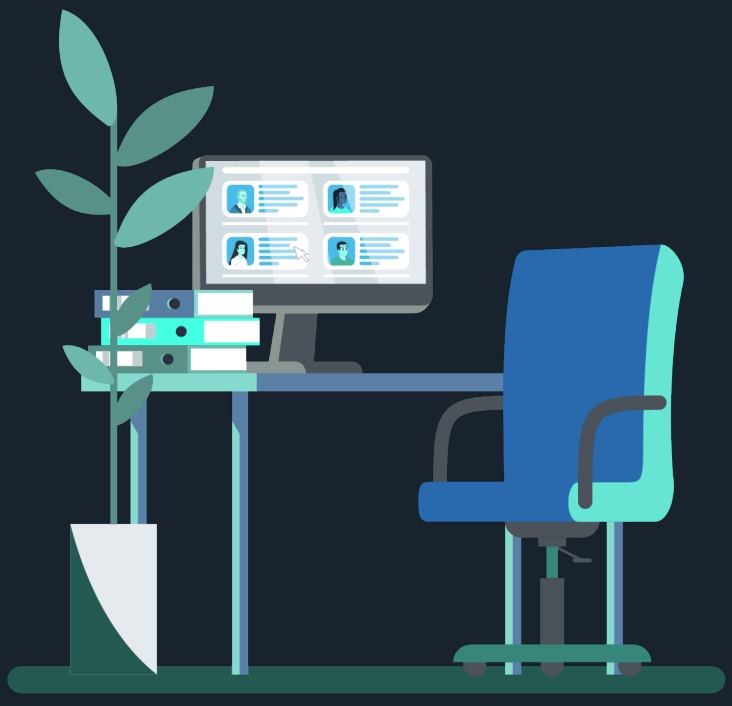
ENTERPROTECT

WHITE PAPER

# Securing RDP Connections: Protect Your Business from Cyber Attacks

Learn the best practices for securing Remote Desktop Protocol (RDP) connections and protect your business from cyber-attacks.



WWW.ENTERPROTECT.COM

# Disclaimer

Nothing contained in this document or relayed verbally will be deemed to amend, modify or supersede the Enterprotect Terms of Service or any other terms and conditions of any written agreement between the reader or reader's company and Enterprotect, or Enterprotect's subsidiaries or affiliates. Enterprotect does not make any promises or guarantees that any of the methods or suggestions described in this document will provide 100% protection against cybercrime, cyberattacks, disaster or similar incident. This document is not intended as legal advice nor should you consider it as such. The reader exclusively assumes all risk of utilizing or not utilizing any guidance described in this document.

ENTERPROTECT

# Introduction

Remote Desktop Protocol (RDP) is a widely used protocol that enables users to remotely connect to and control a computer over the internet. It is commonly used by businesses and organizations to allow employees to access their work computers from remote locations, such as when working from home or traveling. However, if RDP is left open to the internet, it can be easily exploited by cybercriminals.

RDP is a commonly targeted protocol and many attackers use automated tools to scan the internet for open RDP ports. Once they find an open RDP port, they can attempt to guess the login credentials or use other methods to gain access to the computer. This can allow cybercriminals to steal sensitive information, install malware, or even take control of the infected computer. This is a significant concern for businesses and organizations, as a successful RDP attack can lead to data breaches, financial losses, and reputational damage.

The purpose of this white paper is to raise awareness on the importance of ensuring RDP is not open to the internet and to provide organizations with best practices to secure their RDP connections. This paper will cover the overview of RDP attacks, the RDP vulnerabilities and risks, and the best practices to secure RDP. It will also provide some statistics and references to back-up the importance of this issue.

# Overview of RDP Attacks

In recent years, there have been many high-profile RDP attacks that have resulted in significant financial losses and reputational damage for organizations. For example, in 2019, a cybercrime group known as "GandCrab" used RDP to spread malware and extort victims for millions of dollars. The group was able to gain access to victims' networks by exploiting open RDP connections, and then used the access to spread malware and steal sensitive information.

Another example is the ransomware group "Sodinokibi" which used RDP to gain access to the networks of several organizations, including a major U.S. hospital in 2020. The group used the access to spread malware and encrypt the organization's data, demanding a ransom payment to restore access. The attack caused major disruptions to the hospital's operations and resulted in significant financial losses.

These examples demonstrate the dangers of RDP attacks and the importance of securing RDP connections. Cybercriminals are able to exploit open RDP connections to gain access to networks and spread malware, resulting in data breaches, financial losses, and reputational damage for organizations.

Additionally, according to a report by the Cybersecurity and Infrastructure Security Agency (CISA), RDP was the most common method used by cybercriminals to gain initial access to a network in 2019. This highlights the need for organizations to take proactive measures to secure their RDP connections and protect against these types of attacks.

# RDP Vulnerabilities and Risks

Remote Desktop Protocol (RDP) has several vulnerabilities and risks that can be exploited by cybercriminals. One of the most common vulnerabilities is weak authentication. Many organizations use weak or easily guessable passwords for RDP connections, making it easy for cybercriminals to gain access to networks by guessing login credentials. Additionally, many organizations do not implement two-factor authentication (2FA) or multi-factor authentication (MFA), further increasing the risk of unauthorized access.

Another vulnerability is outdated software. RDP is a complex protocol that relies on many different software components, including the operating system, RDP client, and RDP server. If any of these components are outdated or not properly configured, they can create vulnerabilities that cybercriminals can exploit to gain access to networks.

These vulnerabilities, if not properly addressed, can lead to significant risks for organizations. Cybercriminals can use open RDP connections to steal sensitive information, install malware, or even take control of the infected computer. This can lead to data breaches, financial losses, and reputational damage for organizations.

It is crucial for organizations to be aware of these vulnerabilities and risks and to implement best practices to secure RDP connections. This includes implementing strong authentication methods, regularly updating software, and monitoring for suspicious activity.

# Best Practices for Securing RDP

Ensuring Remote Desktop Protocol (RDP) is not open to the internet is critical for organizations to protect against RDP attacks. There are several best practices organizations can implement to secure their RDP connections, including:

- Configuring firewalls and network security devices to block incoming RDP connections. This can prevent unauthorized access to networks by blocking incoming RDP connections from the internet.
- Using a virtual private network (VPN) to securely connect to the network. A VPN encrypts data in transit and ensures that only authorized users can access the network.
- Implementing strong authentication methods. Organizations should use multi-factor authentication (MFA) or two-factor authentication (2FA) to increase the security of RDP connections.
- Regularly updating systems and software. Organizations should keep their systems and software up-to-date to reduce the risk of vulnerabilities being exploited. This includes updating the operating system, RDP client, and RDP server.
- Monitoring for suspicious activity. Organizations should monitor their networks for suspicious activity, such as failed login attempts, and respond quickly to any security incidents.

By implementing these best practices, organizations can significantly reduce the risk of RDP attacks and protect their networks from unauthorized access.

It is also important to note that organizations should conduct regular security assessments and penetration testing to identify any vulnerabilities and address them as soon as possible. This can help organizations stay ahead of potential threats and minimize the risk of a successful RDP attack.

ENTERPROTECT

# Conclusion

In this white paper, we have discussed the importance of ensuring Remote Desktop Protocol (RDP) is not open to the internet. RDP is a widely used protocol that enables remote access to computers, but if left open to the internet, it can be easily exploited by cybercriminals. We have seen examples of high-profile RDP attacks in recent years, which have resulted in significant financial losses and reputational damage for organizations.

We have also discussed the RDP vulnerabilities and risks, as well as best practices for securing RDP connections. Organizations should take proactive measures to secure their RDP connections, such as configuring firewalls and network security devices to block incoming RDP connections, using a virtual private network (VPN) to securely connect to the network, implementing strong authentication methods, and regularly updating systems and software.

In conclusion, it is crucial for organizations to be aware of the potential risks associated with RDP and to take the necessary steps to secure their RDP connections. This includes implementing best practices and regularly conducting security assessments and penetration testing. By taking these steps, organizations can protect their networks from unauthorized access and minimize the risk of a successful RDP attack.

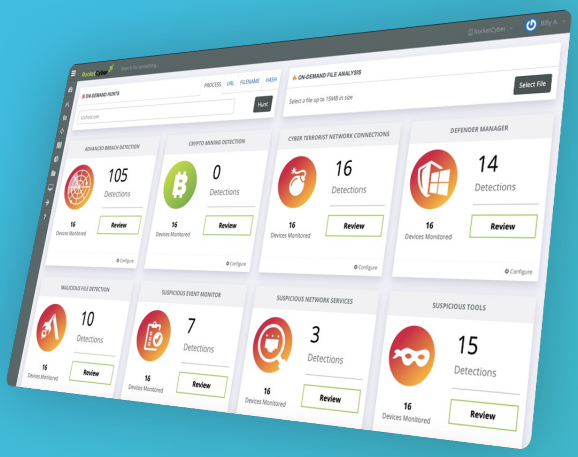
Additionally, it is important to note that the security landscape is constantly evolving, and organizations should stay informed about the latest RDP vulnerabilities and threats, and adopt new technologies and best practices as they become available.

Introducing

# ENTERPROTECT 360

## The Cybersecurity Platform for Busy IT Professionals

Enterprotect 360 is an all-in-one solution that provides powerful protection across your endpoints, network, and cloud - monitored 24/7 by security experts and integrated into a single, easy-to-use console.




**Protect Against Ransomware and Zero-day Threats**
Multi-layer prevention, protection, detection, and response system stops emerging threats quickly with industry-leading efficacy.

**Proactively Reduce Your Cyber Risk**
Continuous scanning your endpoints, network, and internet-facing assets for vulnerabilities combined with simple-to-follow remediation guidance backed by support from security experts.

**Detect and Eliminate Persistent Threats**
Threat Hunting powered by real-time threat intelligence feeds detects, and eliminates, malicious footholds and persistent threats dwelling in your environment.

**Add Cyber Experts to Your Arsenal**
Extends your workforce with a team of security experts who reduce alert noise, review suspicious activity, and respond to security incidents 24/7.

**Detect & Respond to Intrusions and Attacks Quickly**
Real-time monitoring of malicious and suspicious activity, identifies attacker TTPs and triggers human response from the Security Operations Center 24x7.

**Unified Cybersecurity Dashboard**
Single, Cloud-based Cybersecurity Console lets you see all of your cybersecurity in one place, and provides easy access to alerts, tools and reports.

**Try Enterprotect 360 including the 24/7/365 Security Operations Center**

WWW.ENTERPROTECT.COM/FREE-TRIAL

ENTERPROTECT

# Your Cybersecurity Partner

When it comes to cybersecurity, smaller IT teams have the toughest job out there. That's because you have to take care of everything IT-related - in addition to managing cybersecurity.

All too often, there is no one on your team dedicated to security – and even if there is, the bad guys don't clock out, and you/your security person can't work 24/7.

The choice seems to be - to go it alone - or try and get the budget to bulk up your security stack with more (often ineffective) cybersecurity tools.

That's why we created Enterprotect.

Enterprotect combines best-in-class technology and seasoned cybersecurity experts to make the job of managing cybersecurity much easier for smaller IT teams; without breaking the bank.

WWW.ENTERPROTECT.COM

Do you have feedback on this document?

Let us know what you think