Zscaler and Okta Solution Brief for M&A and Divestitures

Challenges with M&A Integration and Divestitures

Mergers and acquisitions (M&A) bring challenges for user integrations and separations due to separate identity providers, duplicate or overlapping infrastructure, lack of security posture, and more. For a long time, this was considered a roadblock for realizing timely synergy and savings. Let's dive deeper into the challenges for small and medium–large size transactions:

1 **Small–size acquisition or separation (companies with few users)**

- **No identity provider:** Many companies who have a small user count may not have an existing identity provider which creates a delay in integrating them to the buyer company's existing identity provider. This setup means that applications cannot be shared unless the user is onboarded.

- **Poor security posture:** Small companies may have little to no security posture, which increases the risk compared to the value of the business.

- **Data exfiltration:** Small organizations that do not have a good data protection program would face issues with users uploading sensitive data to public SaaS applications that are used for moving data, causing a potential compromise of sensitive data.

2 **Medium–to–large size acquisition or separation:**

- **Multiple identity providers:** Large companies using multiple identity providers or identity providers that are different than the ones being used by a buyer organization can cause integration and access issues between users and applications.

- **Inconsistent security posture:** Due to the vast global and local presence of big companies, managing multiple sites and locations can cause an inconsistent security posture across the organization, creating loopholes in overall corporate security.

- **Data exfiltration:** Data protection is a big challenge for companies going through a transaction as users transition across or leave organizations.

- **Multiple application hosting realms:** Applications are hosted in multiple cloud environments, on–premises data centers, and even on factory floors. Varying hosting realms create an access challenge for applications across the environment.

- **Custom applications that cannot be migrated:** There are custom applications that cannot be migrated to the cloud, which require provisioned access during a transaction until alternative solutions are found.

- **Overlapping network constructs:** By following best practices in network design, companies are likely to have overlapping IP addresses which prevents the merged entities from being able to be directly connected.
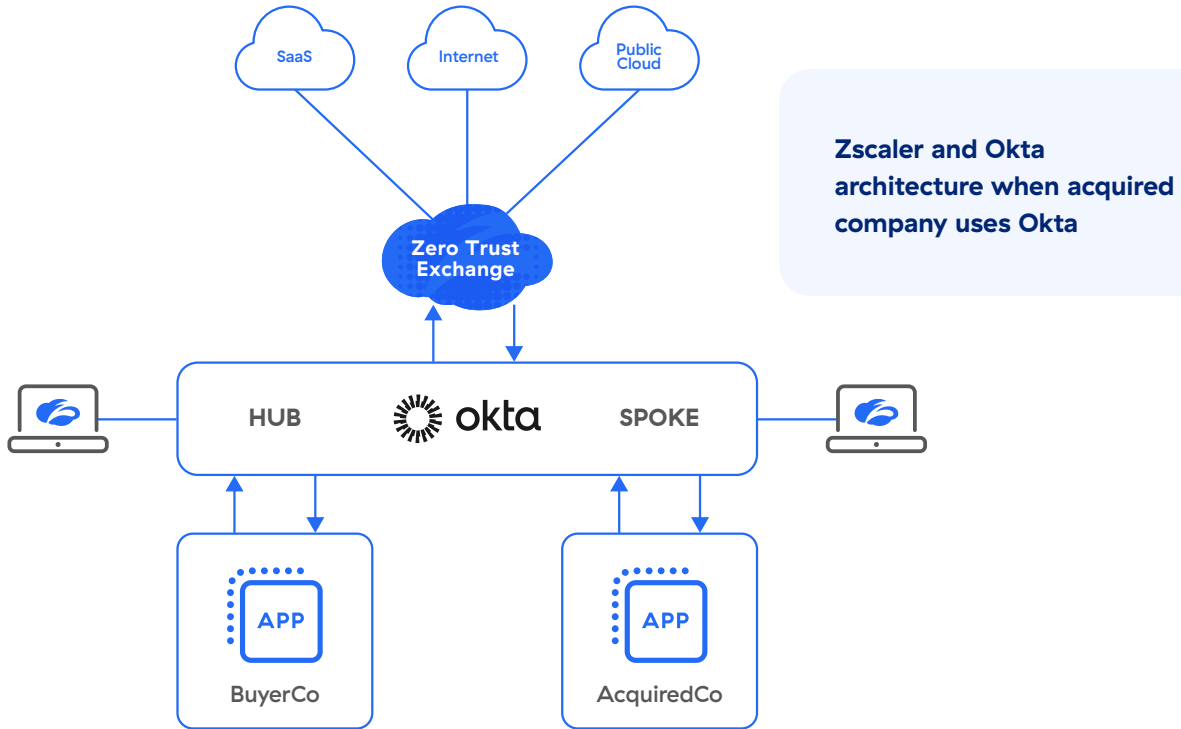
Zscaler & Okta

Zscaler and Okta seamlessly combine to build a platform which allows organizations to mitigate challenges during M&A/Divestiture transactions by adding Okta's best-in-class identity and access management to Zscaler's cloud solution. System admins can apply zero trust policies to every employee, regardless of where they are or what device they're using.

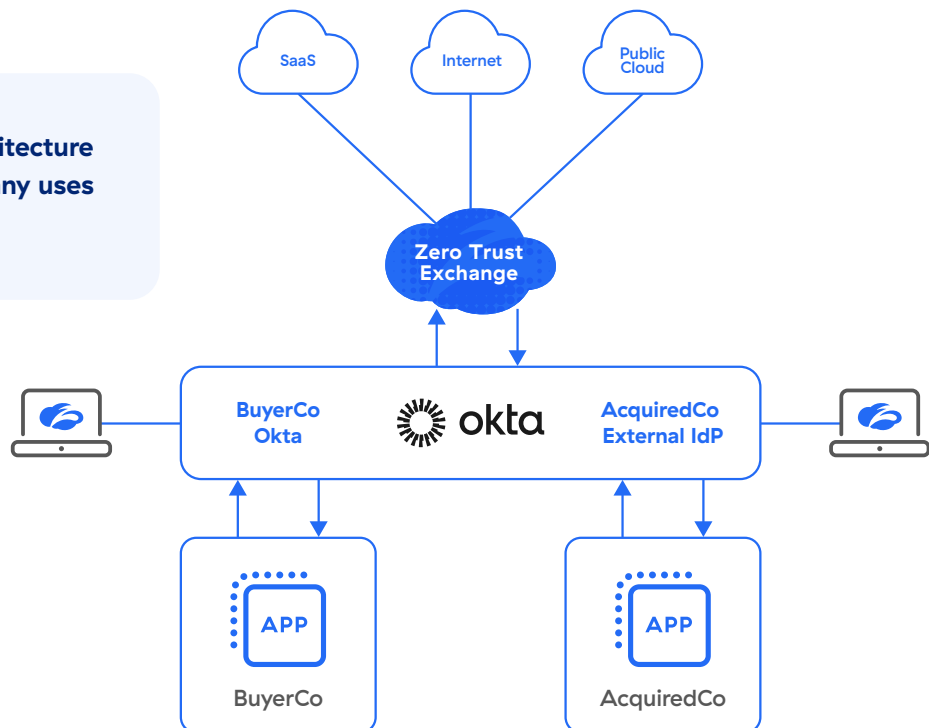**Mergers, Acquisitions and Divestitures:**

• For M&A transactions, we can use Active Directory using the Okta AD agent for user provisioning, application provisioning, and authentication. This alleviates the challenge of connecting two Active Directories, mitigating the challenges with domain consolidation.

• Zscaler multi-factor authentication for applications – accessed alongside zero trust security architecture provided by the Zero Trust Exchange.

• Zscaler Multiple IdP for integrating multiple organizations at once.

• Using Okta contextual access with Zscaler ZCC posture checks to ensure the right user gets access to the right resources.

• Leveraging Okta hub-and-spoke architecture to provide application access to AcquiredCo users.

• During an M&A transaction where Zscaler takes the user to the front door of the applications, Okta can help take the user beyond the front door and facilitate user access provisioning for the application, providing a complete solution for user-to-application access during an M&A transaction.

• Zscaler provides access to applications that may not be natively reachable due to overlapping network constructs. This access is not only immediate, but more secure than legacy direct access.
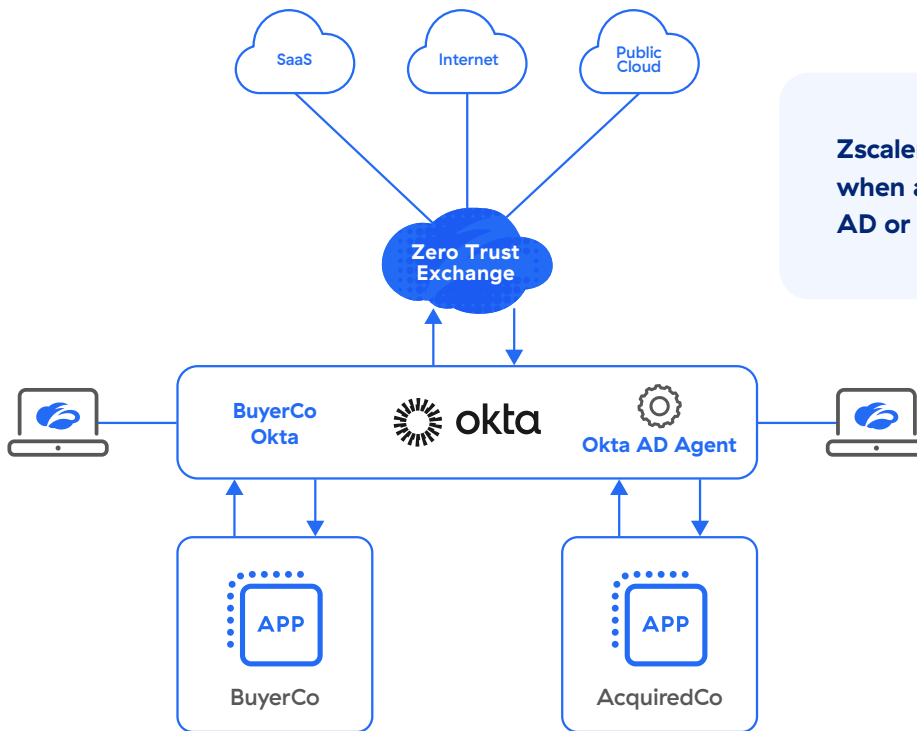
Once Day 1 integration or separation targets have been achieved, organizations can leverage Okta API Access/Lifecycle Management and workflow automation for automating user provisioning and deprovisioning. Using SCIM, Okta propagates these changes to Zscaler, which can terminate or allow access.

Architecture Diagrams (Mergers and Acquisitions)

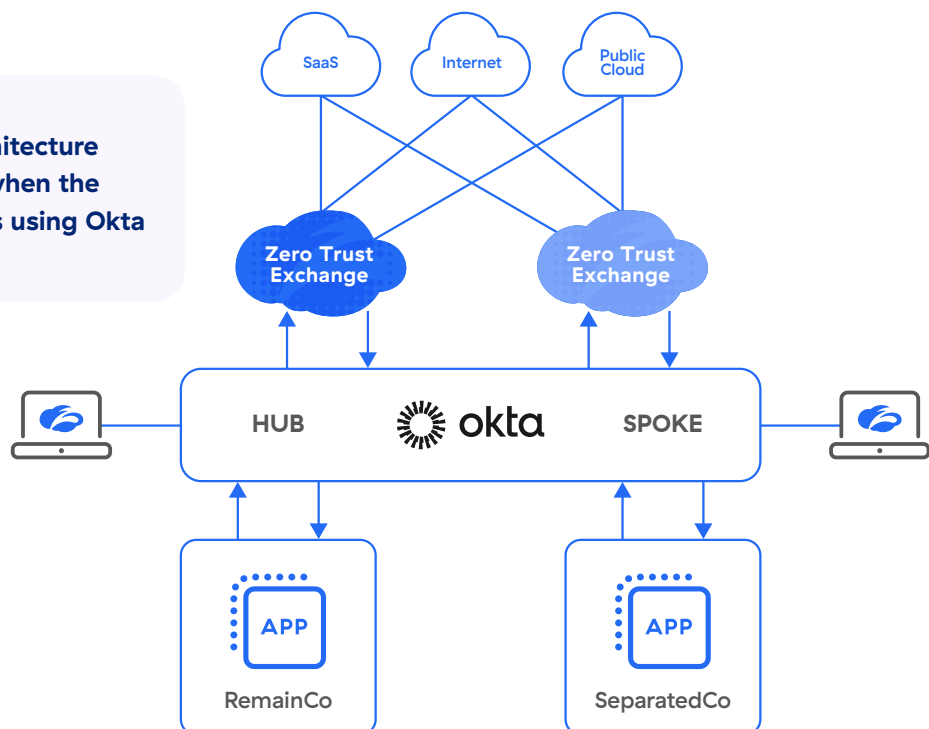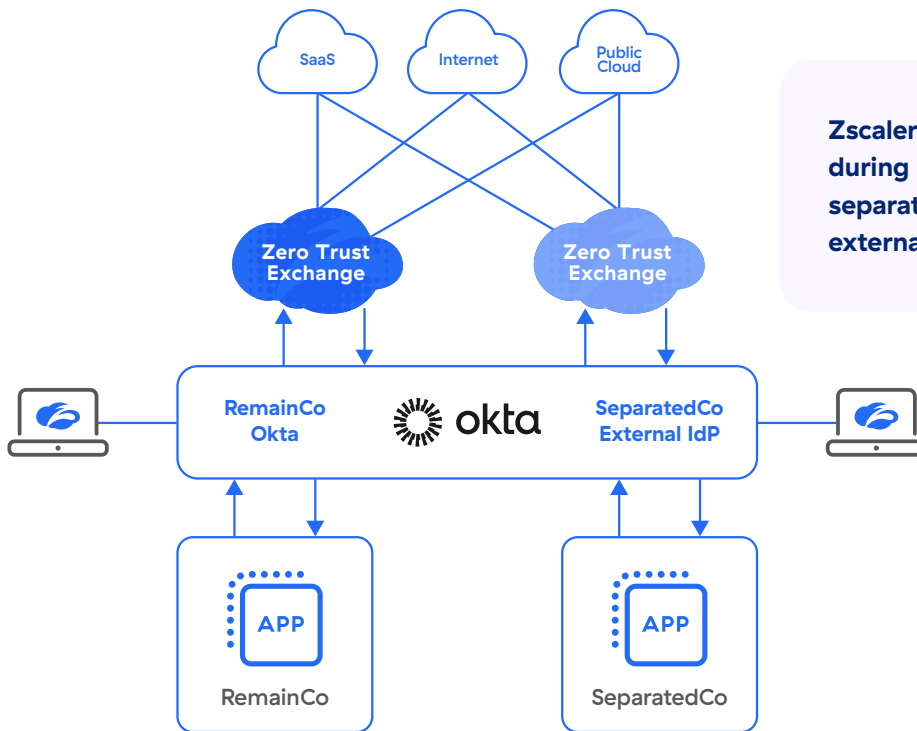**Zscaler and Okta architecture when acquired company uses Okta**

Zscaler and Okta architecture when acquired company uses an external IdP

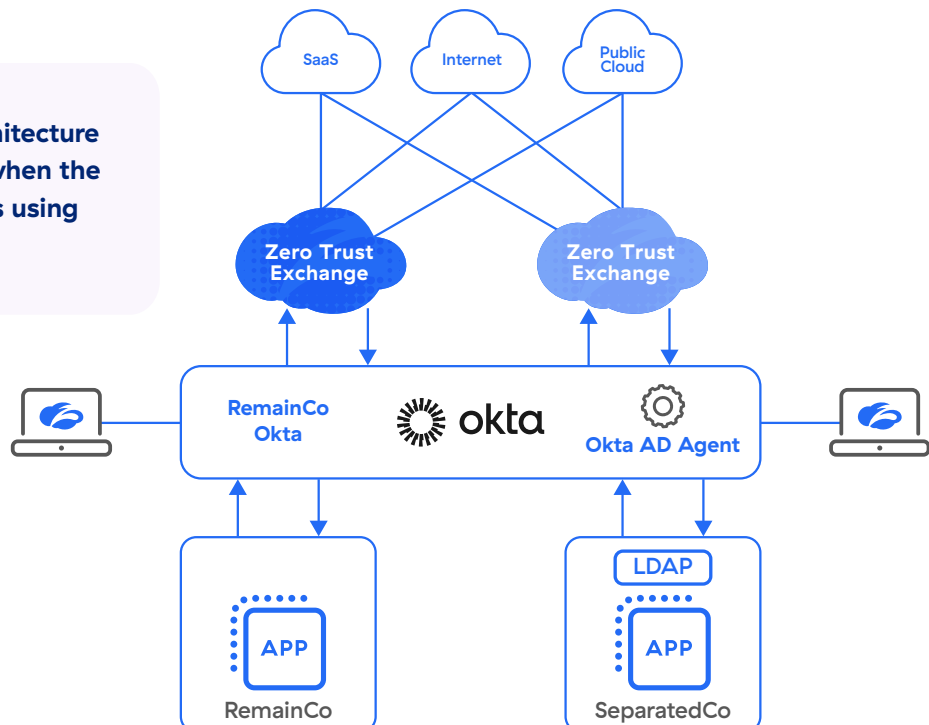**Zscaler and Okta architecture when acquired company uses AD or LDAP**

SaaS

Internet

Public Cloud

Zero Trust Exchange

BuyerCo Okta

okta

Okta AD Agent

APP
BuyerCo

APP
AcquiredCo

Architecture Diagrams (Divestitures)

Zscaler and Okta architecture during a divestiture when the separated company is using Okta

SaaS

Internet

Public Cloud

Zero Trust Exchange

Zero Trust Exchange

HUB

okta

SPOKE

APP
RemainCo

APP
SeparatedCo

Zscaler and Okta architecture during a divestiture when the separated company is using an external IdP

Zscaler and Okta architecture during a divestiture when the separated company is using AD/LDAP
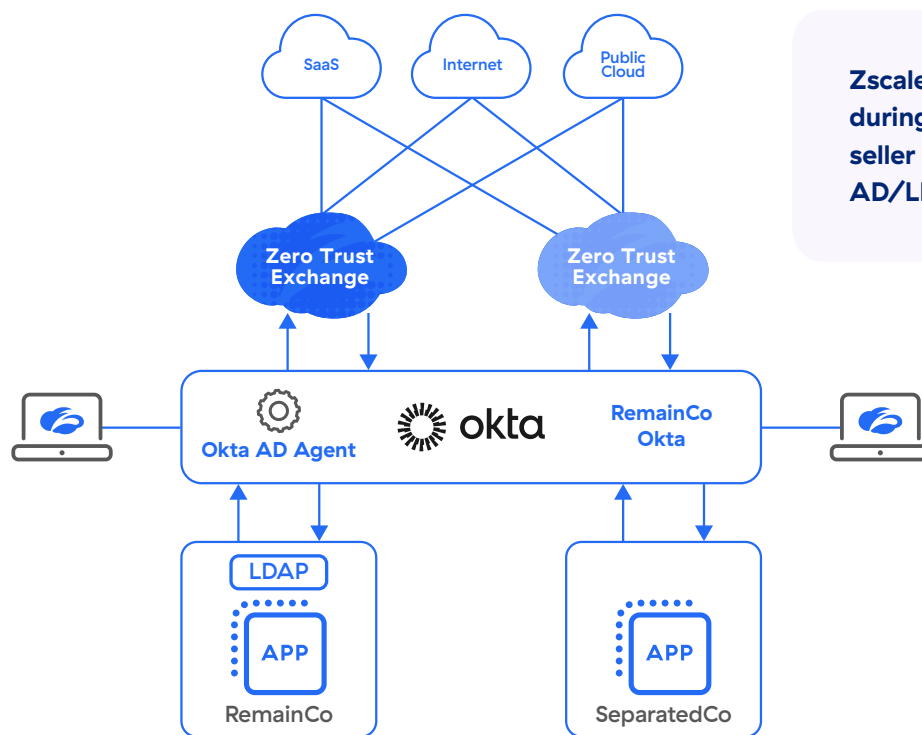
Zscaler and Okta architecture during a divestiture when the seller company is using AD/LDAP