

The COVID-19 crisis has transformed the workplace.

97% of CEOs cite “keeping employees **safe and PRODUCTIVE**” as a top concern.

34% of commuting U.S. workers in February **WORKED FROM HOME** in March.

250% INCREASE in Zoom video-conferencing app use in March 2020.

Sources: Fortune, MIT, NYT



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**.

ONLY 8% of NOV employees had ever **CONCURRENTLY USED VPN** for remote access before the COVID-19 crisis.

75% of CEOs have **ACCELERATED** digital transformation in response to COVID-19.

Sources: Fortune, Zscaler

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.

96,000 **NEWLY-REGISTERED** COVID-19-related domains.

30,000% INCREASE in COVID-19-themed phishing, websites, and malware targeting remote users.

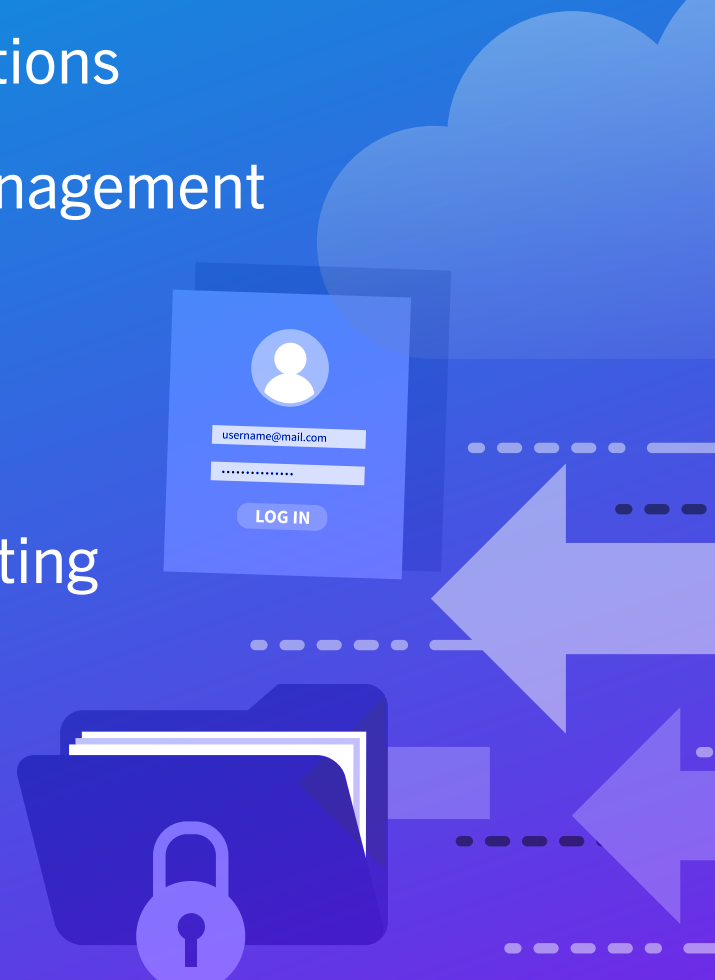
Source: Zscaler Cloud Platform data, January through March 2020



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

Source: Zscaler



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**.

nab National Australia Bank enabled **SECURE REMOTE ACCESS** for **18,000** employees in just **4 WEEKS**.

DB SCHENKER DB Schenker transitioned **4,000** employees in its Asia/Pacific offices to **SECURE REMOTE ACCESS** in **20** days.

Source: Zscaler



Learn how Zscaler enables work-from-anywhere.

zscaler.com/securing-remote-work