Protégez votre **personnel en télétravail** des cybermenaces en perpétuelle croissance

Plus que jamais, les employés sont en télétravail. Les VPN sont en difficulté, ce qui signifie que vos employés se passent des VPN et contournent vos mesures de sécurité et de protection des données.

Les cybercriminels l'ont remarqué, et font de votre personnel à distance une cible privilégiée. Comment pouvez-vous inverser la tendance et protéger au mieux vos télétravailleurs?

1 Contrôler les connexions hors réseau avec **Cloud Firewall**

Vous avez besoin de votre politique d'entreprise pour les utilisateurs hors réseau. Grâce à Advanced Cloud Firewall, vous pouvez facilement contrôler les connexions, telles que BitTorrent, RDP, FTP et d'autres activités à risque.

2 Neutralisez les fichiers inconnus suspects avec **Cloud Sandbox**

Avec Cloud Sandbox, vous pouvez couvrir tous les utilisateurs avec la puissance d'un sandbox inline qui met en quarantaine les fichiers dangereux inconnus et ne laisse passer que des fichiers confirmés non suspects.

3 Contrôlez les pertes de données à travers le trafic SSL et partout avec **cloud DLP**

Cloud DLP élimine les angles morts dans le trafic SSL. Il permet d'éviter la perte intentionnelle ou non de données confidentielles et de PII — quelle que soit la façon dont vos utilisateurs se connectent — avec une capacité illimitée d'inspection du trafic SSL.

Prêt à sécuriser les failles de sécurité liées à votre personnel en télétravail?

En savoir plus