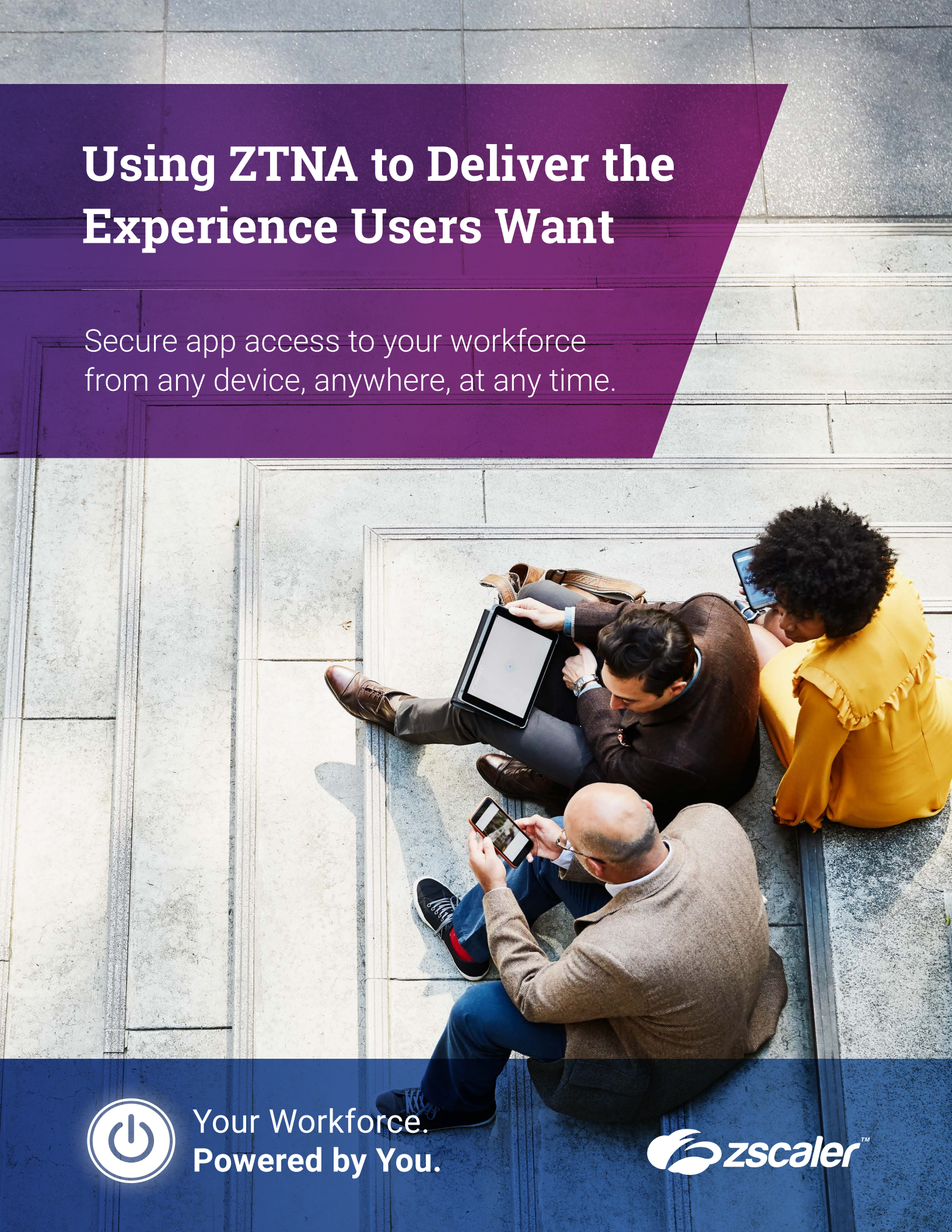
Using ZTNA to Deliver the Experience Users Want

Secure app access to your workforce
from any device, anywhere, at any time.



Your Workforce.
Powered by You.

zscaler™

"We want people to not have to think about how they will get access to their apps, and we want to support that capability quickly with as little friction as possible."

- Mike Towers, CSO at Takeda

Your user-base has evolved

It's 2020 and your workforce is no longer confined to the office. They are working from home, from hotels, and from airports. The devices they use are no longer managed BlackBerry devices given to them by the endpoint team. They are personal BYOD smartphones, tablets, and laptops used for both leisure and work.

You are responsible for not only securing your employees, but also third-party contractors who are on the company's payroll as well. All of these users need identical access to private apps across all devices, locations and application types. Providing access from these devices, without compromising security was at one point an impossibility. Not anymore.

A look at your portfolio of users

With a diversified workforce that is now globally distributed: providing secure access to private applications has become a challenge for IT teams. While the workforce may look different than it did 15 years ago, there is still something they have in common, all your users need fast, reliable access to private applications to keep the business running smoothly. Your modern workforce may look something like this:

The Traveler

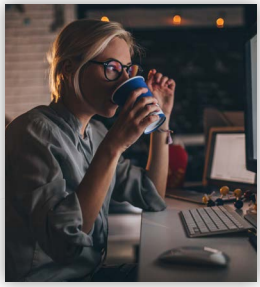
Sam Davis, VP of Sales

"I'm probably on the road about 75% of the time. More often than not, I'm in an airport, hotel, or customer site trying to get work done in the waiting periods. While my work setting may be constantly changing, I still need access to our business resources quickly so I can better serve our customers."

The Local

Danielle Allen, Finance Manager

"I'm based in our HQ in San Jose, California and am, for the most part an "in office" employee. I receive requests daily from other employees asking about their payments. I am constantly using our finance applications and need to access them quickly so I can stay on top of the requests."



The Contractor

Elaina Thalin, Web Development Contractor

"I've been on contract with the company for about 8-months now. While I'm not an employee or located in the office, I still need access to a few private applications in order to get my work done. If I can't access them then I really can't do my job."

The WFH-er

Justin Miller, Marketing Manager

"I live in Florida and am often impacted by weather warnings, including hurricanes. In those times, I've needed to ensure the safety of myself and my family while still upholding my work responsibilities."

Regardless of user type or job function, your workforce still needs to be able to access your private applications quickly and securely wherever they may be. IT needs to be empowered with the right technology to make this possible and ensure security isn't working against user productivity. This is why VPN isn't a match for the modern workforce.

Your users deserve better than VPN

Because VPN was developed over 30-years ago, they are no longer adequate for use with today's modern workforce, as their flawed security design delivers a poor user experience.

High latency, limited scale and poor experience
VPNs were designed to secure access to the network. This means that all user traffic is backhauled first to the datacenter, even if apps now run in public cloud. This causes network tromboning, which in turn creates latency for users. Also, the VPN appliances have user capacity limitations and can boil over if too many concurrent users are accessing the VPN server at once.

Repetitive logins and dropped connections
Every time there is a network change or inactivity, the VPN connection drops. For a now mobile workforce this can happen quite frequently which results in user frustration and loss of productivity.

Confusion on when to use VPN… Or not
Often times your users may not even know what the difference is between your public and private applications. Now with applications moving to cloud, there is evenmore confusion for the user knowing when, where, and how they should be using VPN. Needless to say, VPN is not seamless or intuitive for your users.

Just as Netflix could not have been built by connecting thousands of DVD players, private application access solutions for anywhere, anytime access must be purpose-built. They must be always available, highly scalable and user- centric. Retrofitting VPN appliances in the datacenter, virtualizing them, or placing them in the cloud, will not solve the user experience or network security related challenges that a mobile world creates. **A new approach is needed.**

"By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA."

Gartner, Market Guide for Zero Trust Network Access
Steve Riley, Neil MacDonald, Lawrence Orans, April 2019

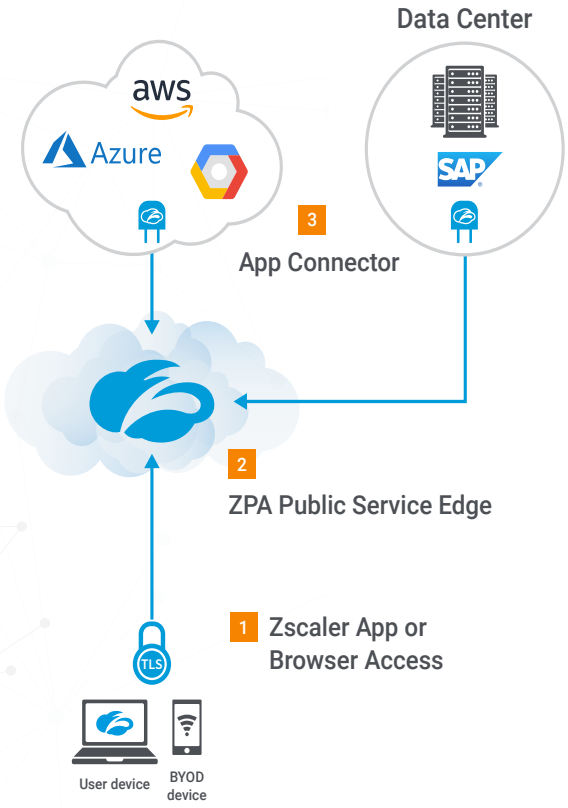
Ensuring users are productive with ZTNA

Whether accessing SAP in the public cloud, an SSH, RDP, custom intranet, or web-based timesheet app, the user experience should always be seamless. This is why Gartner recommends organizations adopt **zero trust network access (ZTNA)** technologies as a replacement for remote access VPN.

In most cases, ZTNA services are cloud-hosted and use policies to determine which authorized users get access to a specific private application. These polices take into consideration the identity of the user, their group, device posture and several other criteria.

Since many ZTNA services are fully cloud delivered, they allow users to connect to one of the service's many global points of presence, which then brokers the secure connection to a private application. This provides greater availability and far more scale than a VPN appliance. Users are never placed on the network, so traffic is no longer backhauled to a datacenter. This means that ZTNA service makes access seamless to the end-user while still empowering you to minimize risk to your business.

Zero trust network access (ZTNA) architecture



1 Zscaler App or Browser Access

- Redirects traffic to IDP provider for authentication
- Client Connector automatically routes traffic to Public Service Edge
- Browser Access removes need for client on device when accessing web-based applications

2 ZPA Public Service Edge

- Secures the user-to-app connection
- Enforces all customized admin policies

3 App Connector

- Sits in front of private applications in the cloud and/or data center
- Only responds to requests from ZPA Public Service Edge
- No inbound connections. Responds with inside-out connections only

Start delivering the experience users want

As you look to enable your users to be productive, consider a ZTNA service.

Be sure to check out how Steve Day, EGM of Infrastructure, Cloud and Workplace at National Australia Bank, enabled his users to be productive.

Watch National Australia Bank's Story

What's next? Take our ZTNA service for a test drive.

Start a 7-day ZTNA Demo

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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