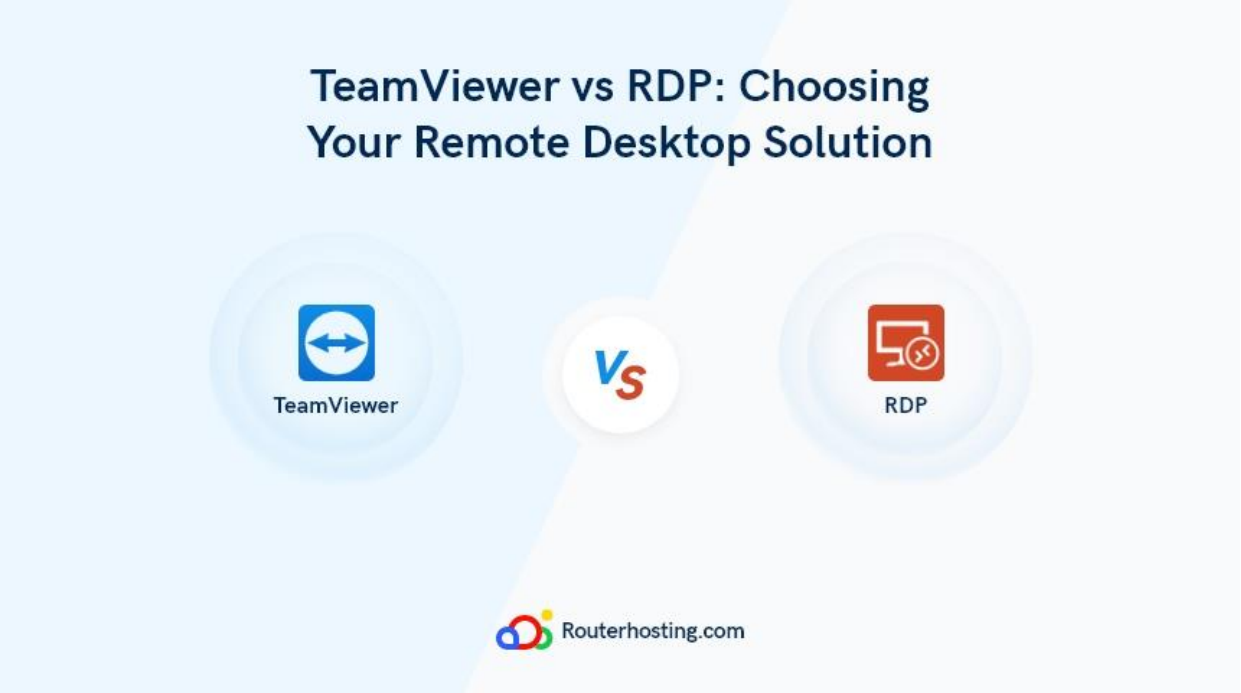
TeamViewer vs RDP: Choosing Your Remote Desktop Solution



Do you want to connect to another computer over the network? Do you want unattended access but wonder which remote desktop technology is your answer? Do you know what RDP is exactly? How about TeamViewer? Which one is better for you? What are the main differences between them? This article will answer all these questions.

Contents

the Most Significant Differences between TeamViewer and Microsoft RDP

If you want to remotely manage or access one or more desktops, you'd want to choose the best remote desktop software/technology in order to equip yourself. By selecting the right tools for your purpose, anyone can access any device, from anywhere in the world. This article reviews the differences between Microsoft RDP and TeamViewer, two of the most famous software in remote desktop.

What does RDP stand for?

Remote Desktop Protocol (**RDP**) is a Microsoft protocol designed for making connections to another computer or server, remotely. This technology is a built-in solution for both Windows and Mac operating systems for years. In RDP, a graphical interface is used over a network connection for connecting, accessing, and controlling data on another computer. In this technology, the user works with the RDP client software, while the other computer must run an RDP server software.

What is TeamViewer?

On the other hand, TeamViewer is an online collaboration tool, which is compatible with various platforms such as Windows, macOS X, Linux, Android, and iOS. This software allows organizing online meetings, file transferring, desktop sharing, and internet-based remote control between computers. You can also access another computer via a web browser.

The Difference in Security – Which One Is Safer?

RDP's traffic is encrypted by default, but it is still subject to Address Resolution Protocol (**ARP**) poisoning. Also, RDP doesn't come with multi-factor authentication by default, which makes the RDP ports remain open. If someone has your network address or your email, a brute-force attempt will be inevitable.

Besides, if you use RDP without a VPN, you will be a nice target for hackers. Therefore, make sure to use firewall-to-firewall VPN, and establish a site-to-site VPN tunnel connection before jumping into this type of connection.

In the case of security on TeamViewer, we should mention that this program uses AES 256-bit encryption, and can use two-factor authentication. This encryption is recognized as a high-quality standard, that also uses forced password reset in the event of suspicious activity.

Although, TeamViewer has vulnerability flaws that could occur when using a weak or re-used password. Moreover, due to Screen-unlock capability for facilitating a remote session, TeamViewer offers less physical security.

A solution for the physical security problem can be screen blacking. In the case of screen blacking, you can install TeamViewer monitor driver on the remote desktop for Windows 7 and below which is dependent on the implementation of hardware vendors.

> Another difference between RDP and TeamViewer in security matters, is in supporter actions. Due to disconnecting from the session, the user of **RDP won't see** the supporter action during remote desktop connection. On the contrary, the user of **TeamViewer** will be **allowed** to see everything that is done by the supporter.

Differences in Firewall and Port-forwarding

Configuration for port-forwarding and firewall is required in RDP, but TeamViewer doesn't need port-forwarding or any configuration for the firewall.

Differences in Function – RDP:

Pros:

- Remote Desktop Protocol has no need for a fast internet connection because you will be using your remote server as the resource to run applications.
- Monitoring and controlling all connected devices is very simple.
- The option to connect from any device.
- Easy access to files and folders.
- Quick troubleshooting.

Cons:

- Requires advanced configuration
- An entire network/system inaccessible in downtime
- Costly and complicated for multi-user environments
- Remote rebooting isn't allowed
- Needs third-party in some cases
- Resource bottleneck may occur depending on the power of the host and the number of users trying to access at the same time.
- Works only with Windows devices

Differences in function – TeamViewer:

Pros:

- Multi-platform support including Windows, macOS, Linux, Chrome OS, iOS, Android, and IoT devices.
- Easy installation and update.
- Team file sharing across multiple locations
- Easy communications with chat, video, and voice calling
- Free of charge for non-commercial use
- Doesn't need router configuration
- Allows teams to conduct training sessions for up to 25 members
- Excellent customer support
- Application windows, screens, and entire desktop sharing
- File sharing with the option of dragging and dropping
- Let's you know if your device is being remotely accessed

Cons:

- Costly for commercial purposes and needs license
- Large file sharing isn't allowed
- It needs the same version of TeamViewer installed on both ends of the connection
- Doesn't work through proxy servers
- Fast continuous internet connection is needed

Conclusion

Both Microsoft RDP and TeamViewer have their advantages. But selecting one of them entirely depends on your needs. However, TeamViewer offers you some features that go far beyond the functionality of RDP.

Note: This is a PDF version of our web page, you can also read this article in the following address:

https://www.routerhosting.com/teamviewer-vs-rdp-remote-desktop-solutions/