Documento técnico

Garantizar la integridad cibernética durante una desinversión o disociación

Introducción

Durante las desinversiones, los líderes de TI tienen la tarea doble de prepararse de manera segura para la separación sin interrumpir las operaciones del vendedor (RemainCo) o la entidad desinvertida (SpinCo). Como parte del Acuerdo de Servicio de Transición (TSA), el vendedor acepta brindar soporte técnico de TI hasta que SpinCo pueda respaldar por completo sus operaciones o se logre una integración completa con el comprador. Esto supone un desafío único en el que RemainCo tendrá que crear una ruta de acceso segura a su entorno para SpinCo y los usuarios de sus compradores.

El vendedor generalmente comienza a prepararse para la venta varios meses antes de poner el negocio en venta. Una vez que se ha establecido el alcance de la venta desde una perspectiva comercial, el primer paso es que el vendedor comprenda el perímetro del acuerdo, incluidos los activos tecnológicos y las personas que se traspasarán de SpinCo, así como los que permanecerán con el RemainCo y que, por tanto, requieren TSA. Esto es fundamental para garantizar el éxito de la transacción mediante la protección de los activos de TI.

Una vez finalizado el perímetro del acuerdo, el vendedor tiene que crear estados financieros proforma que muestren los gastos operativos y de capital independientes para operar SpinCo como un negocio independiente. Finalmente, el vendedor tendrá que trabajar en un enfoque de arquitectura provisional que proporcione acceso a la tecnología a los empleados de SpinCo de forma segura.

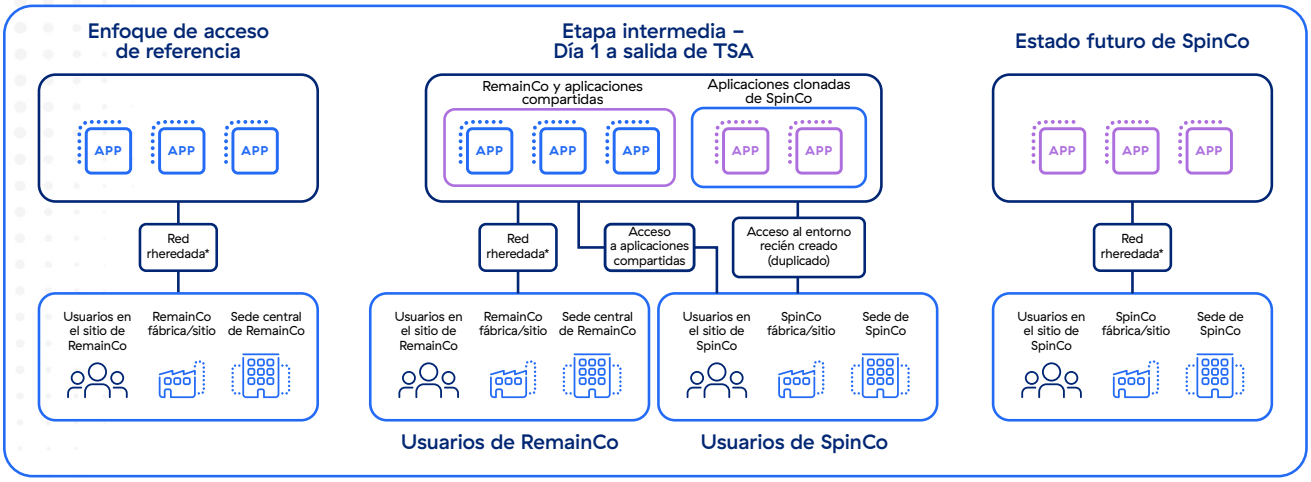
Enfoque de legado tradicional

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

Descripción	Posibles inconvenientes
Acceso compartido para los usuarios de SpinCo dentro del entorno actual del vendedor	El riesgo de una infracción es muy alto debido al acceso de usuarios con una postura de seguridad desconocida.
Siga un enfoque híbrido; mueva las aplicaciones dedicadas de SpinCo a un entorno separado y proporcione acceso a las aplicaciones compartidas dentro del entorno actual.	El riesgo de una infracción es muy alto debido al acceso de usuarios con una postura de seguridad desconocida. Además, se requerirá un esfuerzo inicial significativo para que el vendedor cree un entorno separado y segmente el tráfico.
Migre todas las aplicaciones a un entorno separado; las aplicaciones dedicadas se pueden mover tal como están, mientras que las aplicaciones compartidas se pueden clonar y solo se conservan los datos de SpinCo.	Este enfoque requerirá una comprensión profunda de todas las aplicaciones y datos que deben migrarse al nuevo entorno. Además, esto puede ser muy complicado por la dependencia de múltiples flujos de trabajo (p. ej., aplicaciones, datos, alojamiento, redes).

Como se ha señalado anteriormente, este enfoque requiere meses de planificación inicial, lo que lleva a las empresas a establecer plazos conservadores teniendo en cuenta los problemas de la cadena de suministro para los componentes de infraestructura de red y hardware, así como estableciendo redes intermedias seguras incluso antes de que comience el proceso de separación. Además, la red RemainCo está expuesta a los usuarios de SpinCo, lo que presenta riesgos de movimiento lateral y pérdida de datos.

Enfoque tradicional: red clonada de SpinCo con red intermediaria para acceso entre entidades



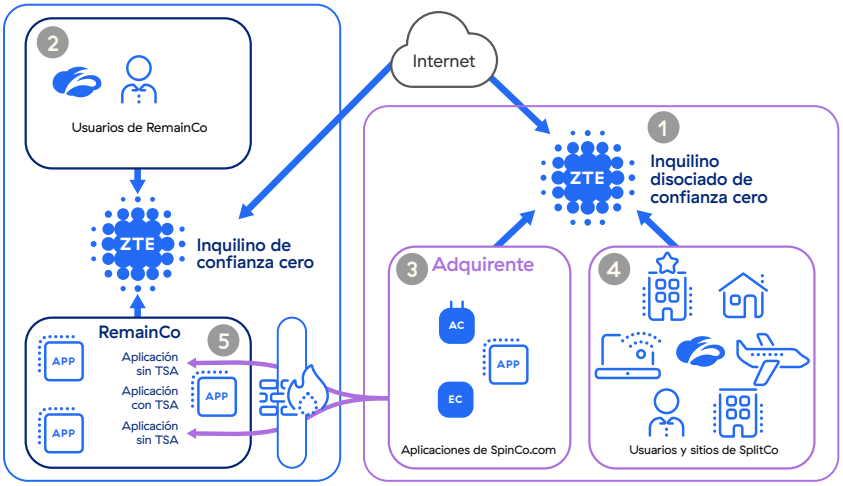
*El enfoque heredado aprovecha MPLS, cortafuegos, balanceadores de carga, etc.

Por ejemplo, un gran minorista se dividió recientemente en dos entidades separadas, y aprovechó las aplicaciones, la infraestructura y la red compartidas con un período de TSA de 2 años. Para garantizar el éxito, deberán crear entornos de TI separados, duplicar aplicaciones y desenredar una compleja red de redes. Esto supone un gran desafío para los líderes empresariales y de TI por igual, y puede resultar un riesgo para el valor del acuerdo.

Un enfoque moderno respaldado por la plataforma en la nube Zscaler

La plataforma de confianza cero basada en la nube de Zscaler elimina la necesidad de segmentación de red heredada y enfoques de conectividad basados en hardware. Nuestra plataforma le ayuda a lograr la segmentación a nivel de usuario y aplicación mediante la definición de políticas de acceso que aplica la nube Zscaler. Por lo general, en las desinversiones se activa un usuario para habilitar las conexiones a aplicaciones compartidas en un entorno compartido. A partir de ahí, se pueden definir políticas y usuarios afectados y otorgar acceso.

Enfoque de Zscaler: acceso de confianza cero a SpinCo a través de un usuario de disociación



1. Establezca usuario, IDP y dominios de ZTE de Splitco (la nueva empresa)
2. Perfile entornos para definir usuarios, aplicaciones y políticas
3. Redirija a los usuarios de Splitco al ZTE de Splitco
4. Asigne las aplicaciones de Splitco al ZTE de Splitco
5. Establezca controles para las aplicaciones TSA que quedan rezagadas

Recientemente, Zscaler trabajó con un gran conglomerado industrial en el que se creó un usuario separado para la entidad comercial desinvertida y se restringió el acceso a las aplicaciones compartidas mediante las configuraciones de políticas. Al final, todos los usuarios comerciales desinvertidos se migraron al nuevo usuario. Cuando se dan estas desinversiones, Zscaler puede admitir usuarios en diferentes ubicaciones con diferentes personas que acceden a entornos dedicados y compartidos.

Casos de uso comunes que contempla Zscaler durante una desinversión

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

2. **Protección del tráfico de Internet:** Zscaler Internet Access (ZIA) se puede aprovechar para proteger el acceso a aplicaciones SaaS y sitios web abiertos de Internet. Además, las funciones avanzadas de protección contra amenazas se pueden habilitar haciendo clic en un botón para proteger a un vendedor de posibles ciberataques e infracciones durante el período de transición.

3. **Detección de aplicaciones:** Zscaler, una vez completamente implementado, puede descubrir las aplicaciones utilizadas por los usuarios de SpinCo para ayudar a los equipos de TI a comprender qué aplicaciones se usan más, así como sus patrones de uso, lo que ayuda a determinar las exigencias de separación durante el período TSA.

4. **Supervisión del rendimiento:** Zscaler Digital Experience (ZDX) reduce la carga de las operaciones de TI al proporcionar un panel único, el portal de administración Zscaler ZTE, a través del cual los equipos de soporte técnico del vendedor y SpinCo pueden supervisar de cerca las interrupciones de la red y los problemas de rendimiento. ZDX libera a los equipos de soporte técnico tanto del vendedor como de SpinCo de los arduos procesos de gestión de tickets e identificación de quienes sufren problemas particulares al proporcionar los datos de telemetría necesarios en los dos entornos.

Ventajas del enfoque Zscaler

 **Tiempo para obtención de valor**	• Finalice rápidamente el inventario de aplicaciones • Logre la conectividad entre el usuario y la aplicación en semanas • Disminuya la duración del TSA
 **Sencillez**	• Elimine la TI de la ruta crítica para la preparación del día 1 • Aproveche un enfoque de conectividad 100 % basado en la nube • Asegure la ruta de acceso y el tráfico de Internet con una solución de confianza cero
 **Aspectos financieros**	• Costes de separación únicos y recurrentes más bajos • Reduzca los costes de TSA y los activos varados/deuda técnica • Reduzca el coste de soporte de TI al permitir la transferencia de la plataforma Zscaler
 **Integridad**	• Minimice el riesgo de pérdida de datos • Reduzca las amenazas internas y el acceso no autorizado de terceros • Habilite controles auditables para cumplir el día 1

Conclusión

En las desinversiones, la separación de TI a menudo se ve plagada de complicaciones y desafíos a la hora de brindar acceso seguro a los empleados en el momento adecuado para que sean productivos. Además, los enfoques tradicionales son propensos al riesgo cibernético debido a la exposición entre las dos redes. Zscaler desempeña un papel fundamental al permitir que los usuarios accedan de forma segura a aplicaciones clave como parte del perímetro del acuerdo, ya sea participando en una gran separación a nivel empresarial o vendiendo activos más pequeños. Zscaler reduce significativamente el riesgo cibernético al tiempo 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 de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

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