4 Ways To Improve Your Remote Desktop Security

Generally, remote desktop hacks all operate in a similar way. A malicious user will first compromise a computer on your network, and attempt to connect to your remote desktop system using your standard remote desktop protocol. They will then attempt to elevate their privileges on this network in order to gain administrative power. Even if they are not successful in gaining this level of access, the flood of incoming connections can paralyze your network, and make it impossible for legitimate users to connect.

Use a VPN

Using a Virtual Private Network (VPN) is one of the best ways to stay safe when working remotely. When using a VPN, your machine will first make an encrypted connection to your private network, and only then will it attempt to sign in to your remote desktop system.

Network Firewalls

Firewalls are another extremely effective way of reducing the risk associated with remote desktop environments. If you take security seriously, you are likely already using a firewall to protect and monitor your website. If you are not, do that immediately.

Restricting the RDP Port

By default, remote desktop connections are handled by one port: 3389. Restricting access to this port on your server firewall is a good way of limiting the scope for malicious connections. You can restrict access to this port to a specific set of IP addresses so that no-one else can connect to it.

Changing The RDP Port

Going further, you can even change the default RDP port to another one. Because hackers know the default RDP port, most brute-force attacks are designed to target this port. By changing the default port, you can avoid this type of attack.

Securely connect and control remote devices and servers to resolve issues faster. Take advantage of high-speed stable connections regardless of the computer's global location with onQloud.

We can't wait to show how it will works.

Get started