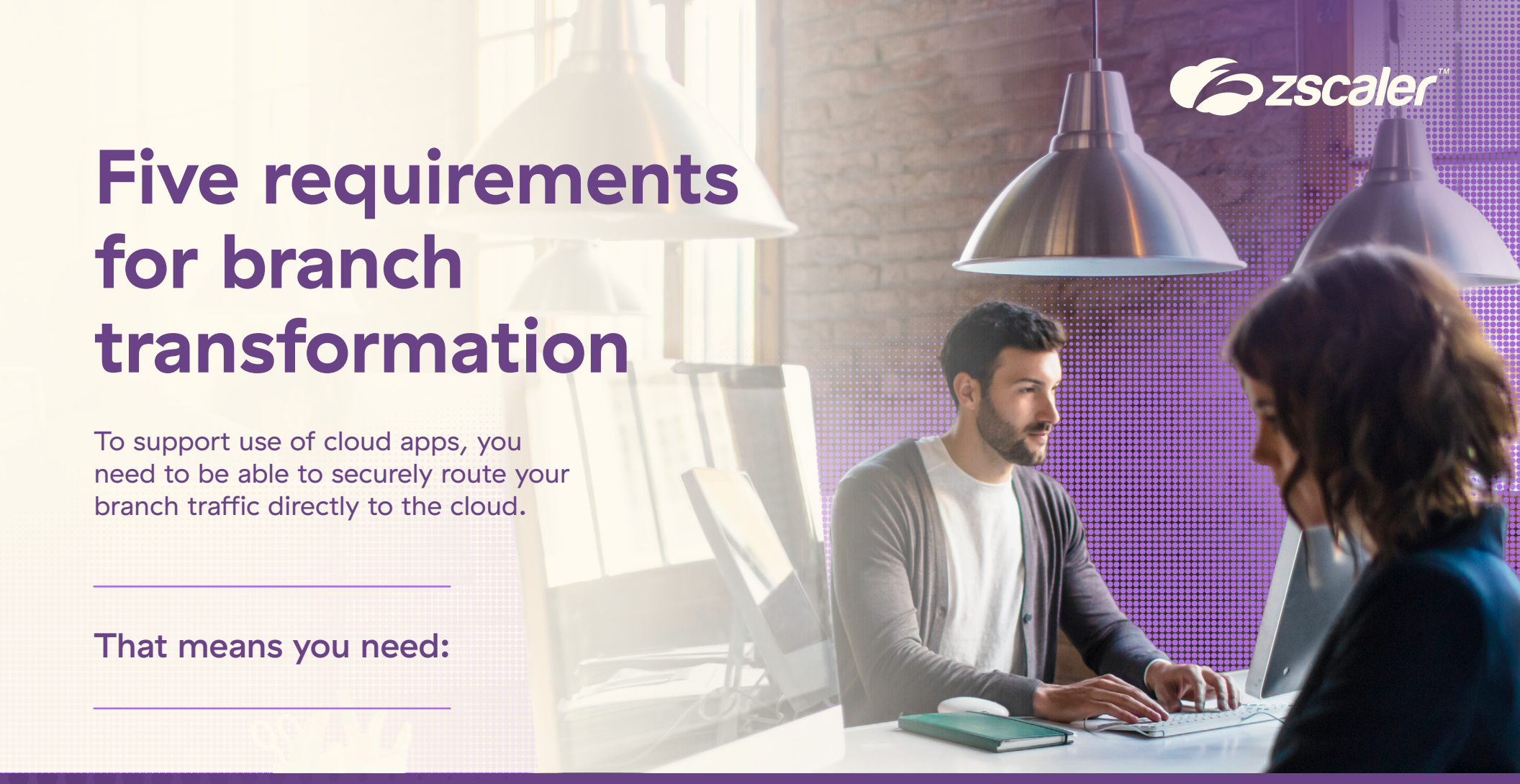
Five requirements for branch transformation



To support use of cloud apps, you need to be able to securely route your branch traffic directly to the cloud.

That means you need:

1 A global cloud

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

2 A full security stack

For identical protection across all locations, you need an integrated platform that inspects all ports and protocols, delivering cloud sandbox, firewall, advanced threat protection, and more.

3 A proxy-based architecture

With 95% of traffic across Google now encrypted,[1] TLS/SSL inspection isn't optional anymore. You need a solution that can natively inspect encrypted traffic at scale without degrading performance.

4 An elastic cloud

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

5 Real-time policy management and 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 at:

zscaler.com/transform

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

zscaler™ | Experience your world, secured.™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com