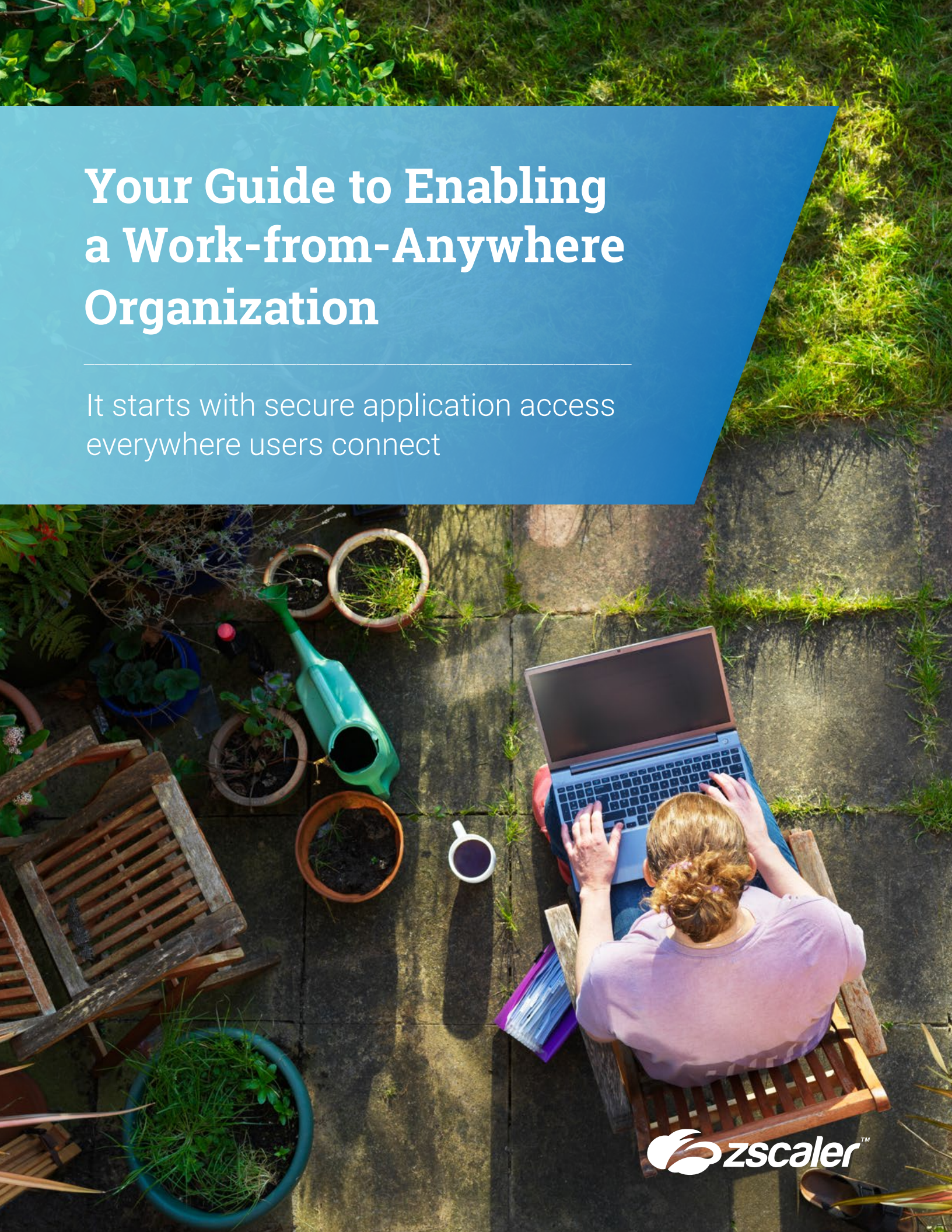
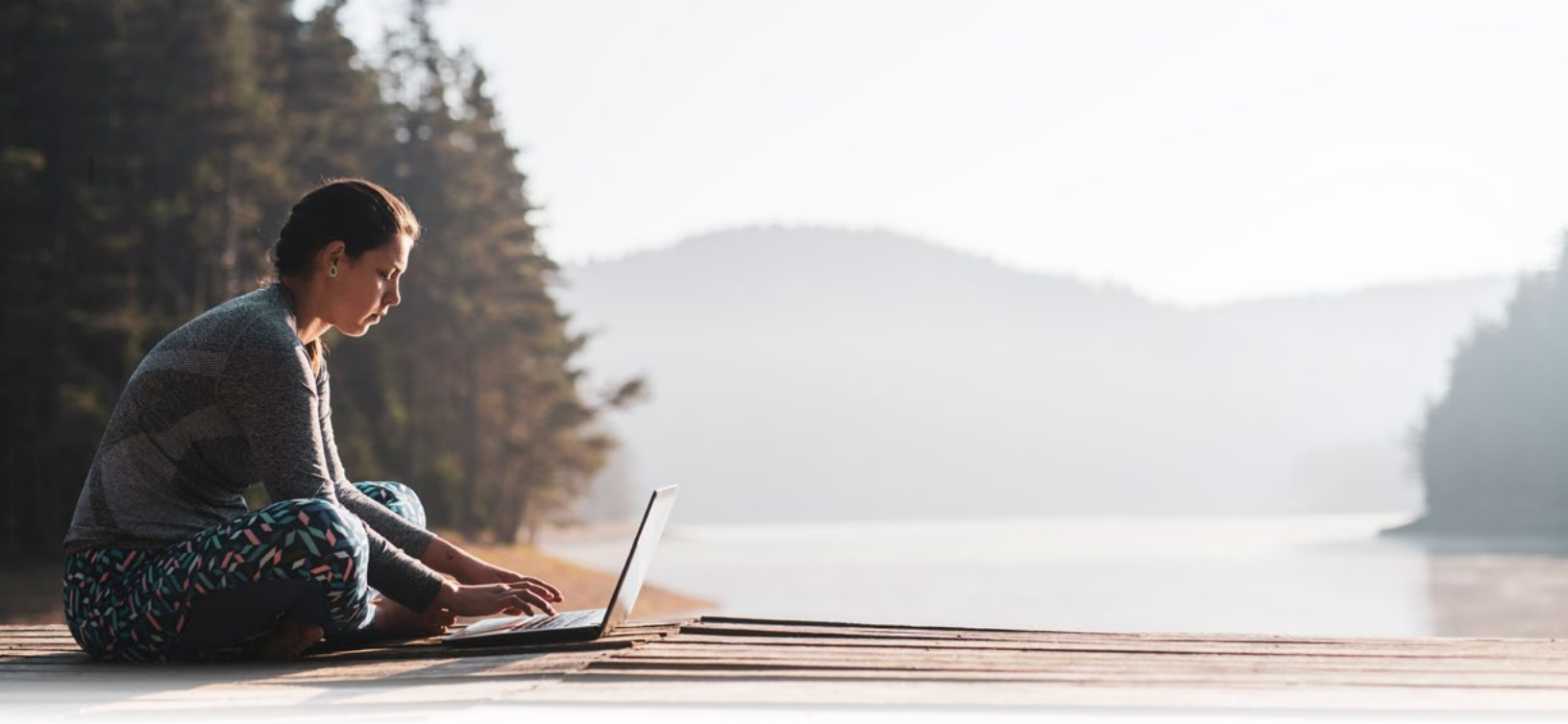
Your Guide to Enabling a Work-from-Anywhere Organization

It starts with secure application access everywhere users connect



zscaler™



The way employees work has changed dramatically in the past year as the world has had to quickly adopt work-from-home technologies for the sake of user productivity and business operations. While this has given employees the freedom to access data from practically anywhere, it also brings with it a host of challenges when it comes to mitigating business risk.

Mary, the sales rep

Mary is a sales representative who typically spends half of her time on the road. Now, she's working from home. But once the buildings start opening back up, she plans to go meet with customers. When she's at home (instead of her local airport) she likes to grab a hot coffee and catch up on work. She cracks open her laptop and away she goes, browsing the internet and accessing business applications. But, Mary may be opening up more than just her laptop. If her company requires her to use a VPN, she is directly accessing the corporate network and is exposing it to a host of potential threats. At the same time, she's frustrated by the slow experience while doing so. Risk with no reward.

The enterprise must be able to prevent the risk of exposure while still allowing Mary (and thousands of others like her) to access the internet and applications needed to stay productive. **But how?**

Mobility: The big security challenge

Typically, organizations have between 40 and 60 percent of their employees working remotely. Now that number is probably closer to 90 percent.

This means that the majority of knowledge workers and third-party contractors are accessing the open internet and business data using their home networks (which may or may not have robust security) and public Wi-Fi (a haven for cybercriminals), as their location fluctuates between home, office, and practically anywhere else.

IT professionals must become comfortable with the fact that a mobile landscape has reduced their span of control. The classic perimeter no longer exists. It's no longer possible to lock down their environment with a stack of network gateway appliances anchored in a data center (the moat to their castle) as they did in the days when employees worked solely in the office or remotely using only company-managed devices.

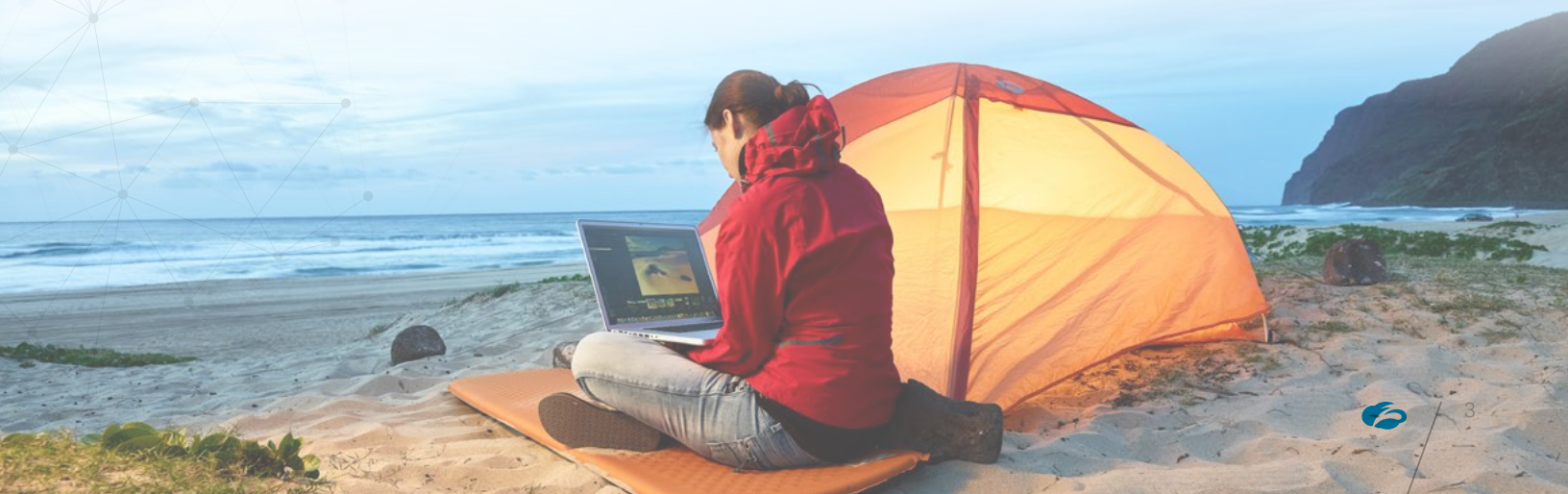
Technology decisions are critical to obtaining business productivity and protection, as well as providing IT leaders with an opportunity to drive transformation. The traditional network-centric technologies that teams have relied on for more than 30 years, such as remote access VPNs, have frustrated users and are now being used as a conduit for cyberattacks. For example, Travelex, a currency exchange company, was shut down due to attacks by cyber thugs using the company's Pulse Secure VPN as a Trojan horse to deploy ransomware (Sodinokibi).

VPN servers are exposed to the internet; and attackers have begun scanning for them as a way to gain access to the network. They achieve domain admin access, steal passwords, disable multifactor authentication and endpoint solutions, then deploy the ransomware. Such an attack locks a company out of its systems, which are then held for ransom.

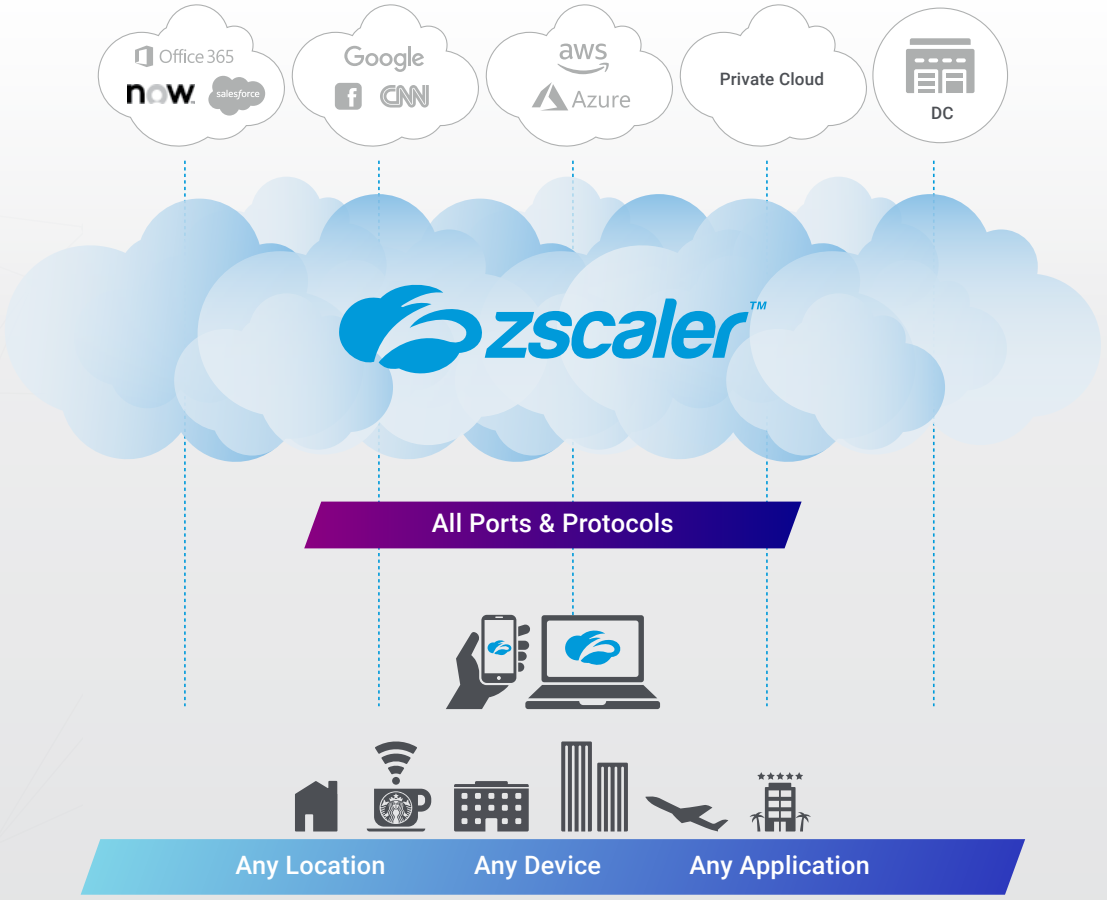
Best practices to live by in the work-from-anywhere world

IT leaders must shift to a cloud-based access solution as they adapt to the evolving needs of the business. When doing so they should focus on the following priorities the following topics and leverage cloud-delivered solutions to accomplish them:

- **Focus on user experience** – To provide the best experience and avoid hundreds of IT tickets, access solutions must support a variety of device types, and have a large, distributed presence that users can connect to. More points of presence will mean less latency, and a faster, more productive user experience for those working from home as well as when they return to the office.



- **Use identity-based policies** – Connect an authorized user to a specific application based on context (identity, device postures, etc.), and never to the network. This will provide a more granular means of connection, reduce lateral movement on the network, and minimize exposure of critical business resources to the internet.
- **Strive for simplicity and scale** – Leverage cloud-delivered technologies that integrate well together to simplify management. For example, consider secure access service edge (SASE) platforms, which include zero trust network access (ZTNA) services, cloud access security broker (CASB), and more. SASE platforms integrate with modern identity providers, such as Okta, Azure Activity Directory, and Ping Identity, as well as user endpoint management software, such as CrowdStrike and Carbon Black. Since the platform is cloud-delivered, IT can easily scale up the number of remote users without having to worry about capacity.
- **Don't lose visibility** – Cloud access services that are inline provide rich information around who is accessing what applications, from what device, and from where. This includes inspections of data encrypted within SSL. Traffic logs can then be streamed to Splunk, Sumo Logic, or another syslog service to help minimize remediation time in the event of a breach and react quickly to anomalous activity.
- **Consider country-specific challenges** – Countries, such as China, can present a challenge due to country-wide firewalls that make it difficult for employees to access resources outside the country. Consider services that can solve these challenges.



> "Zscaler was able to adapt quickly and increase capacity to more than satisfy our needs. As employee feedback from around the world has come in, I'm hearing exactly what I had hoped–it feels normal."
>
> **- Alex Philips, CIO, National Oilwell Varco (NOV)**

Cloud makes access from anywhere feel just like at the office

Zscaler™ provides cloud-delivered security and access services to ensure that businesses are able to operate under any conditions, at any scale, with employees anywhere in the world and on any device. The key is that a cloud-delivered service remains inline, securing all connections between users and the applications they need to help keep the business running smoothly.

The Zscaler cloud platform provides secure, seamless access to the internet and cloud apps (Zscaler Internet Access™), or to private apps in the data center or public and private clouds (Zscaler Private Access™). Access is based on software-defined business policies that follow users no matter where they connect or what devices they're using. With more than 150 globally distributed data centers, security is brought as close to the user as possible, providing fast, local connections to users everywhere.

Ensure your business is ready for work-from-anywhere

With the right technology IT can deliver the experience their users want and the security the business needs. As you look to enable the shift to this "new normal" and become a work-from-anywhere business, you can now develop a plan to accomplish it.

Learn how Zscaler has helped hundreds of companies secure their mobile workforce and adapt to work from anywhere. Visit **zscaler.com/solutions/work-from-home** or request a meeting with our team by emailing **sales@zscaler.com.**

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**.

©2020 Zscaler, Inc. All rights reserved. Zscaler™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. V072020

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