

# Making work-from-home work. A CISO's checklist



Global events have thrust CISOs into the spotlight as they work quickly to enable an at-home workforce without compromising security.

## Here are six things CISOs must consider:



### Prioritize work.

What tasks are most critical?  
What resources are needed.  
What can be postponed?



### Prioritize devices.

Some organizations haven't prioritized remote work, so you'll need to decide who will use the (possibly) limited number of portable devices.



### Stagger work hours.

You may have to switch mission-critical work to graveyard-shift hours to overcome connectivity limitations.



### Prioritize access.

What work requires always-on vs. occasional connectivity? You may have to provide "tiered" connectivity based on employees' work priorities.



### Ration collaboration applications.

You're going to need more licenses. In the short term, work with finance to reallocate "on hold" spending (say, travel or events) to enable remote work operations.



### Deploy local internet breakouts.

With employees connecting directly and securely to resources, you reduce your attack surface and alleviate VPN bottlenecks.



**Read more** about the keys to enabling an at-home workforce in a recent **blog** by Stan Lowe, Zscaler's Chief Global Information Security Officer. Or visit the Zscaler work-from-home (WFH) resources page.

[Explore WFH Solutions](#)