White paper

Garantire l'integrità informatica nel corso di una cessione o di un carve-out

Introduzione

Durante le cessioni, i responsabili IT hanno il duplice compito di preparare le aziende ad affrontare in modo sicuro la separazione senza interrompere le operazioni del cedente (RemainCo) o dell'entità ceduta (SplitCo). Nell'ambito del Transition Service Agreement (TSA, o accordo sui servizi di transizione), il cedente si impegna a fornire assistenza informatica fino a quando la SplitCo non sarà in grado di avviare completamente in modo autonomo le proprie operazioni o fin quando non verrà realizzata un'integrazione completa con l'acquirente. Si tratta di una sfida molto delicata, in quanto la RemainCo dovrà creare un percorso di accesso sicuro al proprio ambiente per la SplitCo e gli utenti dell'acquirente.

In genere, il cedente inizia a prepararsi per la cessione diversi mesi prima di mettere in vendita l'azienda. Una volta stabilito cosa verrà ceduto dal punto di vista aziendale, il primo passo per il cedente consiste nel comprendere il perimetro dell'operazione, che include il personale e gli asset tecnologici che saranno trasferiti alla SplitCo e quelli che rimarranno invece nella RemainCo, richiedendo quindi un TSA. È un passaggio fondamentale per garantire il successo della transazione tutelando le risorse informatiche.

Dopo aver definito il perimetro interessato dall'accordo, il cedente deve creare dei bilanci pro forma che mostrino le spese di gestione e in conto capitale specifiche per l'amministrazione della SplitCo come azienda indipendente. Infine, dovrà lavorare su un'architettura provvisoria che consenta ai dipendenti della SplitCo di accedere in modo sicuro alla tecnologia.

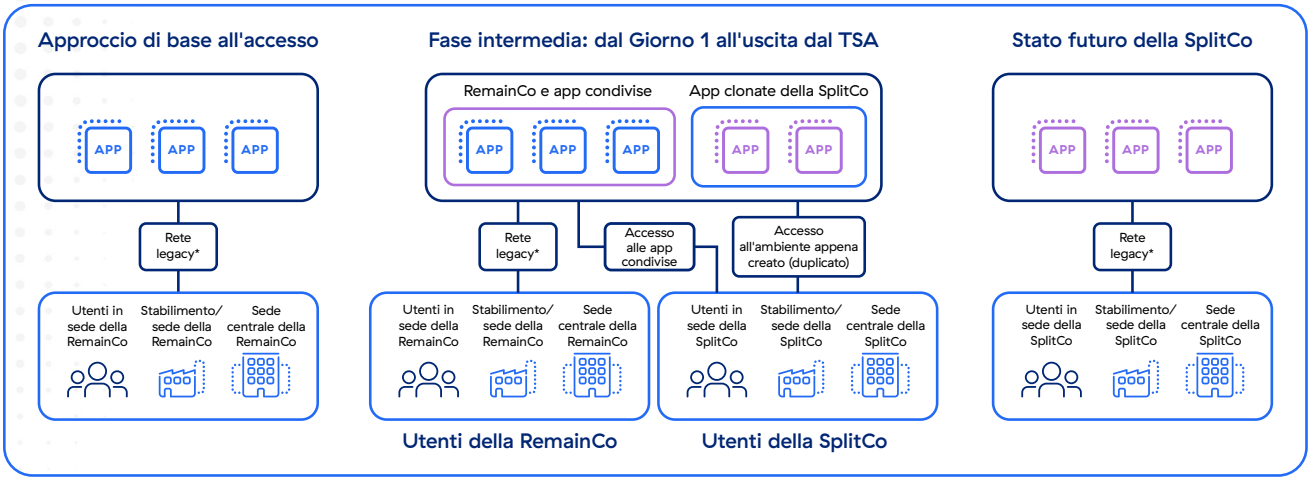
L'approccio tradizionale

L'approccio tradizionale prevede una strategia di separazione basata sulla rete, dove il cedente ha a disposizione alcune opzione per fornire l'accesso alle applicazioni durante il periodo coperto dal TSA:

Descrizione	Potenziali svantaggi
Accesso condiviso agli utenti della SplitCo all'interno dell'ambiente esistente del cedente.	Il rischio di violazione è molto elevato, a causa dell'accesso di utenti con un profilo di sicurezza non definito.
Seguire un approccio ibrido, spostando le applicazioni dedicate della SplitCo in un ambiente separato e fornendo l'accesso alle applicazioni condivise all'interno dell'ambiente esistente.	Il rischio di violazione è molto elevato, a causa dell'accesso da parte di utenti con un profilo di sicurezza non definito. Inoltre, il cedente dovrà compiere un notevole sforzo iniziale per generare un ambiente separato e segmentare il traffico.
Spostare tutte le applicazioni dedicate in un ambiente separato così come sono, mentre le applicazioni condivise possono essere clonate preservando solo i dati della SplitCo.	Questo approccio richiede una conoscenza approfondita di tutte le applicazioni e dei dati che devono essere spostati nel nuovo ambiente. Inoltre, questa strategia può essere molto complicata e dipendere da più flussi di lavoro (come applicazioni, dati, hosting, reti).

Come già detto, questo approccio richiede mesi di pianificazione anticipata e porta le aziende a definire tempistiche molto prudenti, tenendo conto dei problemi legati alla fornitura di componenti per hardware e infrastruttura di rete e della creazione di reti intermedie sicure già prima che inizi il processo di separazione. Inoltre, la rete della RemainCo è esposta agli utenti della SplitCo, con il rischio che si verifichino movimenti laterali e perdite di dati.

Approccio tradizionale: rete clonata della SplitCo, con una rete intermedia per l'accesso reciproco tra le diverse entità.



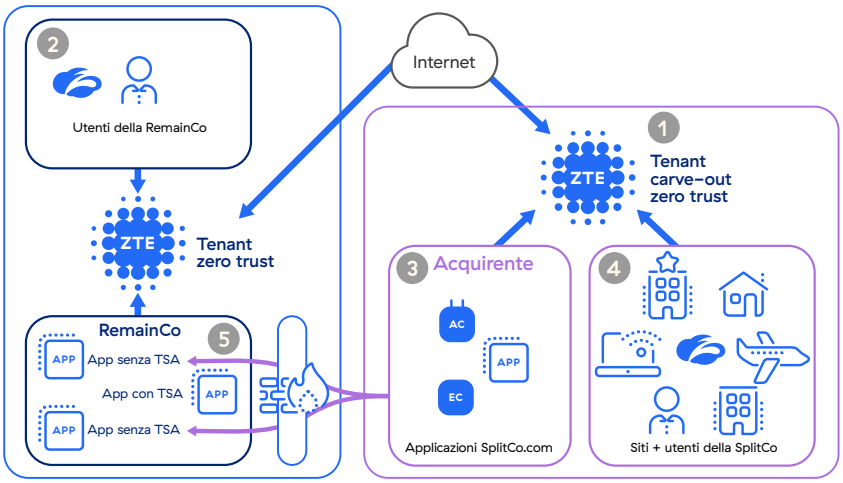
*L'approccio legacy sfrutta MPLS, firewall, bilanciatori di carico, ecc.

Ad esempio, un grande rivenditore si è recentemente diviso in due entità separate, sfruttando applicazioni, infrastrutture e reti condivise con un periodo coperto da TSA di 2 anni. Per garantire il successo dell'operazione, dovrà creare ambienti IT separati, duplicare le applicazioni e districarsi in una complessa trama di reti diverse. Si tratta di una sfida molto impegnativa sia per l'IT che per i leader aziendali, e può influire negativamente sul valore dell'accordo.

Un approccio moderno, supportato dalla piattaforma cloud di Zscaler

La piattaforma zero trust con base cloud di Zscaler elimina la necessità di effettuare la segmentazione della rete e di ricorrere ad approcci alla connettività basati su hardware. La nostra piattaforma aiuta a ottenere una segmentazione a livello di utente e di applicazione definendo policy di accesso che verranno applicate dal cloud di Zscaler. In genere, durante le cessioni, viene creato un tenant per consentire la connessione alle applicazioni condivise ospitate in un ambiente condiviso. Da qui è possibile definire le policy e gli utenti che ne saranno interessati e concedere l'accesso.

Approccio di Zscaler: accesso zero trust alla SplitCo attraverso un tenant carveout



1. Per la SplitCo vengono generati tenant di ZTE, IdP e domini
2. Viene eseguita una profilazione dell'ambiente, per definire utenti, applicazioni e policy
3. Gli utenti della SplitCo vengono reindirizzati a ZTE della SplitCo
4. Le applicazioni della SplitCo vengono assegnate a ZTE della SplitCo
5. Vengono istituiti controlli per le applicazioni rimanenti soggette a TSA

Recentemente, Zscaler ha collaborato con un grande conglomerato industriale in cui è stato creato un tenant separato per l'entità aziendale ceduta e l'accesso alle applicazioni condivise è stato limitato attraverso le configurazioni di policy. Dopodiché, tutti gli utenti dell'azienda ceduta sono stati spostati sul nuovo tenant. Quando si verificano queste tipologie di cessioni, Zscaler è in grado di supportare gli utenti di sedi diverse con svariate entità che accedono sia agli ambienti dedicati che condivisi.

I più comuni casi d'uso supportati da Zscaler durante una cessione

1. **Accesso ad applicazioni personalizzate:** la soluzione Zscaler Private Access (ZPA) può essere utilizzata per proteggere l'accesso ad applicazioni personalizzate ospitate in un data center on-premise o in un cloud pubblico. Zscaler offre la possibilità di proteggere l'accesso all'ambiente del cedente, che ospita applicazioni condivise e dedicate, nonché all'ambiente della SplitCo e alle sue applicazioni dedicate. Tutto questo può essere ottenuto rapidamente, sia per gli utenti in remoto che per quelli in ufficio, grazie a un approccio basato sulla configurazione cloud, senza la necessità di ricorrere ad hardware aggiuntivo.

2. **Protezione del traffico Internet:** la soluzione Zscaler Internet Access (ZIA) può essere sfruttata per proteggere l'accesso alle applicazioni SaaS e ai siti web sulla rete Internet aperta. Inoltre, le funzioni di protezione dalle minacce avanzate possono essere attivate con un semplice clic, per proteggere il cedente da potenziali attacchi informatici e violazioni durante il periodo di transizione.

3. **Rilevamento delle applicazioni:** una volta completata la distribuzione, Zscaler è in grado di rilevare le applicazioni utilizzate dagli utenti della SplitCo per aiutare i team IT a capire quali sono quelle più usate e quali sono i relativi schemi di utilizzo, aiutando con le esigenze di separazione durante il periodo coperto da TSA.

4. **Monitoraggio delle prestazioni:** Zscaler Digital Experience (ZDX) riduce la gravosità delle operazioni IT fornendo un pannello di controllo unificato, Zscaler ZTE Admin Portal, attraverso il quale i team di assistenza tecnica del cedente e della SplitCo possono monitorare da vicino le interruzioni di rete e i problemi prestazionali. ZDX consente ai team di assistenza del cedente e della SplitCo di evitare farraginosi processi di gestione dei ticket e di identificazione dei soggetti che riscontrano particolari problemi fornendo dati telemetrici fondamentali a entrambi gli ambienti.

I vantaggi dell'approccio di Zscaler

 **Time to value**	• Finalizzazione rapida dell'inventario delle applicazioni • Connettività utente–app ottenuta in poche settimane • Riduzione della durata del TSA
 **Semplicità**	• Eliminazione dell'IT dal percorso critico per consentire rapidità sin dal primo giorno • Approccio alla connettività basato al 100% sul cloud • Percorso di accesso e traffico Internet protetti con una soluzione zero trust
 **Dati finanziari**	• Riduzione dei costi una tantum e ricorrenti della separazione • Abbattimento dei costi associati a TSA e stranded asset/debito tecnico • Riduzione dei costi per la ripresa del controllo da parte dell'IT grazie alla trasferibilità della piattaforma Zscaler
 **Integrità**	• Riduzione al minimo del rischio legato alla perdita di dati • Riduzione delle minacce interne e degli accessi non autorizzati da parte di terzi • Attivazione di controlli verificabili per soddisfare i requisiti di conformità dal Giorno 1

Conclusione

Durante le cessioni, la separazione delle tecnologie informatiche viene spesso condizionata da numerose problematiche e difficoltà relative alla necessità di fornire un accesso sicuro ai dipendenti al momento giusto per renderli più produttivi. Inoltre, gli approcci tradizionali sono soggetti al rischio informatico, a causa dell'esposizione delle due reti. Zscaler svolge un ruolo fondamentale nel consentire agli utenti di accedere in modo sicuro alle applicazioni principali che rientrano nell'ambito dell'accordo, sia che si tratti della separazione di una grande impresa o di una cessione di attività più ridotte. Zscaler riduce significativamente il rischio informatico, semplificando al contempo il processo di separazione.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata sull'SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

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