To support the use of cloud apps, you must be able to securely route your branch traffic direct-to-internet.

Key requirements for branch transformation

Here's what you need to do it:

Global Cloud
Data centers and egress points must be close to branch users in all geographies, and directly peered with your critical applications to provide fast connections and simplify compliance.

Full Security Stack
For identical protection across all locations, you need an integrated platform that inspects all ports and protocols, delivering the entire security stack of services: sandbox, firewall, advanced threat protection, and more.

Proxy-Based Architecture
Today, 91% of traffic across Google is encrypted¹, so SSL inspection is no longer optional. Your solution must natively inspect SSL-encrypted traffic, at scale, without degrading performance.

Elastic Cloud
To support your bandwidth-hungry applications and handle increases in network traffic—without added costs or complexity—you need a multi-tenant security platform that scales elastically.

Real-Time Policy Management & Visibility
You shouldn’t have to piece together fragmented logs, or use separate subscriptions or management platforms. Get real-time policy deployment and visibility by user, application, and location.

Learn how to establish secure local breakouts for all your branches. Zscaler.com/transform

¹ Google Transparency Report https://transparencyreport.google.com/https/overview