5 Reasons to Offer a VPN to Remote Employees

One of the best ways to keep employees and business data protected is by having them connect via Virtual Private Network (VPN). Here are five ways VPNs can keep remote employees secure.

Better network and firewall protection.

By routing a remote employee's internet traffic through your company VPN, you can provide the same firewalls and network-level protection that they'd have working at an office with robust cybersecurity defenses.

VPN can add another factor of authentication.

Multi-factor authentication helps add an extra layer of security to your network. It also enables you to create complex passwords for employees to be able to access company data.

You can restrict access to company data.

Restricting access to a VPN to current employees means it's easier to spot a usage anomaly. For example, if you're seeing 19 employees connected from Toronto, ON and one connected from Moscow, it's easier to spot a potential cyber event.

VPN can protect your data from the outside world.

Data leaks from unsecured servers are a regular occurrence, and the risk only grows from having more remote employees accessing them from multiple offsite locations. Putting your data behind a VPN and requiring authenticated access can prevent your data from being discovered online.

Protection from public and shared Wi-Fi.

With so many employees working from home, some may not have reliable or fast internet access and may need to rely on either public or shared Wi-Fi. A well-secured VPN connection means that employee data is encrypted and harder to intercept when being transmitted through a shared or suspect internet connection.

sovereign®
INSURANCE

Source: CyberScout