CAMEYO

eBOOK &
HOW-TO-GUIDE

How to Secure Remote Desktop Protocol (RDP)

Protecting Against Ransomware with Zero Trust

Cybersecurity firm Kaspersky reports a 767% increase in ransomware attacks last year, and research from Palo Alto Networks shows that Remote Desktop Protocol (RDP) has been the primary attack vector in 50% of all ransomware attacks since 2018.

In a world where enabling hybrid & remote work is critical, protecting against ransomware, brute force attacks, and malware has become increasingly difficult since many organizations are using RDP to enable remote access for their employees' endpoints.

The problem is that these existing remote access technologies (Microsoft RDP, Citrix, etc.) were born in an era of implicit trust where users are either all the way in, or all the way out. These technologies require organizations to either open up ports in their firewall to give people access, or to put everything behind a VPN. Both scenarios introduce significant security risks.

In This Guide

The basics of the Remote Desktop Protocol (RDP)

Before we dive into a potential fix for Remote Desktop Protocol vulnerabilities, it's important to understand what it is and why it's used. Otherwise you could risk breaking essential functionality.

RDP is the set of network rules used for communication between Microsoft's Terminal Server and the Terminal Server Client, which is a widely used means of providing remote desktop functionality to end users.

Whenever you have Remote Desktop Services enabled on any Windows server, it has RDP port number 3389 open by default. That standardization is helpful from a networking perspective, but it also makes that port number very attractive to malicious actors. They know there's a good chance that 3389 is going to be perpetually open as a listening port, especially among enterprise or distributed organizations, and they'll try to use it as a way to deliver a ransomware payload or DDOS attack.

So, to eliminate the problem, should you just disable RDP? Well, not exactly. The Remote Desktop Protocol is used by any number of applications that tap into Windows Server, and disabling it would mean losing essential services. It would make about as much sense as removing the engine of your car to make it less attractive to thieves.

A possible fix: Changing the RDP port in Windows

One way to thwart some of the less ambitious hackers and bots is to change the default RDP port number to something other than 3389. This is a good idea for both Windows clients and Windows Server, given that both use the same listening port for Remote Desktop Connection traffic.

Please note that this involves making fundamental system tweaks in the Windows Registry Editor. As a result, it could have knock-on effects for your device- and network-level firewall settings, which means that features related to remote desktop could break. Before starting, be absolutely sure you have a Windows registry backup and enough technical skill to reverse the steps below if that happens.

Bearing that caveat in mind, here are the basic steps to take to change RDP port on a Windows machine.

1. Double-click on the Windows Start button. Type in "regedit" (don't worry if there's not a dedicated text entry field) and then press Enter. This will launch the Registry Editor.
2. In the Registry Editor, look for HKEY_LOCAL_MACHINE in the navigation sidebar. Navigate to HKEY_LOCAL_MACHINE\SYSTEM by extending the drop-down list. From there, keep extending the drop-downs next to CurrentControlSet > Control > Terminal Server > WinStations > RDP-Tcp.
3. Click on RDP-Tcp. That will open up a list of items in the main window.
4. Find the dword file named "PortNumber". Right-click on the PortNumber dword file and select "Modify..."
5. You'll see a dialog with three fields: Value name, Value data and Base. Change the base to Decimal. In the Value data field, enter a new port number between 1025 and 65535. Make sure that the new remote desktop port number you choose is not already in use by another application or service.
6. Click OK, then reboot the computer.

All being well, you will have now successfully changed the default RDP port on your Windows machine. An important thing to remember is that, with Windows Server, you'll need to update your Windows firewall rules and also mimic this change across any clients that are still using the default RDP port. If you've only made the change on a Windows client machine, you'll have to manually update the Remote Desktop client the next time you connect. This is done by adding a colon and the new RDP port number after the machine's hostname or IP address (e.g., "hostname:1234").

Lock down your RDP ports with Cameyo

Rather than trying to dodge RDP security risks with Registry Editor workarounds, why not choose a solution that enhances security while facilitating hybrid and remote work?

Here at Cameyo we believe that for a solution to provide true Zero Trust security, Zero Trust must be foundational and systemic. Our platform was designed from day one as a native Zero Trust system where all security capabilities are baked into the core of the platform, never treated as an additional or optional layer.

Our single Zero Trust security architecture includes:

- **Complete Isolation –** Cameyo never trusts any device (even managed devices) because those devices can be compromised. Cameyo gives users secure access to the apps they need to be productive while providing complete isolation between devices and their organization's network/data.
- **Segmentation –** Even once users are in a session, Cameyo segments that session from customers' networks and data to ensure ongoing separation.
- **Prevention of Lateral Movement –** Even in the case where a device has ransomware or malware, that malware cannot reach the customer organization's network/data, nor can malware on their systems reach the Cameyo system.
- **Always-On Monitoring & Validation –** Cameyo utilizes non-persistent servers, so all customer user data is wiped from the Cameyo server every time the user logs out.
- **Least Privilege –** With Cameyo all traffic is encrypted and apps are delivered from a secure HTML5 browser, separating the user's device from the corporate network and eliminating the need for VPNs. Cameyo also utilizes Windows Terminal Services and temporary user profiles, ensuring users are unable to access admin privileges, settings, and files.
- **Identity & Access Management –** Cameyo integrates with the customer's Single Sign-On (SSO) provider of choice, and the Multi-Factor Authentication (MFA) they have set up with their SSO applies to Cameyo.

Whether you're concerned about cybercrime involving phishing, backdoors, antivirus/malware issues, RDP attacks, brute force attacks, preventing data breaches or likely all of the above, it's clear that hybrid work requires a complete revamp of how we think about and approach security. With the shortcomings of past and current solutions in mind, here are some things to consider going forward:

- **Limit your attack surface:** The more moving parts a solution has, the more potential points of exploitation it offers to rogue actors. Organizations, regardless of their size or sophistication, need solutions that eliminate the need for additional gateways and appliances that can inadvertently become security risks.
- **Control your ports:** Many remote technologies leave RDP ports open by default, which leaves your network vulnerable to brute force attacks. Your remote and hybrid work solutions should help lock down your ports by design, not haphazardly leave them open.
- **Eliminate VPNs:** VPNs simply create a secure tunnel between a user's device and the corporate network. That model is based on implicit trust of the user. But if that user is on a personal device that's riddled with malware, VPNs become a liability as they enable the user's infected machine to access your corporate network and data.
- **Keep it clean:** When your remote and hybrid employees are using remote technologies to access their apps and files, their user data must be deleted from the server every time they log out. That way, in the unlikely event that the secure browser is compromised, the hacker only has fleeting access to the user's session.

To that end, Cameyo makes use of multiple innovative technologies that mitigate risk and avoid common attack vectors like RDP port vulnerabilities. Some of these core technologies include:

- **Secure Cloud Tunneling:** Enables secure, user-friendly Virtual App Delivery independent of a VPN (which carries its own risks) and without needing to open any ports in the Windows firewall. You can read a detailed explanation of Cameyo's Secure Cloud Tunneling here.
- **Port Shield:** Provides built-in security that dynamically opens or closes HTTP(S) and RDP ports in response to authenticated users. Even though the RDP listening port remains active, it's inaccessible to non-authorized traffic—no Windows Registry Editor hacks needed. More info on Cameyo's Port Shield is available here.
- **NoVPN:** Ensures that all data traffic is encrypted and that apps are delivered from a secure HTML5 browser via an HTTPS session. This effectively separates the client device from the corporate network. This Cameyo help center article has more details on NoVPN and how it works.

Conclusion

Technologies like these—not to mention additional ones like non-persistent servers and single sign-on (SSO) support—are what set Cameyo apart from other app virtualization solutions and remote work strategies. In a survey conducted by the research firm TechValidate, 98% of respondents reported that Cameyo's security beats the competition (TVID: 8A7-240-702) while also being simpler to deploy and manage (TVID: FD6-B62-2F3).

To learn more or to see for yourself how Cameyo can help you meet your Zero Trust security goals while enabling ultra-secure remote & hybrid work, schedule a demo or get started with a free trial.

Let Cameyo Help

Here at Cameyo, our team has decades of experience in IT security, and our founder & CTO has 12 security patents. In addition to building the Cameyo platform with one of the industry's most robust Zero Trust architectures, our experienced team is here to help you every step of the way. Schedule a demo below to discuss with one of our experts today.

Schedule a Demo

cameyo.com