# VNC® Connect versus VPNs

This document addresses common security misconceptions made when comparing the remote access capabilities of VPNs with screen sharing technologies such as VNC® Connect.

Version 1.0

# Executive summary

A VPN and VNC® Connect are both inherently secure means of connecting to computers at a different location, but there has been a perception in some sectors (such as healthcare and manufacturing) that VPNs are superior in terms of the security they offer to customers, and that a screen sharing solution like VNC® Connect is not as secure as a VPN.

VPN technology has been around for a long time and has an established security model, but this document argues that VNC® Connect can be made just as secure as a VPN.

# VPN or screen sharing?

It's important to emphasize that, though the two technologies can be used to solve similar problems, the way they each work is quite distinct, so we are not necessarily comparing like with like.

A VPN provides a secure connection from a remote computer to a network of computers at a different location so that, for example, an employee can access the office network from home. A VPN effectively makes the remote computer accessing the network part of that network, with all the security implications this entails. All communication is encrypted, and routed through intermediate known or anonymous servers.

VNC® Connect and other similar screen sharing software enables a user to connect remotely from one desktop and control another desktop by mirroring the latter's graphical interface. Unlike a VPN, at no point is the remote computer part of the network and its resources.

Perhaps the only occasion that you might prefer to use a VPN over a secure screen sharing solution like VNC® Connect is when the remote computer is connected to an untrusted network, such as the public Wi-Fi in a coffee shop. In these circumstances, VNC® Connect only encrypts the data that is transmitted during the screen sharing session itself. All other traffic sent from the remote computer (for example, email) is not protected. In contrast, a VPN encrypts *all* traffic from the remote computer. In this situation, if you want to secure all traffic you might want to establish a VNC® Connect screen sharing session over a VPN. If you only want to control a remote computer using the medium of screen sharing, VNC® Connect is a perfectly secure solution.

However, in almost all other circumstances, VNC® Connect is just as safe as a VPN, as we will demonstrate in the key points below.

# Separation of environments

A key security advantage of VNC® Connect over a VPN is what we might call the separation of environments. When using any VPN, the remote computer that you connect from becomes part of the network to which you're connecting. Any malware on the remote computer can be transferred to the network and *vice versa*. This can present serious security issues. For example, in May 2017 the Wannacry ransomware, which spread over vulnerable networks, infected 230,000 computers in over 150 countries within a single day.

In contrast, when you use VNC® Connect, the remote computer is never part of the network. By default, only screen data and control events (keyboard, mouse, and/or touch) are transferred over the screen sharing session. You would actively have to use VNC® Connect's file transfer facility and transmit an infected file in order to infect the network, providing an enhanced level of security.

# Security protocols

Both a VPN and VNC® Connect are protected by robust security protocols, designed to protect your data. What you may not know is that VNC® Connect offers numerous features that should reassure customers in any doubt about the effectiveness of its security in comparison to a VPN.

VNC® Connect is designed in such a way that even if someone gains access to your RealVNC® account, they are not able to connect to your computers, since they would not know the computer password that is additionally required (see the *Remote computer authentication* section, below). Many other similar fail-safe design principles are included in our software.

Like a VPN, VNC® Connect protects your sensitive data by encrypting sessions end-to-end using industry-standard AES 128-bit encryption, with the option of using AES 256-bit encryption if required. Every session is treated as though it is made in a hostile environment. Connecting via a VPN *may* require that you open certain additional ports on your firewall, exposing it to the internet and possible malicious activity. In contrast, VNC® Connect never requires you to open any ports. All network negotiations are brokered via our secure cloud connectivity services, enhancing your security.

The RealVNC® accounts of all VNC® Connect users can be protected by 2-step verification (2FA). Once mandated by the system administrator, every user signing in to VNC® Connect must first enter their RealVNC® account credentials (email address and password) and then a Time-based One-Time Password (TOTP) generated by a mobile device app such as Authy.

An important security feature that some VPNs might not be able to offer is the ability to fine-tune the permissions of connected users, giving you the ability to grant or deny access to areas of functionality. A VPN might only be able to grant blanket access to any user who connects, but VNC® Connect allows you to customize these permissions. This ability to lock down areas of functionality, such as file transfer, offers yet another level of security.

Like any reputable VPN, VNC® Connect does not record your sessions, and session data cannot be decrypted, now or in the future. Behind the scenes, staff at RealVNC® are constantly checking for suspicious patterns of sign-in activity and other markers that help us identify attempts to illegally access your account, and blocking suspicious activity.

For an independent assessment of VNC® Connect's security, a recently commissioned report by Falanx Cyber Defence, a CREST-approved company with more than 20 years' penetration testing experience, is available here. In brief, their conclusion is that, based on the issues and risk rating identified, RealVNC's security is at a 'high level'.

# Remote computer authentication

As mentioned in the previous section, VNC® Connect provides two separate authentication mechanisms, so that no one password controls remote access. First, users must sign in to VNC® Connect on the remote computer they want to exercise control from, in order to see a list of available computers. Then, they must separately authenticate to the particular computer they want to control.

Like most VPNs, VNC® Connect supports multiple authentication schemes, and features the ability to customize them to your requirements, for example:

- **Windows/Mac/Linux password**—connecting users enter the Active Directory (or equivalent) user name and password they normally use to log on to their user account on that computer.

- **Single sign-on**—connecting users are transparently authenticated by secure network services (Kerberos), without having to enter a password.
- **Smartcard/certificate store**—connecting users are transparently authenticated by an X.509 certificate (stored on a smartcard or authentication token or in a certificate store), without having to enter a password.
- **Windows/Mac/Linux password + RADIUS server authentication**—connecting users enter their user account credentials, and then must authenticate to a RADIUS server.

You can use any of the above methods in combination to create your own custom authentication scheme. For example, you could combine certificate authentication with RADIUS server authentication and with your Windows/Mac/Linux password. Any user wanting to connect would have to know all three pieces of information. A failure at any step of the authentication process terminates the connection.

This ability to use multi-factor authentication (MFA) allows you to construct a very robust security framework, and makes VNC® Connect equally as secure as a VPN. This is particularly important for organizations that must adhere to compliance regulations. For example, The Health Insurance Portability and Accountability Act (HIPAA) demands that healthcare providers clearly document the data acquisition and transmission process. Multi-factor authentication is a strong authentication process that enables compliance with this standard.

# Ease of configuration

As we have seen, when correctly configured VNC® Connect can be made as secure as a VPN. However, VPNs often require a great deal of configuration, involving multiple credentials and the exchange of client certificates and private keys, before a connection can be established. Certificates need to be pre-deployed to users and there can be considerable IT support overhead. Correctly configuring servers for a VPN can be difficult and using one can present a steep learning curve for non-technical users unfamiliar with such software.

In contrast, VNC® Connect is a simple, streamlined application with an intuitive user interface that can be used by anyone within your organization without training. It is typically easier to set up a secure implementation of VNC® Connect than a VPN and you can customize it to provide the precise level of security that you require for your organization.

# Conclusion

Which solution you choose depends on many factors, but it is clear that VNC® Connect can be configured to be equally secure as a VPN, and has considerable other benefits in terms of ease of use and the flexibility that screen sharing itself provides.

More information about how VNC® Connect keeps your data secure and supports your regulatory compliance initiatives can be found in our security whitepaper.

VNC® Connect - the only remote access and support software you'll need. Head to realvnc.com/trial for a free 30-day trial.

**If you have any further questions, please contact us at enquiries@realvnc.com or visit realvnc.com/connect.**

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC® is the original developer of VNC® remote access software and supports an unrivalled mix of desktop and mobile platforms.  Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.



www.realvnc.com