Solution Brief

okta | zscaler™

Identity Continuity at the Edge

Okta Open Access Gateway (OAG) and Zscaler Private Cloud Controller (PCC) – Maintain secure access to applications, even when connectivity is denied or disrupted.

The Challenge

Zero Trust architectures depend on cloud connectivity, but that's not always guaranteed.

Zero Trust architectures route through cloud data centers, which creates a critical dependency. When connectivity is denied, disrupted, intermittent, or bandwidth-limited (DDIL), that dependency becomes an outage.

In remote or isolated environments, users lose the ability to authenticate and access critical apps precisely when business continuity is needed the most. Security teams lose visibility, access policies go unenforced, and operations come to a standstill.

The Solution

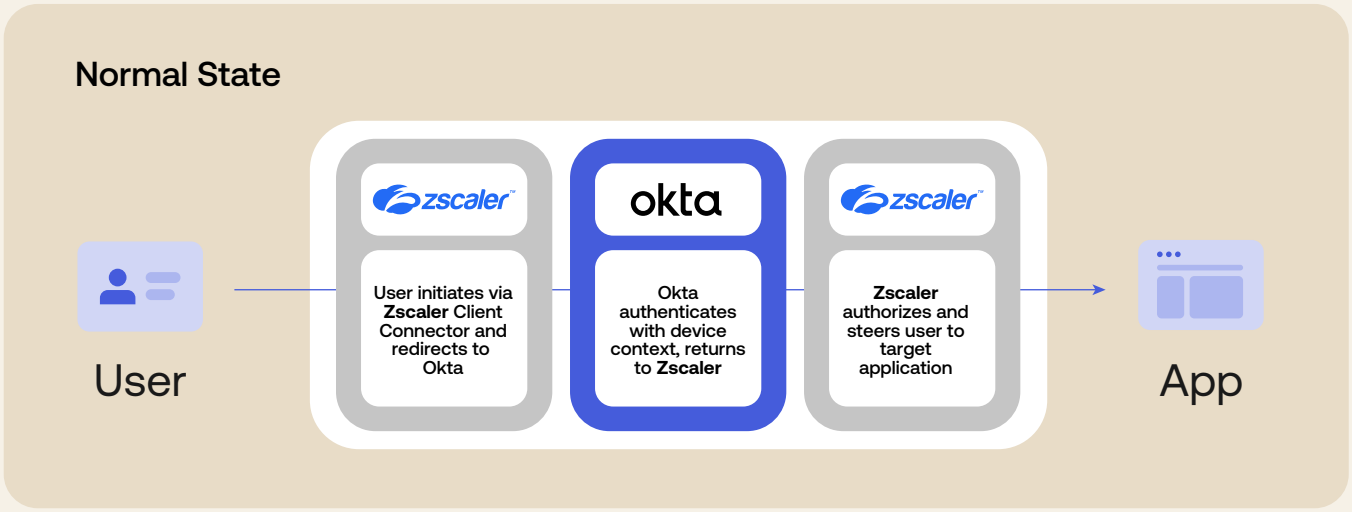
Continuity for both identity and access management.
Okta and Zscaler solve the DDIL problem through coordinated, independent continuity mechanisms. Neither vendor replaces the other – together, they cover both sides of the access equation.

Provider	Role
Okta Open Access Gateway (OAG)	Deploys in front of critical on-premises applications. When the Okta cloud IdP is unreachable, OAG authenticates users locally using pre-configured policy, keeping app access active without a live cloud connection.
Zscaler Private Cloud Controller (PCC)	When endpoints can't reach the Zscaler cloud control plane, ZPA fails over to a customer-hosted PCC. The PCC enforces cached policy for up to 90 days and maintains private app connectivity locally until cloud is restored.

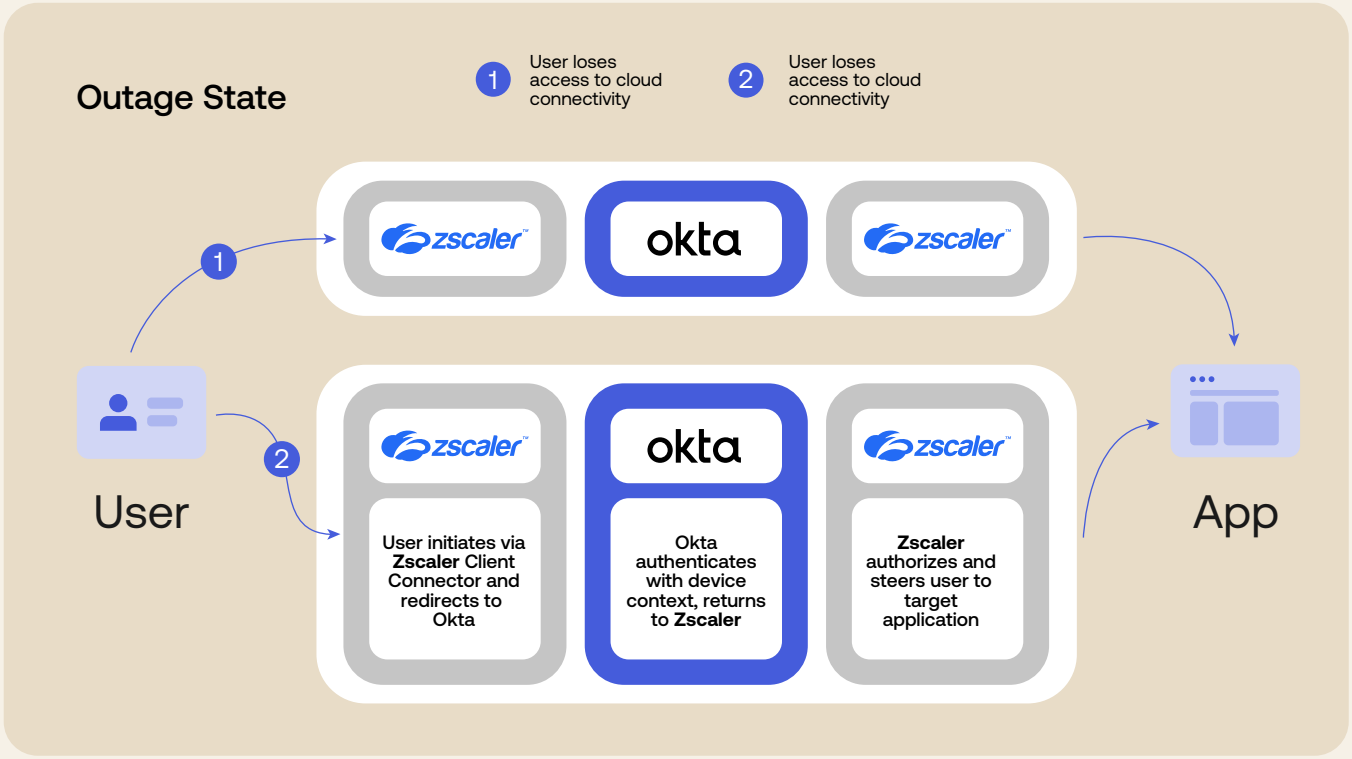
Together, Okta and Zscaler preserve end-to-end connectivity – from verifying the user to connecting them securely to applications (Zscaler) – even when the cloud is unreachable.

How It Works: In Both Normal and Outage States

In a normal state, when cloud connectivity is active, Okta acts as the IdP and Zscaler enforces policy for application access.



When cloud connectivity is active, Okta acts as the IdP and Zscaler enforces policy for application access. However, when cloud reachability is denied, disrupted, or bandwidth-limited, both Okta and Zscaler shift critical functions to customer-hosted servers, operating in parallel.



okta | zscaler™

Key Use Cases

Disaster Recovery

When a primary data center is impacted or taken offline, organizations need centralized control over user access. The integration keeps authentication and private access running through local fallback components, giving security teams control even as infrastructure fails over.

Remote and Isolated Environments

In locations with unreliable or limited connectivity – remote facilities, field offices, or sites with constrained bandwidth – users must still access critical systems. Okta OAG offline access and Zscaler PCC ensure that workers in these environments maintain access to private applications without depending on a stable path to the cloud.

Security Visibility During Disruptions

Even during connectivity disruptions, security teams require full visibility into access patterns. This integration ensures that audit trails, access logs, and policy enforcement maintain active during DDIL periods – and synchronize automatically when connectivity is restored.

Get Started

Okta Open Access Gateway Offline Access and Zscaler Private Cloud Controller are available today. Contact your Okta or Zscaler account team to scope a joint deployment or visit: **okta.com/products/access-gateway**