Documento técnico

Garantizar la integridad cibernética durante una desinversión o escisión parcial

Introducción

Durante las desinversiones, los responsables de TI tienen la doble responsabilidad de prepararse de forma segura para la separación sin perturbar las operaciones del vendedor (RemainCo) o de la entidad desinvertida (SpinCo). Como parte del Contrato de Servicios de Transición (TSA), el vendedor se compromete a proporcionar apoyo de TI hasta que SpinCo sea capaz de poner en marcha por completo sus operaciones o se logre una integración total con el comprador. Esto supone un reto único, ya que RemainCo tendrá que crear una vía de acceso segura a su entorno para SpinCo y los usuarios de su comprador.

El vendedor suele empezar a preparar la venta varios meses antes de poner la empresa en venta. Una vez establecido el alcance de la venta desde el punto de vista empresarial, el primer paso es que el vendedor comprenda el perímetro de la operación, incluidos los activos tecnológicos y las personas que se transferirán de SpinCo, así como los que se quedarán en RemainCo, lo que requerirá un TSA. Esto es fundamental para garantizar el éxito de la transacción salvaguardando los activos de TI.

Una vez finalizado el perímetro del acuerdo, el vendedor tiene que crear unos estados financieros pro forma que muestren los gastos de explotación y de capital autónomos para administrar la SpinCo como una empresa independiente. Por último, el vendedor tendrá que trabajar en un modelo de arquitectura provisional que proporcione acceso a la tecnología a los empleados de SpinCo de forma segura.

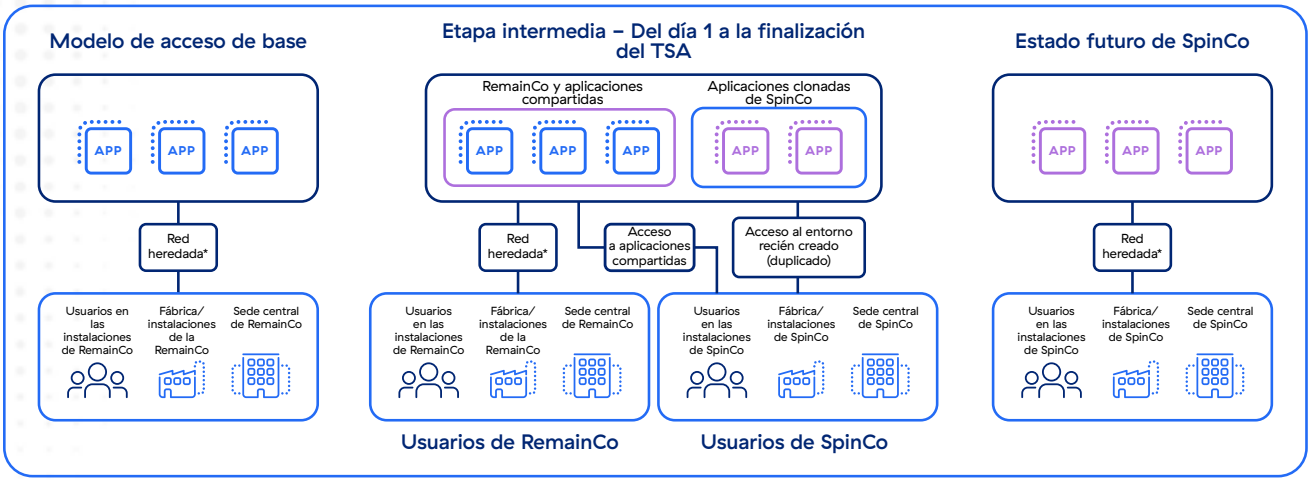
Modelo tradicional heredado

El modelo tradicional implica una estrategia de separación basada en la red con un par de opciones para que el vendedor proporcione acceso a las aplicaciones durante el período de TSA:

Descripción:	Posibles desventajas
Acceso compartido a los usuarios de SpinCo dentro del entorno actual del vendedor	El riesgo de infracción es muy alto debido al acceso de usuarios con una postura de seguridad desconocida
Adoptar un modelo híbrido; trasladar las aplicaciones de SpinCo dedicadas a un entorno independiente y proporcionar acceso a las aplicaciones compartidas dentro del entorno actual	El riesgo de infracción es muy alto debido al acceso de usuarios con una postura de seguridad desconocida. Además, el vendedor tendrá que realizar un esfuerzo importante al inicio para crear un entorno separado y segmentar el tráfico.
Migrar todas las aplicaciones a un entorno independiente; las aplicaciones dedicadas pueden trasladarse sin más, mientras que las compartidas pueden clonarse conservando únicamente los datos de la SpinCo.	Este modelo requerirá un conocimiento exhaustivo de todas las aplicaciones y datos que deben migrarse al nuevo entorno. Además, esto puede ser muy complicado al depender de múltiples flujos de trabajo (por ejemplo, aplicaciones, datos, alojamiento, redes)

Como ya se ha señalado, este modelo requiere meses de planificación previa, lo que lleva a las empresas a establecer plazos conservadores al tener en cuenta los problemas de la cadena de suministro para el hardware y los componentes de la infraestructura de red y establecer redes intermediarias seguras incluso antes de que comience el proceso de separación. Además, la red de RemainCo está expuesta a los usuarios de SpinCo, lo que presenta riesgos de desplazamiento lateral y de pérdida de datos.

Modelo tradicional: Red de SpinCo clonada con red intermediaria para el acceso entre entidades



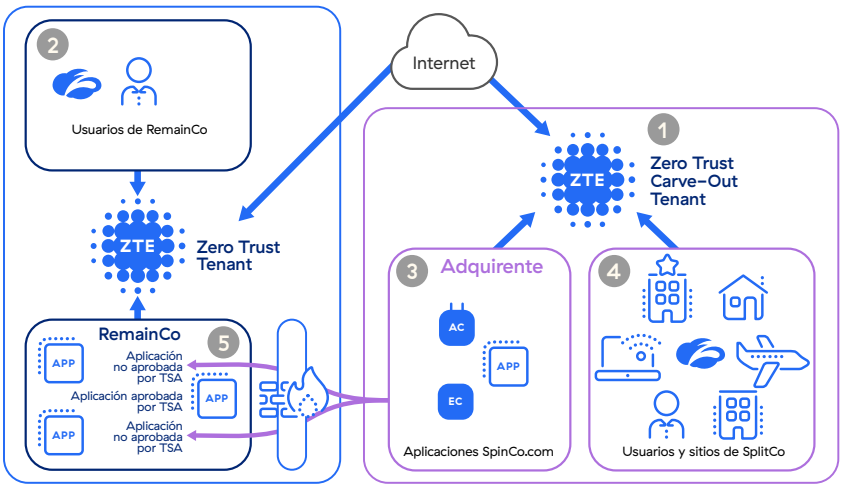
* El modelo heredado aprovecha MPLS, firewalls, balanceadores de carga, etc.

Por ejemplo, un gran minorista se dividió recientemente en dos entidades separadas, aprovechando las aplicaciones, la infraestructura y la red compartidas con un período de TSA de 2 años. Para garantizar el éxito, tendrán que crear entornos de TI separados, duplicar aplicaciones y desenredar una compleja maraña de redes. Esto supone un problema tanto para los responsables de TI como para los de la empresa, y puede suponer un riesgo para el valor del acuerdo.

Un modelo moderno respaldado por la plataforma en la nube de Zscaler

La plataforma Zero Trust basada en la nube de Zscaler elimina la necesidad de la segmentación de red heredada y los modelos basados en hardware para la conectividad. Nuestra plataforma le ayuda a lograr la segmentación a nivel de usuario y aplicación mediante la definición de políticas de acceso aplicadas por la nube Zscaler. Normalmente, en las desinversiones, se establece un usuario para permitir las conexiones a las aplicaciones compartidas en un entorno compartido. Partiendo de este punto, se pueden definir las políticas y los usuarios afectados y concederles acceso.

Modelo de Zscaler: Acceso de Zero Trust a SpinCo a través de un usuario de escisión



1. Establezca usuarios, IdP y dominios de SplitCo ZTE.
2. Identifique el perfil del entorno para definir usuarios, aplicaciones y políticas.
3. Redirija a los usuarios de Splitco a SplitCo ZTE.
4. Asigne aplicaciones Splitco a Splitco ZTE.
5. Establezca controles para las aplicaciones de TSA que queden rezagadas.

Recientemente, Zscaler trabajó con un gran conglomerado industrial en el que se creó un usuario independiente para la entidad empresarial desinvertida y se restringió el acceso a las aplicaciones compartidas mediante configuraciones de políticas. Al final, todos los usuarios de la empresa desinvertida migraron al nuevo usuario. Cuando se producen estas desinversiones, Zscaler puede dar soporte a usuarios en diferentes ubicaciones con diferentes personas que acceden tanto a entornos dedicados como compartidos.

Casos de uso comunes asistidos por Zscaler durante una desinversión

1. **Acceso a aplicaciones personalizadas:** Zscaler Private Access (ZPA) puede aprovecharse para asegurar el acceso a aplicaciones personalizadas alojadas en un centro de datos local o en una nube pública. Zscaler permite asegurar el acceso al entorno de un vendedor que aloja aplicaciones compartidas y dedicadas, así como al entorno de SpinCo y sus aplicaciones dedicadas. Todo esto puede lograrse rápidamente tanto para los usuarios remotos como para los de la oficina mediante un modelo basado en la configuración en la nube, sin necesidad de hardware adicional.

2. **Asegurar el tráfico de Internet:** Zscaler Internet Access (ZIA) puede aprovecharse para asegurar el acceso a aplicaciones SaaS y sitios web de Internet abiertos. Además, se pueden habilitar funciones avanzadas de protección contra amenazas con solo pulsar un botón para proteger a un vendedor de posibles ciberataques e infracciones durante el período de transición.

3. **Descubrimiento de aplicaciones:** Una vez instalado por completo, Zscaler puede mostrar las aplicaciones utilizadas por los usuarios de SpinCo para ayudar a los equipos de TI a entender qué aplicaciones son las que más se utilizan, así como sus patrones de uso, lo que ayuda a determinar las demandas de separación durante el período del TSA.

4. **Supervisión del rendimiento:** Zscaler Digital Experience (ZDX) reduce la carga de las operaciones de TI al proporcionar un panel único, el Zscaler ZTE Admin Portal, a través del cual los equipos de servicio de asistencia tanto del vendedor como de SpinCo pueden supervisar de cerca las interrupciones de la red y los problemas de rendimiento. ZDX libera tanto a los equipos de asistencia técnica del vendedor como a los de SpinCo de los arduos procesos de administración de incidencias y de identificación de los afectados por problemas concretos al proporcionar los datos de telemetría necesarios en los dos entornos.

Ventajas del modelo de Zscaler

Tiempo de creación de valor	• Finalice rápidamente el inventario de aplicaciones • Logre la conectividad entre usuarios y aplicaciones en semanas • Disminuya la duración del TSA
Sencillez	• Elimine la TI de la ruta crítica para la preparación del Día 1 • Aproveche un modelo de conectividad basado totalmente en la nube • Asegure la ruta de acceso y el tráfico de Internet con una solución de confianza cero
Finanzas	• Menores costos de separación únicos y recurrentes • Reduzca los costos del TSA y los activos bloqueados/deuda técnica • Disminuya el costo de preparación de TI permitiendo la transferibilidad de la plataforma Zscaler
Integridad	• Minimice el riesgo de pérdida de datos • Reduzca las amenazas internas y el acceso no autorizado de terceros • Permita controles auditables para cumplir con la preparación del Día 1

Conclusión

En las desinversiones, la separación de las TI suele verse consumida por complicaciones y problemas a la hora de proporcionar un acceso seguro a los empleados en el momento adecuado para que sean productivos. Además, los modelos tradicionales son propensos al riesgo cibernético debido a la exposición entre las dos redes. Zscaler desempeña un papel fundamental a la hora de permitir que los usuarios accedan de forma segura a las aplicaciones claves como parte del perímetro del acuerdo, tanto si se trata de una gran separación a nivel empresarial como de la venta de activos más pequeños. Zscaler reduce significativamente el riesgo cibernético a la vez que simplifica el proceso de separación.

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes contra los ciberataques y la pérdida de datos al conectar de manera segura a los usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos a nivel mundial, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com.mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com.mx