The COVID-19 crisis has transformed the workplace. 97% of CEOs cite “keeping employees safe and PRODUCTIVE” as their top priority. 34% of employees work FROM HOME in March. 250% INCREASE in remote work. 97% of commuting US workers in February WORKED FROM HOME in March. 34% INCREASE in Zoom video-conferencing app use in March 2020. 46% of CEOs say they will not bring workers back to the office before JUNE 2021. 75% of CEOs have ACCELERATED digital transformation in response to COVID-19. 46% of CEOs say they will not bring workers back to the office before JUNE 2021.

Enabling work-from-anywhere (WFA) is a challenge for enterprises. 96% of NOV employees had ever CONCURRENTLY USED VPN for remote access before the COVID-19 crisis.

Hackers are taking advantage of the remote workforce. 85% increase in PHISHING ATTACKS targeting remote users. 25% INCREASE in blocked malicious websites and MALWARE files. 17% INCREASE in THREATS targeting enterprise users.

The 7 considerations for enabling work-from-anywhere (WFA):

1. Secure access to applications
2. Cloud identity access management
3. Fast user experience
4. Rapid deployment
5. Visibility and troubleshooting
6. Cyber threat protection
7. Data protection

Enterprises successfully make the shift to work-from-anywhere with Zscaler:

- Takeda Pharmaceuticals REDUCED its firewall hardware appliances by 96% after shifting to SECURE REMOTE ACCESS.
- National Australia Bank enabled SECURE REMOTE ACCESS for 18,000 employees in just 4 WEEKS.
- DB Schenker transitioned 4,000 employees in its Asia/Pacific offices to SECURE REMOTE ACCESS in 20 days.

Learn how Zscaler enables work-from-anywhere.

zscaler.com/securing-remote-work