White Paper

Ensuring Cyber Integrity Throughout a Divestiture or Carveout

Introduction

During divestitures, the IT leaders are tasked with a dual mandate of securely preparing for the separation without disrupting the operations of the seller (RemainCo) or the divested entity (SpinCo). As part of the Transition Service Agreement (TSA), the seller agrees to provide IT lights-on support up until the SpinCo is able to fully stand up its operations or a full integration with the buyer is accomplished. This provides a unique challenge, wherein the RemainCo will have to create a secure access path into its environment for the SpinCo and its buyer's users.

The Seller typically starts preparing for the sale several months before putting the business up for sale. Once the scope of sale has been established from a business perspective, the first step is for the seller to understand the deal perimeter, including the technology assets and people that will be carried over from the SpinCo as well as the ones that will stay with the RemainCo thereby requiring TSA. This is critical to ensure the success of the transaction by safeguarding IT assets.

After the deal perimeter is finalized, the seller has to create pro forma financials showing the standalone operating and capital expenses to run the SpinCo as a standalone business. Finally, the seller will have to work on an interim architecture approach that will provide technology access to the SpinCo employees in a secure way.

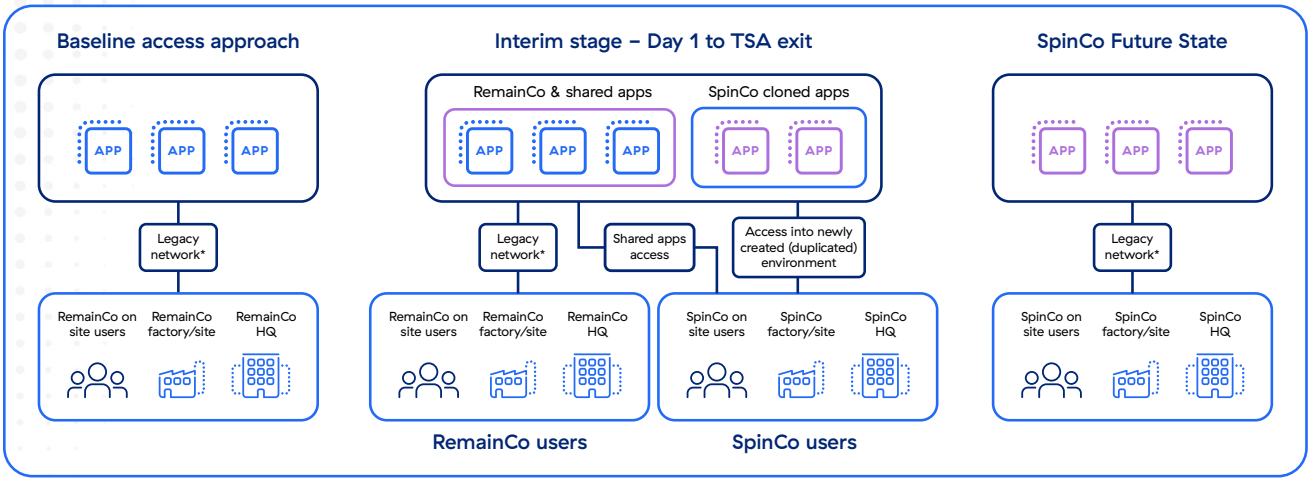
Traditional legacy approach

The traditional approach involves a network–based separation strategy with a couple of options for the Seller to provide access to applications during the TSA period:

Description	Potential drawbacks
Shared access to SpinCo users within the Seller's current environment	Risk of a breach is very high because of access from users with unknown security posture
Follow a hybrid approach; move dedicated SpinCo applications into a separate environment and provide access to shared applications within the current environment	Risk of a breach is very high because of access from users with unknown security posture. Additionally, significant upfront effort will be required for the Seller to carve out a separate environment and segment the traffic.
Migrate all the applications to a separate environment; dedicated applications may be moved as they are, while shared applications may be cloned with only SpinCo data retained	This approach will require a thorough understanding of all the applications and data that should be migrated to the new environment. Additionally, this may be highly complicated with dependency on multiple workstreams (e.g., applications, data, hosting, networks)

As noted above, this approach requires months of upfront planning, leading to companies establishing conservative timelines by factoring in supply chain issues for hardware and network infrastructure components and setting up secure intermediary networks even before the separation process begins. Moreover, the RemainCo network is exposed to the SpinCo users, presenting the risks of lateral movement and data loss.

Traditional Approach: Cloned SpinCo Network with Intermediary network for inter entity access



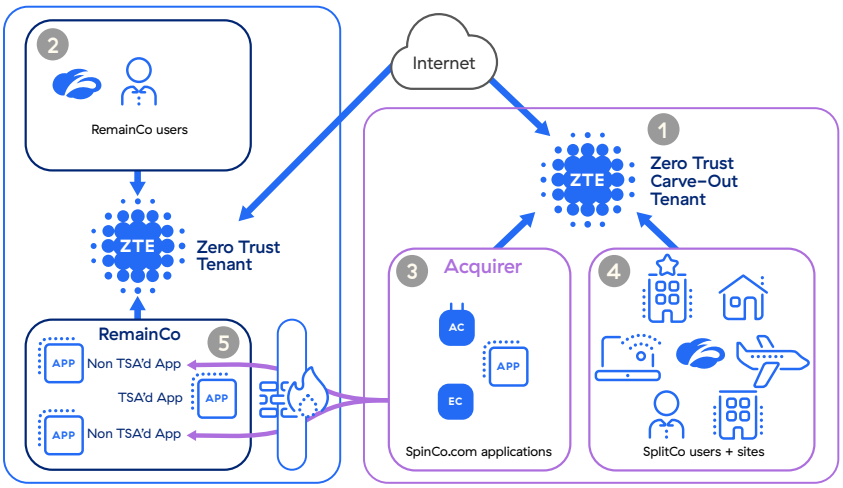
*Legacy approach leverages MPLS, firewalls, load balancers, etc.

For example, a large retailer recently split into two separate entities, leveraging shared applications, infrastructure, and network with a 2-year TSA period. In order to ensure success, they'll need to create separate IT landscapes, duplicate applications, and untangle a complex web of networks. This is a challenging push for IT and business leaders alike, and can prove risky for deal value.

A modern approach underpinned by the Zscaler cloud platform

Zscaler's cloud-based Zero Trust platform eliminates the need for legacy network segmentation and hardware-driven approaches to connectivity. Our platform helps you achieve segmentation at the user and application level by defining access policies enforced by the Zscaler cloud. Typically in divestitures, a tenant is stood up to enable connections to shared applications in a shared environment. From there, policies and impacted users can be defined and access granted.

Zscaler Approach: Zero Trust Access to SpinCo through a carveout tenant



1. Establish Splitco ZTE tenant, IdP, and domains
2. Profile environment to define users, applications, and policies
3. Redirect Splitco users to Splitco ZTE
4. Assign Splitco applications to Splitco ZTE
5. Establish controls for TSA applications remaining behind

Recently, Zscaler worked with a large industrial conglomerate wherein a separate tenant was created for the divested business entity and access to shared applications was restricted using policy configurations. In the end, all divested business users were migrated to the new tenant. When these divestitures occur, Zscaler can support users in different locations with different personas who are accessing both dedicated and shared environments.

Common use cases supported by Zscaler during a divestiture

1. **Access to custom applications:** Zscaler Private Access (ZPA) can be leveraged to secure access to custom applications hosted in an on-premises data center or in a public cloud. Zscaler provides the ability to secure access into a seller's environment hosting shared and dedicated applications as well as the SpinCo's environment and their dedicated applications. All of this can be achieved quickly for both remote and in-office users through a cloud configuration-based approach—without the need for additional hardware.

2. **Securing internet traffic:** Zscaler Internet Access (ZIA) can be leveraged to to secure access to SaaS applications and open internet websites. Additionally, advanced threat protection features can be enabled through a click of a button to protect a seller from potential cyberattacks and breaches during the transitional period.

3. **Application discovery:** Zscaler, once fully deployed, can discover applications used by SpinCo users to help IT teams understand which apps see the most use as well as their usage patterns, helping to determine separation demands during the TSA period.

4. **Performance monitoring:** Zscaler Digital Experience (ZDX) reduces the burden on IT operations by providing a single pane of glass—the Zscaler ZTE Admin Portal—through which helpdesk teams of both the seller and the SpinCo can closely monitor for network outages and performance issues. ZDX relieves helpdesk teams of both the seller and the SpinCo of the arduous processes of handling tickets and identifying the owners of particular issues by providing necessary telemetry data across the two environments.

Benefitss of Zscaler approach

 **Time to value**	• Rapidly finalize application inventory • Achieve user–to–application connectivity in weeks • Decrease the duration of the TSA
 **Simplicity**	• Remove IT from the critical path for Day–1 readiness • Leverage a 100% cloud–based approach to connectivity • Secure access path and internet traffic with a zero trust solution
 **Financials**	• Lower one–time and recurring separation costs • Reduce TSA costs and stranded assets/technical debt • Decrease IT standup cost by allowing transferability of the Zscaler platform
 **Integrity**	• Minimize the risk of data loss • Reduce insider threats and unauthorized third–party access • Enable auditable controls to meet Day–1

Conclusion

In divestitures, IT separation is often consumed by entanglements and challenges in providing secure access to employees at the right time for them to be productive. Additionally, traditional approaches are prone to cyber risk due to exposure between the two networks. Zscaler plays a pivotal role in enabling users to securely access key applications as part of the deal perimeter, whether engaging in a large enterprise level separation or selling off smaller assets. Zscaler significantly reduces cyber risk while simplifying the separation process.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE–based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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