mayoría de los principales intercambios para reducir la latencia a aproximadamente 1-2 ms de tiempo de ida y vuelta, adaptarse para manejar el alto número de conexiones de larga duración, permitir descargas rápidas de archivos y proporcionar una rápida resolución de DNS con menos saltos (véase la Figura 15).

Es especialmente importante proteger sus 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 todas las comunicaciones hacia y desde las aplicaciones de M365. Sin embargo, tenga en cuenta que ciertas aplicaciones de M365 como Teams pueden no necesitar ser inspeccionadas, dado que gran parte de este tráfico es de voz/vídeo vía UDP.

⚠ ¿Qué debo tener en cuenta?

Ya que en nuestro mundo trabajamos desde cualquier lugar (work from anywhere [WFA]), hay muchos enlaces débiles a lo largo de la cadena para suministrar un buen rendimiento de las aplicaciones en el entramado global de redes inalámbricas y por cable. Optimizar la experiencia del usuario es difícil incluso con una arquitectura superior y con conjuntos de herramientas que sirven para medir y diagnosticar los problemas de UX. Es esencial establecer unas expectativas razonables con los usuarios finales sobre lo que constituye una experiencia de usuario aceptable de las aplicaciones críticas. A continuación, es vital utilizar estas expectativas para establecer unas líneas de base que controlar y gestionar.

Diagnosticar los problemas de la experiencia del usuario es más un arte que una ciencia. Requiere unas herramientas y una arquitectura excelentes, pero también depende de que se disponga de los conocimientos adecuados para interpretar los datos y actuar en relación a ellos. Aunque las herramientas de DEM que ofrecen los proveedores de SSE pondrán de manifiesto la mayoría de las causas de los problemas (wifi, ISP, red troncal, punto final o problemas de DNS), un subconjunto requerirá una ampliación y conjuntos de datos adicionales. Por ejemplo, pueden ser necesarios el rastreo de registros y 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.

Desconfíe de los proveedores que meten el tráfico en un bucle invertido. 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 nativa de la nube no debería dirigir el tráfico mediante bucles invertidos a unas pocas ubicaciones centralizadas para inspeccionarlo. Por ejemplo, si un usuario aparece en Melbourne, la inspección de su tráfico debería realizarse localmente con servicios de prevención de amenazas y protección de datos, y no ser retornada a otras regiones como Sídney o Singapur. Los proveedores de SSE que ejecutan su nube en hiperescaladores a menudo acaban dirigiendo el tráfico de los usuarios mediante bucles invertidos. Un hiperescalador puede tener 120 puntos perimetrales, pero es probable que el 80 % de ellos sean cauces de entrada para llevar el tráfico a un número menor de centros de datos del hiperescalador donde se pueda aplicar el control de la política de SSE. Es importante entender cuántos centros de datos son cauces de entrada y cuántos pueden realmente aplicar la política.

Resultados:

El éxito de cualquier transformación, ya sea digital, de red o de seguridad, dependerá de cómo la experimente el usuario final. El objetivo final de cualquier proyecto de SSE es mejorar la experiencia del usuario final y, al mismo tiempo, reducir la exposición a las amenazas y proteger los datos confidenciales. Por lo tanto, el resultado ideal es que la capacidad de un proveedor de SSE para mejorar la UX pueda medirse con la capacidad de DEM. Esto debería ser una tarea fácil, ya que alejarse del uso de bucles invertidos hacia un centro de datos o alejarse de las VPN son formas perfectamente aceptables de mejorar la experiencia del usuario:

- La solución SSE debe modernizar la experiencia del usuario y actualizar la experiencia de resolución de problemas. Al adoptar un enfoque proactivo de la experiencia del usuario, el servicio de resolución de problemas puede reaccionar antes de que los usuarios se quejen.
- La solución SSE debe proporcionar información sobre el rendimiento del audio y vídeo en tiempo real para plataformas de colaboración como Teams y Zoom.
- La solución SSE debe recopilar métricas de las capas de aplicación, extremo y red para encontrar anomalías y determinar la 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 limitada en cuanto a la integración y orquestación con un ecosistema de proveedores ajenos

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

- Se integren a través de API sólidas con otros de los mejores reproductores de ecosistemas (como CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) para garantizar una protección y una experiencia de usuario óptimas.
- Aprovechen estas integraciones para permitir la automatización y la orquestación, así como para reducir la complejidad operativa y los gastos generales.
- No añadan deuda técnica combinando una cartera de soluciones con una integración limitada tanto dentro de la cartera como con terceros

Cómo los proveedores de SSE adecuados hacen que esto funcione:

La mayoría de las organizaciones que tienen dificultades con la deuda técnica son conscientes de que gran parte de ella se debe a la adquisición de tecnologías de proveedores a lo largo de los años que no logran interactuar entre sí.

Peor es la llamada "plataforma" que ofrece un único proveedor que no está realmente integrada, sino que es una colección de productos puntuales adquiridos que no tienen una integración real más allá de un cuadro de mandos. A menudo, la operación de estas tecnologías de proveedores requiere conocimientos especializados y son tecnologías que coexisten frágilmente con las tecnologías que las acompañan. SSE puede eliminar gran parte de esta deuda técnica con una plataforma de seguridad unificada en la nube suministrada por un único proveedor. Teniendo en cuenta esta visión, SSE sigue viviendo en un ecosistema de tecnologías complementarias, y los vendedores deben considerar la interoperabilidad con este ecosistema como un objetivo primordial **(véase la Figura 16)**. Este ecosistema se compone, en general, de otras soluciones de seguridad, red y nube.

Figura 16: No se encuentre como si estuviera en el desierto, sin recursos, con un proveedor que no tenga un rico ecosistema de integraciones de terceros, ya que esto conduce a una deuda técnica, una interoperabilidad limitada y una pila de seguridad frágil (no ágil).

©2022 Zscaler, Inc. Todos los derechos reservados.

Para garantizar un despliegue y una integración rápidos, sencillos y seguros, el proveedor de SSE debe proporcionar integraciones con líderes en:

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

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

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

Para las aplicaciones internas que se trasladan a la nube o se desarrollan de forma nativa 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 y de confianza cero a esas 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 la conectividad interna y basada en políticas en lugar de ampliar la red para que accedan a ella.

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 la nube sin añadir ninguna complejidad de segmentación de la red. No depende de ningún dispositivo virtual o físico y aporta las ventajas de la confianza cero para eliminar la superficie de ataque.

En el caso de las aplicaciones SaaS más populares, los proveedores de SSE deberían ofrecer 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 M365 enumeradas, lo que permitirá 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 y una resolución de DNS más rápidas.

La integración 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 basándose en las políticas de DLP y bloquear la carga saliente de archivos de datos confidenciales. La integración con ServiceNow Security Incident Response puede orquestar acciones de respuesta, incluida la actualización de listas de bloqueo personalizadas. Se pueden bloquear IP, dominios y URL peligrosas sin intervención manual, al mismo tiempo que se pueden cerrar las configuraciones incorrectas en la nube para ayudar a reducir el riesgo de infracciones.

Detección y respuesta en puntos finales

El proveedor de SSE debe integrarse con varios socios de seguridad de puntos finales para compartir la telemetría, mejorar la visibilidad mutua y orquestar las respuestas. Dicha integración permite que la defensa en profundidad implemente la confianza cero de manera eficaz y eficiente.

Esta integración debe proporcionar la capacidad de evaluar la identidad del usuario, la ubicación y la postura del dispositivo para aplicar automáticamente las políticas de acceso condicional adecuadas. 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 las amenazas con el contexto de los puntos finales y de la red para una detección y una toma de decisiones eficaces.

©2022 Zscaler, Inc. Todos los derechos reservados.

SD-WAN

El proveedor de SSE debería integrarse con los proveedores de SD-WAN para simplificar el enrutamiento del tráfico desde la sucursal y facilitar el establecimiento de accesos seguros locales a Internet.

Una solución conjunta SSE/SD-WAN puede permitir un acceso seguro y basado en políticas a Internet y a las aplicaciones críticas para la empresa, y proporcionar una protección idéntica para todos los usuarios, dondequiera y cuandoquiera que se conecten a las aplicaciones en la nube y a la Internet abierta. Las soluciones SD-WAN pueden integrarse con SSE mediante la integración de la API. Con esta solución combinada, las sucursales de la empresa son capaces de gestionar el aumento del tráfico de la nube y de Internet sin tener que retornar los datos a la DMZ centralizada del centro de datos, utilizando una arquitectura WAN híbrida para la transformación de la red junto con una seguridad sólida.

Hay que tener en cuenta que cualquier proveedor de SSE debe ser independiente de la red y no estar vinculado exclusivamente a ninguna solución de red subyacente. De hecho, muchos de los beneficios de la SD-WAN provienen de sus capacidades "definidas por software", pero no necesariamente de la WAN, que inherentemente extiende 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 seguir extendiendo la red corporativa a la sucursal y considerar enfoques alternativos (como el de exclusivamente Internet) que sean más seguros.

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

Gestión de identidad y acceso (IAM)

Los proveedores de SSE deben proporcionar integraciones con las IAM para hacer cumplir el acceso de confianza cero basado en la postura de los dispositivos y una protección contra amenazas más eficaz para toda la empresa.

Utilizando estándares como Security Assertion Markup Language (SAML), el despliegue de la integración debería ser sencillo. 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 del inicio de sesión único (SSO) y de la autenticación multifactor (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 grupo de los usuarios y las eliminaciones de cuentas para las instancias de usuarios que salen de la empresa.

©2022 Zscaler, Inc. Todos los derechos reservados.

SIEM y SOAR

Los proveedores de SSE deben incluir integraciones con proveedores de SIEM y SOAR para permitir una gestión efectiva y eficaz del riesgo y el cumplimiento con enriquecimiento y 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 tanto locales como basadas en la nube para facilitar la correlación de registros de múltiples fuentes, lo que permite a las organizaciones analizar patrones de tráfico en todas sus redes. Además, las organizaciones deben ser capaces de aprovechar los datos de registro del SIEM para realizar análisis históricos ampliados (> 6 meses). De este modo, se garantiza el cumplimiento de la normativa mediante el archivo local de los registros.

Herramientas de organización

A medida que la infraestructura como código (IaC) y DevSecOps obliga a los equipos de seguridad a realizar procesos Shift-left, los proveedores de SSE deben proporcionar las API para la orquestación. Aquí, la atención está en las aplicaciones internas donde la instancia de acceso de confianza cero es parte del ciclo de vida de entrega de aplicaciones, habilitada por scripts de orquestación (como Ansible o Terraform), particularmente para la configuración de segmentación de usuario a aplicación o de carga de trabajo a carga de trabajo. Dicha orquestación permite que las capacidades de confianza cero se alineen con los métodos ágiles que utilizan los desarrolladores de software.

A medida que la infraestructura como código (IaC) y DevSecOps obligan a los equipos de seguridad a realizar procesos Shift-left, los proveedores de SSE deben proporcionar las API para la orquestación.

⚠ ¿Qué debo tener en cuenta?

Los responsables de la toma de decisiones en materia de SSE deben evaluar la profundidad de las integraciones de API y la frecuencia de actualización, y supervisar los cambios en el mercado que puedan impedir futuras integraciones (por ejemplo, que un proveedor adquirido se convierta en un competidor). Sea consciente de la escasez de habilidades en su organización, ya que la implementación de estas integraciones (especialmente con herramientas heredadas) requerirá habilidades especializadas.

Resultados:

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

- Los proveedores de SSE que se integran con los principales actores 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 puede disminuir los errores de los operadores.
- Los proveedores de SSE que reúnen apresuradamente una cartera de soluciones mediante adquisición tienden a quedarse atrás en la innovación de productos y a menudo carecen de interoperabilidad con terceros.

Nº 7
Error

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

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

- Puedan pilotar sin problemas su solución con un único agente unificado y acceder a un conjunto global de perímetros de servicio (cerca del usuario), con una interfaz de usuario centralizada y fácil de usar.
- Piloten los numerosos aspectos de la plataforma SSE con requisitos de implementación adicionales mínimos.
- Proporcionen la confianza de que su solución funcionará según lo previsto en la implementación completa con un esfuerzo de posventa mínimo.

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

Cómo los proveedores de SSE adecuados hacen que esto funcione:

Adoptar una plataforma SSE requiere replantear su arquitectura de seguridad, por lo que la elección de un proveedor de SSE no debe tomarse a la ligera. Por lo tanto, poder entender la verdadera capacidad del proveedor de SSE para trabajar en su entorno de producción es fundamental. La facilidad con la que se hace esto es representativa de la arquitectura de la plataforma.

Cuando tenga en cuenta a diferentes proveedores de SSE, comprenda los pasos necesarios para llevar a cabo una prueba piloto. Para los proveedores de SSE adecuados, el proceso debería ser encontrar una manera de reenviar el tráfico al perímetro del servicio SSE y que posteriormente, la propia nube del proveedor SSE se haga cargo. Los pasos que debe dar el administrador de SSE deben ser mínimos, aparte de establecer un mecanismo de reenvío, configurar las políticas básicas, la autenticación y los informes. Por supuesto, las configuraciones avanzadas de políticas tardarán más tiempo.

©2022 Zscaler, Inc. Todos los derechos reservados.

La prueba piloto debería abordar un conjunto de resultados comerciales e involucrar a miembros de varios equipos, incluidos seguridad, red y escritorio (por ejemplo, para la instalación de los agentes de punto final). No obstante, la participación activa de estos equipos debe ser mínima; al fin y al cabo, su objetivo es adquirir una solución SaaS. Los proveedores de SSE que exigen una gran implicación, sobre todo de los equipos de redes para manejar escenarios de enrutamiento complejos en una prueba piloto, deberían hacer saltar las alarmas.

Adopte un enfoque secuencial que refleje los objetivos de su empresa al planificar una prueba piloto de una solución SSE integral:

Todos los pasos anteriores deberían ser sencillos y realizables por parte del proveedor de SSE en poco tiempo (probablemente en cuestión de días) y sin necesidad de realizar grandes revisiones de enrutamiento o configuración. Mientras que el despliegue completo real requerirá más pasos, configuraciones de políticas avanzadas, tratar con varios tipos de aplicaciones y puntos finales, e integraciones y coexistencia con otros agentes/tecnologías, el proveedor de SSE debería ser capaz de mostrar el valor de la plataforma mediante una prueba piloto sencilla pero bien ejecutada.

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

- **Infraestructura global en la nube con una latencia mínima para el usuario final que opera 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.
- **Confianza cero para cada sesión de usuario**, desde la protección de aplicaciones privadas, aplicaciones públicas, e incluso las comunicaciones de carga de trabajo a carga de trabajo (si la prueba piloto lo requiere).
- **Protección frente a amenazas avanzadas y DLP avanzada mediante el análisis del tráfico cifrado**. La gestión de certificados puede requerir algunos pasos adicionales en la prueba piloto, pero demostrar la capacidad del proveedor para realizar la inspección SSL/TLS con una latencia mínima añadida es una excelente manera de diferenciar un proveedor de SSE de otro.
- **Opciones de implementación flexibles**. Aunque esto puede no formar 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 de los perímetros de servicio privado o CBI para los contratistas. El punto clave a verificar es que el proveedor de SSE pueda cumplir con los requisitos de aplicaciones y un personal distribuidos con sus modelos de implementación.

©2022 Zscaler, Inc. Todos los derechos reservados.

- **Experiencia óptima del usuario**. Esta métrica varía desde la facilidad de uso (por ejemplo, ¿cómo interactúa el usuario final con su agente?) hasta la experiencia general del usuario al acceder tanto a aplicaciones públicas como privadas a través de su plataforma SSE. El proveedor debería poder medir y diagnosticar un amplio conjunto de problemas de rendimiento del usuario final (wifi, ISP, CPU, etc.). Esta capacidad de medir/diagnosticar se debe integrar directamente en la plataforma SSE sin la necesidad de implementar nuevos agentes.
- **Integración de proveedores externos**. Aunque esto también puede no formar 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 debería 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, dada la escasez de habilidades y de personal que afronta el sector.

La ventaja de recurrir a un proveedor de seguridad SaaS es confiar al proveedor de SSE las tareas que normalmente realiza el personal interno: la prueba piloto debería proporcionar indicaciones claras de cuánto esfuerzo supondrá la implantación, la gestión y la actualización de la solución SSE.

⚠ ¿Qué debo tener en cuenta?

- En las pruebas piloto no se pueden probar todas las posibilidades y podrían surgir problemas imprevisibles durante un despliegue real.
- Compruebe que el proveedor de SSE está centrado en el cliente y muestra el deseo de superar cualquier problema de implantación que surja.
- Recuerde que probablemente no verá la escala en una prueba piloto y es posible que no vea los daños. Durante la prueba piloto, los proveedores de SSE pueden evitar problemas de red o de enrutamiento que les puedan poner en duda que pueden salir a la luz únicamente durante el despliegue. El proveedor de SSE correcto debe ser el que no depende de ninguna ruta de red para funcionar.
- Tenga en cuenta los gastos generales de gestión necesarios: ¿qué cubrirá usted y qué cubrirá el proveedor de SSE? Calcule el esfuerzo necesario para una implantación en producción y el mantenimiento continuo de la solución.
- Algunos proveedores de SSE pueden no ser verdaderos SaaS. Asegúrese de que la gestión de la solución SSE tenga el menor coste total de propiedad, que es especialmente importante dada la escasez de cualificación a la que se 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 adecuadamente en su entorno de producción y logra sus objetivos.

- Los proveedores de SSE que pueden probar sin problemas su solución auguran el éxito de despliegues integrales. Con el objetivo de un bajo coste total de propiedad, un único agente unificado, acceso a un conjunto global de perímetros de servicio y una interfaz de usuario centralizada y fácil de usar, todo esto hace que el mantenimiento continuo de la solución sea sencillo. Cualquier implantación a gran escala requerirá tiempo y esfuerzo, pero el objetivo debe ser trabajar con el proveedor que los minimice.
- La arquitectura y el diseño de un SSE deben facilitar la incorporación de funciones con unos requisitos mínimos de despliegue adicional (como agentes o máquinas virtuales adicionales). De este modo, los compradores pueden adoptar un enfoque gradual del SSE, sabiendo que el paso de una fase a otra no exigirá grandes esfuerzos.
- En última instancia, el objetivo es tener la confianza de que el proveedor de SSE realizará la implantación sin problemas en un entorno de producción y estará a su lado cuando surjan los problemas inevitables. Los proveedores que se centran en el cliente y con una arquitectura probada son los mejores indicios de que su inversión en seguridad y transformación de red será todo un éxito.

No tienen que creernos ciegamente

Los momentos que permiten a las empresas invertir fuertemente en un nuevo camino son muy escasos. Por eso, las empresas deben considerar un enfoque mesurado para brindar SSE. El alcance de SSE empresarial (compartido públicamente a través de https://trust.zscaler.com), destinado a todos los usuarios, servidores, dispositivos, etc. posibles, se describe en error n.º 2. A continuación se muestra cómo sus contemporáneos han abordado la adopción de SSE:

Referencia A:

El cliente implementó la plataforma Zscaler SSE para el control de confianza cero de:

- Acceso granular del usuario final a servicios privados
- Seguridad de Internet para los usuarios finales, incluidas inspección en línea y protección de datos
- Transformación de la red al eliminar por completo a los usuarios de la red
- Protección de cargas de trabajo, de Internet y del acceso privado
- Control de acceso de terceros limitado

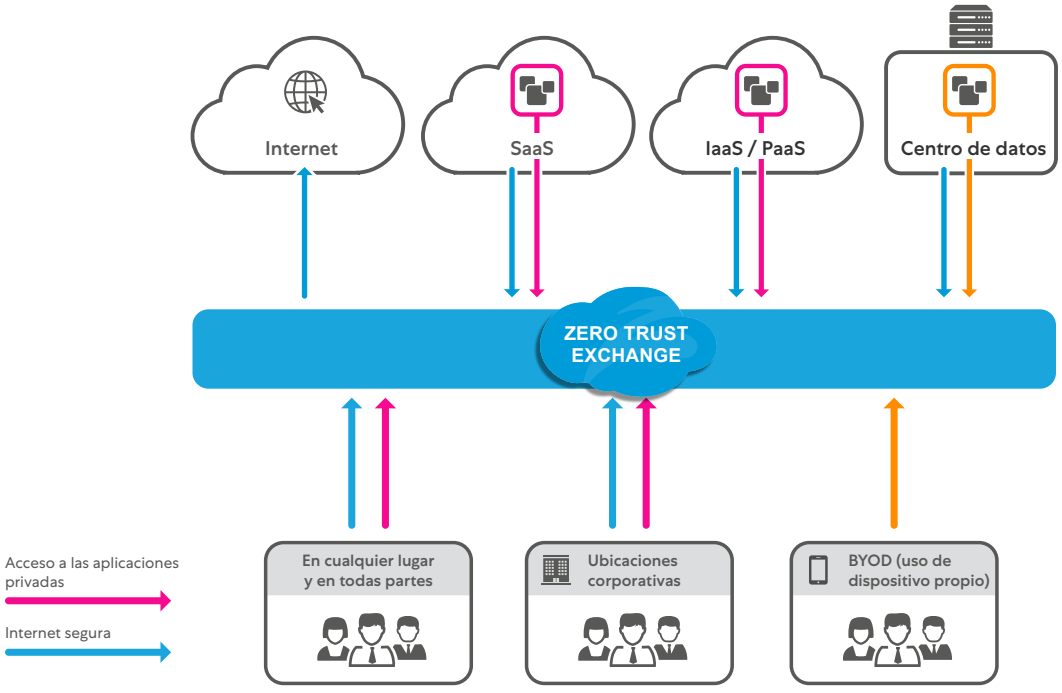

Figura 19: Representación de alto nivel de la conectividad implementada en la empresa con Zscaler

©2022 Zscaler, Inc. Todos los derechos reservados.

"En menos de cinco días, hicimos que, de forma sencilla, segura y rentable, 20 000 empleados pasasen a trabajar desde cualquier lugar reemplazando las VPN por la solución de acceso a la red de confianza cero de Zscaler".

Michael Alvmarken, director de Servicios de Ciberseguridad y Tecnología, Sandvik Group

"Aprovechar la infraestructura de la nube de Zscaler y las integraciones nativas con ZIA y ZPA nos proporcionó la mejor visión de los datos de los usuarios finales".

John Dawes, director de Arquitectura Empresarial, Reckitt Benckiser

"Al no retornar nuestro tráfico sino enviarlo directamente a través de Internet, esperamos poder reducir los costes en un 70 %".

Frederik Janssen, vicepresidente de Cartera de Infraestructura de TI Global, Siemens

Referencia B:

- El cliente desplegó la plataforma Zscaler SSE para tener:
- Visibilidad completa del acceso a todos los servicios de Internet (nube y otros)
- Control total en línea para restringir la pérdida de propiedad intelectual corporativa
- Supervisión de la experiencia digital del acceso de los usuarios cuando trabajan desde casa

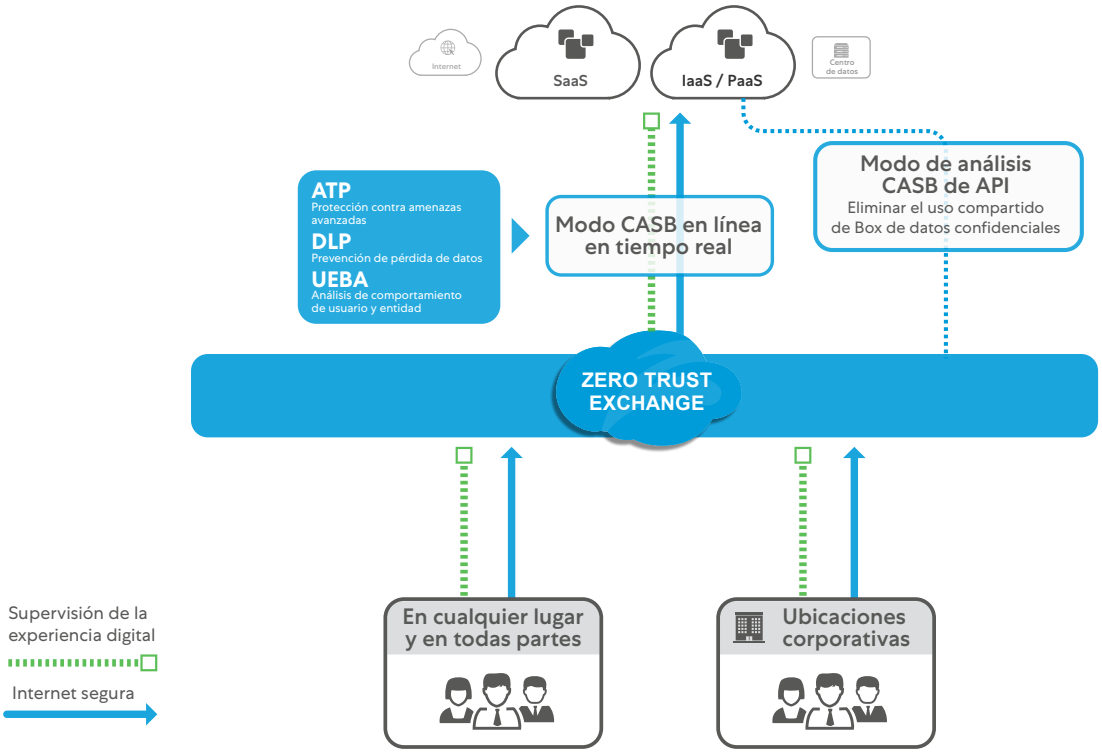

Figura 20: Ejemplo de inspección en línea y supervisión de la experiencia con Zscaler.

©2022 Zscaler, Inc. Todos los derechos reservados.

"Vemos Zscaler Digital Experience como un servicio fundamental para habilitar la experiencia de trabajar productivamente desde cualquier lugar. En el pasado, resolver el 25 % de los problemas de los usuarios ya era todo un logro. Ahora, ZDX es el punto de partida para resolver todos nuestros problemas relativos a la experiencia de usuario y podemos localizar la raíz del problema el 95 % de las veces".

Ed DeGrange, arquitecto principal de seguridad, Ciena

"Ya sea un problema comercial o de fraude, cualquier aspecto del sitio web o fraude interno, todo tiene un impacto financiero y es por ello que la seguridad debe formar parte del mismo".

Frederik Janssen, vicepresidente de Cartera de Infraestructura de TI Global, Siemens

"Con Zscaler Advanced Cloud Sandbox, no hay un trabajo intenso para TI, lo cual es fundamental, ya que el mercado actual de personal con talento es tan escaso que contratar personal es extremadamente complicado".

Mark Ferguson, CISO, Bombardier

Referencia C:

El cliente proporcionó una protección granular de los servicios no informáticos utilizando la plataforma Zscaler:

- Confianza cero a la tecnología operativa (OT), tanto empleados como terceros
- Tecnología operativa a carga de trabajo
- Nube a carga de trabajo

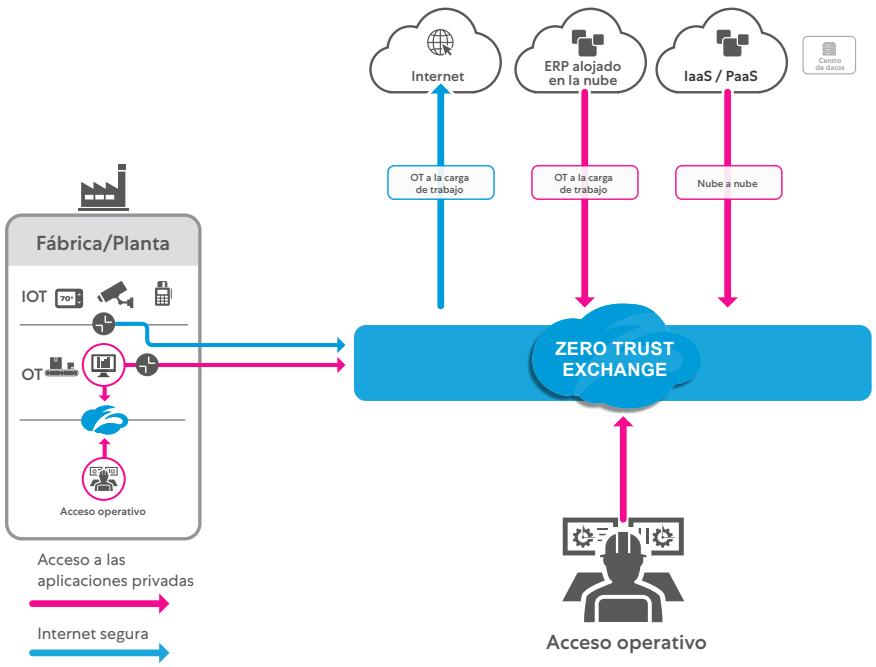

Figura 20: Ejemplo de inspección en línea y supervisión de la experiencia con Zscaler.

©2022 Zscaler, Inc. Todos los derechos reservados.

Principales conclusiones

- ☐ El proveedor de SSE debe ofrecer un SLA documentado basado en la pérdida o degradación del servicio.
- ☐ La solución SSE debe ofrecer el cumplimiento en todos los sitios: en línea, en todo el mundo 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 de confianza cero para todos los usuarios empresariales, cargas de trabajo y dispositivos autorizados a través de cualquier protocolo.
- ☐ La solución SSE debe prestar un servicio de forma independiente a través de 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 incluido).
- ☐ La solución SSE debe proporcionar varios controles de seguridad a través de una única arquitectura de análisis de memoria para obtener ventajas de escalabilidad únicas para el descifrado a escala.
- ☐ El proveedor de SSE debe proporcionar su solución gestionada de forma centralizada y desplegable en múltiples formas para abordar la ubicación del cliente, la región, la localidad y la personalización de la función.
- ☐ La solución SSE debe ampliarse para proporcionar protección para el acceso no gestionado de dispositivos propios, terceros y socios con el mismo nivel de control granular que los empleados.
- ☐ El proveedor de SSE debe optimizar la experiencia del usuario supervisando y diagnosticando los problemas de rendimiento de los servicios empresariales (Teams, Zoom, etc.).
- ☐ La solución SSE debe recopilar métricas de las rutas de aplicación, los puntos finales y las capas de red para identificar anomalías y proporcionar información a los equipos de soporte.
- ☐ El proveedor de SSE debe integrarse con los mejores actores del ecosistema (como CSP, SD-WAN, IAM, SOAR/SIEM, EDR, etc.), aportando un control y una seguridad completos y profundos a todo el panorama empresarial.
- ☐ La solución SSE debe integrarse con estos proveedores para proporcionar una orquestación que minimice la sobrecarga operativa.
- ☐ Los proveedores de SSE deben ser capaces de realizar una prueba piloto sin problemas para demostrar las funciones y ubicaciones que necesita la empresa en producción.
- ☐ La solución SSE debe poderse ampliar con facilidad sin necesidad de hardware o agentes adicionales, permitiendo a las empresas aumentar su uso de SSE mediante un enfoque gradual.

Para más información sobre SSE, visite Zscaler SSE 2022

Sobre los autores

Sanjit Ganguli (vicepresidente de Estrategia de Transformación / CTO de campo) y Nathan Howe (vicepresidente de Tecnologías Emergentes y 5G) tienen trayectorias profesionales que abarcan todo el mundo y empresas como Gartner, Nestlé, Riverbed y Verizon, aportan un liderazgo y una visión innovadora sobre la nube, la seguridad, la transformación y las tecnologías emergentes.

©2022 Zscaler, Inc. Todos los derechos reservados.