



Protect Your **Work-From-Anywhere** Workforce From Increasing Cyberthreats

Employees are working remotely more than ever. VPNs are struggling, which means your employees are dropping off VPN and bypassing your security and data protections.



Cybercriminals have taken notice, and have made your remote workforce a prime target. How can you turn the tide and protect your remote worker better?



1 Control off-network connections with Cloud Firewall

You need your corporate policy for off-network users. With Advanced Cloud Firewall, you can easily control connections, such as BitTorrent, RDP, FTP, and other risky activities.



2 Stop suspicious unknown files with Cloud Sandbox

With Cloud Sandbox, you can blanket all users with the power of an inline sandbox that quarantines dangerous unknown files and only delivers files that are confirmed clean.



3 Control data loss across in SSL and everywhere with Cloud DLP

Cloud DLP eliminates blind spots in SSL. It helps prevent the intentional or unintentional loss of confidential data and PII—no matter how your users connect—with unlimited capacity to inspect SSL.

Ready to close the security gaps with your remote workforce?

[Learn More](#)