Remote-Mitarbeiter vor zunehmenden Cyberbedrohungen schützen

Heute ist Remote-Arbeit aktueller denn je. VPN sind unbequem, daher umgehen Mitarbeiter sie lieber ganz – und damit auch Ihre den Schutz Ihrer Sicherheit und Daten.

Cyberkriminelle haben ihre Chancen erkannt und lassen sie sich natürlich nicht entgehen. Wie können Sie das Blatt wenden und Ihre Remote-Mitarbeiter besser schützen?

1 Verbindungen außerhalb des Netzwerks kontrollieren: **Cloud Firewall**

Sie benötigen eine Unternehmensrichtlinie für User-Verbindungen außerhalb des Netzwerks. Mit der Advanced Cloud Firewall lassen sich Verbindungen wie über BitTorrent, RDP, FTP und andere riskante Aktivitäten problemlos kontrollieren.

2 Verdächtige unbekannte Dateien abfangen: **Cloud Sandbox**

Cloud Sandbox schützt sämtliche User mit einer zuverlässigen Inline-Sandbox, die verdächtige unbekannte Dateien in Quarantäne verschiebt und nur sichere Dateien weiterleitet.

3 Datenverluste in und außerhalb von SSL verhindern: **Cloud DLP**

Cloud DLP eliminiert tote Winkel in SSL. Mit unbegrenzter Kapazität zur SSL-Überwachung werden Datenklau und versehentliche Verluste von vertraulichen Daten und personenbezogenen Identifizierungsdaten auf sämtlichen Kanälen verhindert.

Höchste Zeit, die Sicherheitslücken für standortferne Mitarbeiter zu schließen?

Weitere Informationen