Livre blanc

Garantir la cyber-intégrité tout au long d'une cession ou d'un carve-out

Introduction

Lors des cessions, les responsables informatiques sont chargés d'une double mission : préparer de manière sécurisée la séparation sans perturber les opérations du vendeur (RemainCo) ou de l'entité cédée (SplitCo). Dans le cadre du contrat de service transitoire (TSA), le vendeur accepte de fournir un soutien informatique de base jusqu'à ce que la SplitCo soit en mesure de reprendre complètement ses activités ou jusqu'à ce que l'intégration complète avec l'acheteur soit accomplie. Cela constitue un défi unique, car la RemainCo devra créer un chemin d'accès sécurisé à son environnement à l'intention de la SplitCo et des utilisateurs de l'acheteur.

Le vendeur se prépare généralement plusieurs mois avant de mettre l'entreprise en vente. Une fois que le cadre de la vente a été établi du point de vue de l'entreprise, la première étape pour le vendeur est d'appréhender le cadre de la transaction, notamment les actifs technologiques et les personnes qui seront transférés de la SplitCo ainsi que ceux qui resteront avec la RemainCo, d'où la nécessité d'un TSA. Ceci est essentiel pour assurer le succès de la transaction en protégeant les actifs informatiques.

Une fois le cadre de la transaction établi, le vendeur doit créer des états financiers pro forma affichant les dépenses d'exploitation et d'investissement autonomes pour gérer la SplitCo comme une entreprise indépendante. Enfin, le vendeur devra élaborer une approche d'architecture provisoire qui fournira un accès technologique aux employés de la SplitCo de manière sécurisée.

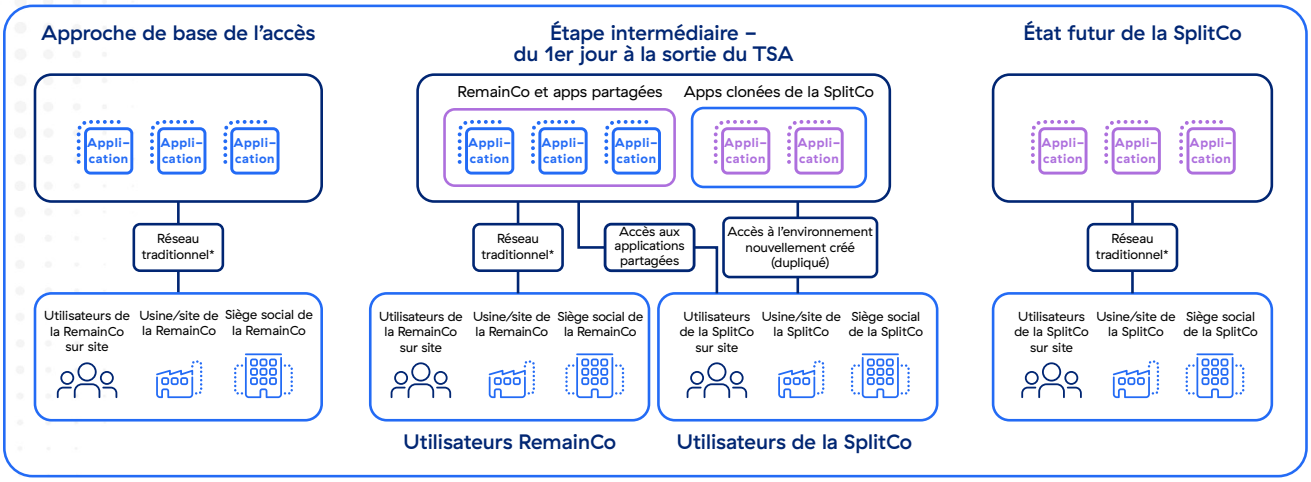
Approche traditionnelle

L'approche traditionnelle implique une stratégie de séparation basée sur le réseau avec quelques options permettant au vendeur de fournir un accès aux applications pendant la période du TSA :

Description	Inconvénients potentiels
Accès partagé aux utilisateurs de la SplitCo dans l'environnement actuel du vendeur	Le risque de violation est extrêmement élevé en raison de l'accès d'utilisateurs dont la posture de sécurité est inconnue.
Suivre une approche hybride ; déplacer les applications dédiées de la SplitCo dans un environnement séparé et fournir un accès aux applications partagées au sein de l'environnement existant.	Le risque de violation est très élevé en raison de l'accès d'utilisateurs dont la posture de sécurité est inconnue. De plus, le vendeur devra fournir un travail initial considérable pour créer un environnement séparé et segmenter le trafic.
Migrer toutes les applications vers un environnement distinct ; les applications dédiées peuvent être déplacées telles quelles, tandis que les applications partagées peuvent être clonées avec les seules données conservées de la SplitCo.	Cette approche exigera une compréhension exhaustive de toutes les applications et données qui doivent être migrées vers le nouvel environnement. Qui plus est, cette approche peut s'avérer très compliquée, car elle dépend de plusieurs flux de travail (par exemple, les applications, les données, l'hébergement, les réseaux).

Comme mentionné ci-dessus, cette approche exige des mois de planification en amont, ce qui conduit les entreprises à établir des calendriers prudents en tenant compte des problèmes de chaîne d'approvisionnement pour les composants de l'infrastructure matérielle et de réseau et à mettre en place des réseaux intermédiaires sécurisés avant même le début du processus de séparation. De plus, le réseau de la RemainCo est exposé aux utilisateurs de la SplitCo, ce qui comporte des risques de déplacement latéral et de perte de données.

Approche traditionnelle : réseau de la SplitCo cloné avec un réseau intermédiaire pour l'accès inter-entités



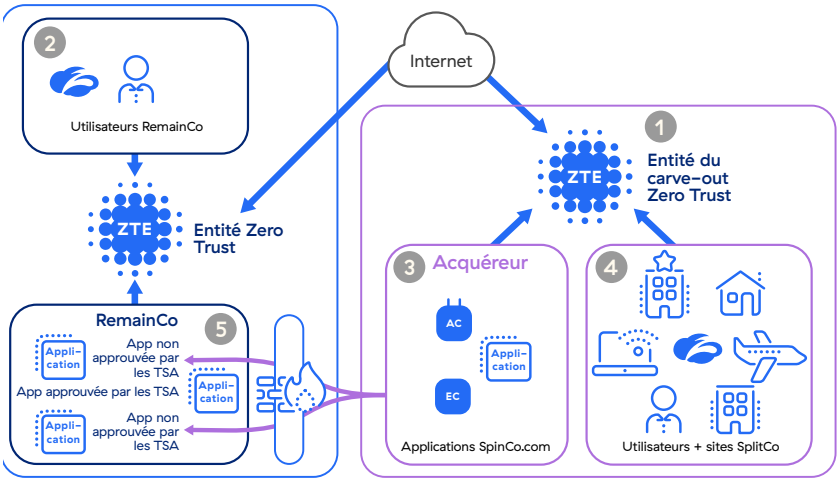
*L'approche traditionnelle utilise des MPLS, des pare-feux, des équilibreurs de charge,

Prenons l'exemple d'un grand détaillant qui s'est récemment scindé en deux entités distinctes, exploitant des applications, une infrastructure et un réseau partagés avec une période de TSA de deux ans. Afin d'assurer la réussite, il devra créer des environnements informatiques distincts, dupliquer les applications et démêler un tissu complexe de réseaux. Il s'agit d'un défi de taille pour les responsables informatiques et les chefs d'entreprise, qui peut s'avérer risqué pour la valorisation de la transaction.

Une approche moderne soutenue par la plateforme cloud de Zscaler

La plateforme Zero Trust de Zscaler, basée sur le cloud, dispense de recourir à la segmentation des réseaux traditionnels et à des approches de la connectivité basées sur le matériel. Notre plateforme vous aide à réaliser une segmentation au niveau de l'utilisateur et de l'application en définissant des politiques d'accès appliquées par le cloud de Zscaler. Généralement, dans le cadre de cessions, une entité est créée pour permettre les connexions aux applications partagées dans un environnement partagé. À partir de là, les politiques et les utilisateurs impliqués peuvent être définis et l'accès accordé.

Approche de Zscaler : Zero Trust Accès à la SplitCo par le biais d'une entité scindée



1. Établir l'entité, le fournisseur d'identité (IDP) et les domaines ZTE de la SplitCo
2. Établir le profil de l'environnement pour définir les utilisateurs, les applications et les politiques
3. Rediriger les utilisateurs de la SplitCo vers le ZTE de la SplitCo
4. Assigner des applications de la société scindée au ZTE de la société scindée
5. Établir des contrôles pour les applications TSA restantes

Zscaler a récemment travaillé avec un grand conglomérat industriel qui a créé une entité distincte pour l'entité commerciale cédée et a restreint l'accès aux applications partagées à l'aide de configurations de politiques. À la fin du processus, tous les utilisateurs de l'entreprise cédée ont été migrés vers la nouvelle entité. Dans le cadre de ces cessions, Zscaler peut assister les utilisateurs de différents sites avec différents personas qui accèdent à la fois aux environnements dédiés et partagés.

Cas d'utilisation courants pris en charge par Zscaler dans le cadre d'une cession

1. **Accès aux applications personnalisées :** Zscaler Private Access (ZPA) peut sécuriser l'accès aux applications personnalisées hébergées dans un centre de données sur site ou dans un cloud public. Zscaler permet de sécuriser l'accès à l'environnement d'un vendeur hébergeant des applications partagées et dédiées, ainsi qu'à l'environnement de la SplitCo et à ses applications dédiées. Le tout peut être effectué rapidement, tant pour les utilisateurs distants que pour ceux qui travaillent dans les bureaux, par le biais d'une approche basée sur la configuration du cloud, sans nécessiter de matériel supplémentaire.

2. **Sécurisation du trafic Internet :** Zscaler Internet Access (ZIA) peut sécuriser l'accès aux applications SaaS et aux sites Internet ouverts. De plus, les fonctions de protection contre les menaces avancées peuvent être activées d'un simple clic pour protéger un vendeur contre les cyberattaques et les violations potentielles pendant la période de transition.

3. **Découverte des applications :** une fois entièrement déployé, Zscaler peut découvrir les applications qu'utilisent les utilisateurs de la SplitCo pour permettre aux équipes informatiques de comprendre quelles sont les applications les plus utilisées ainsi que leurs schémas d'utilisation, ce qui permet de déterminer les demandes de séparation pendant la période TSA.

4. **Surveillance des performances :** Zscaler Digital Experience (ZDX) réduit la charge qui pèse sur les opérations informatiques en regroupant les informations sur un seul écran – le portail d'administration Zscaler ZTE – grâce auquel les équipes d'assistance du vendeur et de la SplitCo peuvent étroitement surveiller les pannes de réseau et les problèmes de performance. ZDX soulage les équipes de helpdesk du vendeur et de la SplitCo des processus fastidieux de traitement des tickets et d'identification des victimes de problèmes particuliers en fournissant les données télémétriques indispensables à travers les deux environnements.

Avantages de l'approche Zscaler

Délai de rentabilisation	• Finaliser rapidement l'inventaire des applications • Assurer la connectivité utilisateur–application en quelques semaines • Diminuer la durée du TSA
Simplicité	• Soustraire l'informatique du chemin critique de la préparation du premier jour • Exploiter une approche de la connectivité entièrement basée sur le cloud • Sécuriser le chemin d'accès et le trafic internet avec une solution Zero Trust
Finances	• Réduire les coûts de séparation ponctuels et récurrents • Réduire les coûts du TSA et les actifs immobilisés/la dette technique • Diminuer les coûts liés à la mise en place de l'informatique en garantissant la transférabilité de la plateforme Zscaler
Intégrité	• Minimiser le risque de perte de données • Réduire les menaces internes et les accès non autorisés de tiers • Permettre des contrôles auditables pour répondre aux exigences du premier jour

Conclusion

Dans le cadre des cessions, la séparation informatique est souvent compromise par des enchevêtrements et des difficultés à fournir un accès sécurisé aux employés en temps opportun pour assurer leur productivité. En outre, les approches traditionnelles sont exposées au cyber–risque en raison de l'exposition entre les deux réseaux. Zscaler joue un rôle central en permettant aux utilisateurs d'accéder en toute sécurité aux applications stratégiques dans le cadre du périmètre de la transaction, qu'il s'agisse d'une séparation au niveau d'une grande entreprise ou de la vente d'actifs plus petits. Zscaler réduit considérablement le cyber–risque tout en simplifiant le processus de séparation.

zscaler™ | Experience your world, secured.™

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr