The COVID-19 crisis has transformed the workplace. 97% of CEOs cite “keeping employees safe and PRODUCTIVE” as a top concern. 34% of employees work from home in March. 250% increase in remote work from February to March. 97% of commuting U.S. workers in February worked from home in March. 34% increase in Zoom video-conferencing app use in March 2020. 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.

Enabling work-from-anywhere (WFA) is a challenge for enterprises. 46% of CEOs say they will not bring workers back to the office before June 2021. 85% increase in phishing attacks targeting remote users. 25% increase in threats targeting remote users. 96,000 new phishing-related domains. 30,000% increase in phishing websites, websites, and malware targeting remote users. 85% of NOV employees had ever concurrently used VPN for remote access before the COVID-19 crisis. Only hackers are taking advantage of the remote workforce. 85% increase in phishing attacks targeting remote users. 25% increase in threats targeting remote users. 17% increase in threats targeting remote users.

Learn how Zscaler enables work-from-anywhere. zscaler.com/securing-remote-work

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

Sources: Fortune, MIT, NYT

Sources: Fortune, Zscaler

Source: Zscaler Cloud Platform data, January through March 2020

Sources: Zscaler

Source: Zscaler

Source: Zscaler

Source: Zscaler

Source: Zscaler

Source: Zscaler

Source: Zscaler

Source: Zscaler