ManageEngine
ADSelfService Plus

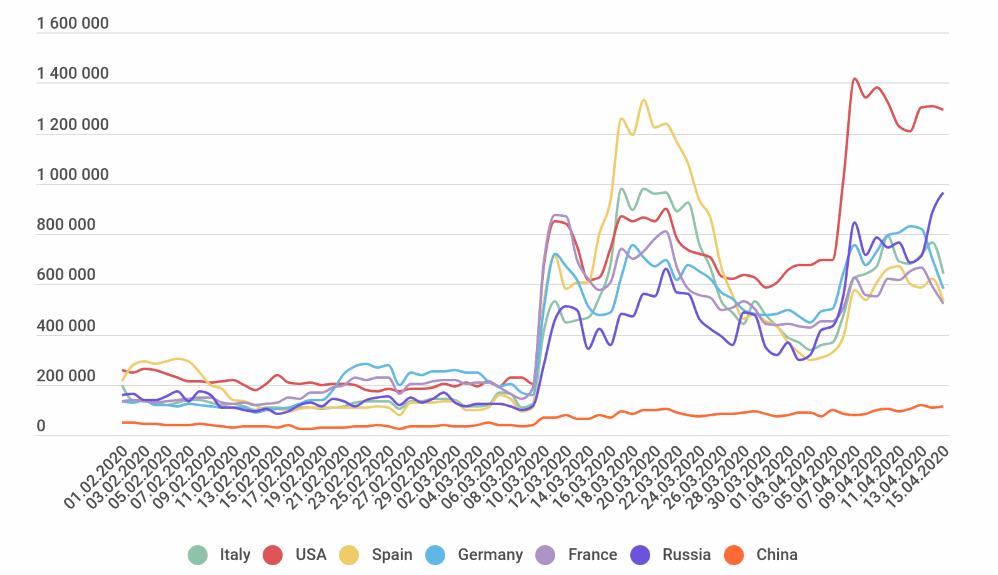
The essential guide to **securing RDP and VPN access** to sensitive resources

www.adselfserviceplus.com

Table of Contents

Cybersecurity in times of crisis

Kaspersky, a cybersecurity firm, indicates that the number of brute-force attacks targeting Remote Desktop Protocol (RDP) endpoints is rising steadily.[1] According to the recent report published, RDP brute-force attacks have constantly been increasing since the outbreak of the COVID-19 pandemic. Kaspersky detected a sharp spike from March 2020, when governments all around the world started imposing stay-at-home orders and lockdowns.

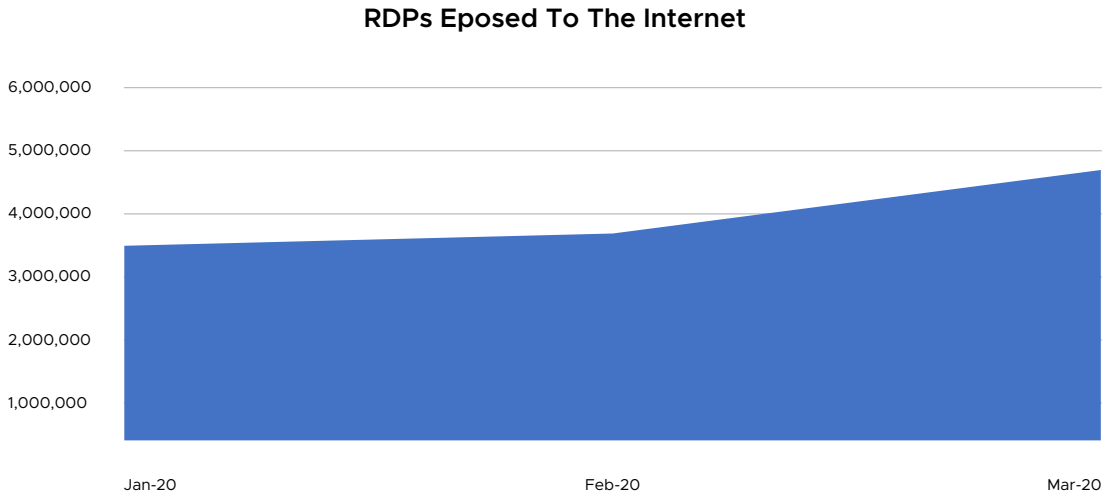


With the world's workforce becoming increasingly decentralized and remote working becoming the new norm, it all comes down to IT administrators and decision makers to implement effective strategies that reduce the organization's attack surface.

What's worse: Open RDP or close up shop?

The surge in telework adoption has caused increased use of Microsoft's Remote Desktop Protocol. RDP helps employees gain access to their work computers—its files, specifically—remotely, i.e., from home. RDP is also commonly used by tech support teams to access employees' remote machines and virtual desktops for troubleshooting purposes. Put simply, RDP enables IT teams and employees to establish a secure remote network connection to Windows-based servers, desktops, and virtual machines (VMs).

However, using RDP systems online comes with its own sets of risks, particularly because open or unguarded remote desktops can quickly be leveraged as a point of entry by hackers. If your organization's RDP port is left open, anyone can find the open port and attempt to access it via the internet. A recent analysis by the Department of Homeland Security discovered a whooping 127 percent increase in exposed RDP endpoints.[2]



Remote desktops are a tempting target for cybercriminals, as they are widely used in enterprise environments. Once an RDP endpoint is breached via brute-force or any other credential-based attack, it can be used for a variety of malicious activities.

RDP brute-force attack in action

1. Hackers use network scanners like Masscan to identify IP and TCP port ranges used by RDP servers.

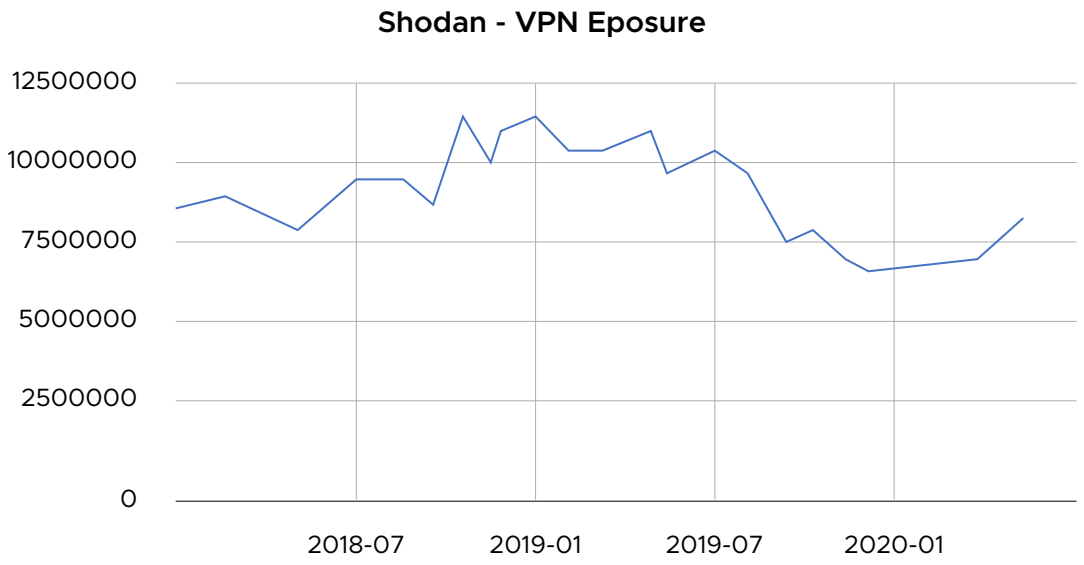
2. Once the open port is identified, hackers use brute-force tools to execute countless logins with multiple user credentials for a specific user account.

3. Hackers eventually crack the targeted user credentials and become capable of compromising not only that machine, but also the information across the organization's network.

Note:
Notably, Masscan, the mostly widely used tool for executing RDP brute-force attacks, is known to scan the entire internet in less than six minutes.

VPN exploits on the rise

Global enterprise IT departments rely on virtual private networks (VPNs), a critical service, to improve the connectivity and security of systems. Due to their broad spectrum network access, VPNs have been a popular point of entry to networks for cybercriminals. Once they are on the network remotely, a cybercriminal can scan for other vulnerable machines, and proceed to wreak havoc.



Due to the COVID-19 outbreak, VPN solutions have become indispensable for employees who need to access their resources on their organizations' internal networks. As a result, network access via VPNs have become the focus of cybercriminals. Recently, Russian cybercriminals reportedly published a list of plain text usernames and passwords, along with IP addresses for more than 900 Pulse Secure VPN enterprise servers.[3] With stolen credentials ranking among the top data breach vectors, it's no surprise that cybercriminals are using brute-force and password spray attacks to try and breach into an employees' VPN accounts.

Security and remote workforce

Gartner estimates that only 12 percent of organizations globally are truly prepared for a disaster such as a pandemic, and the Federal Emergency Management Agency's (FEMA) research highlights that 40-60 percent of small businesses never recover following a disaster.[4,5] This information only solidifies the fact that IT admins need to come up with a foolproof strategy to deal with malicious RDP and VPN activities, and fast.

How ADSelfService Plus can help

ManageEngine ADSelfService Plus is an integrated self-service password management and single sign-on solution for Active Directory (AD) and cloud applications. It offers multiple features to deal with RDP and VPN brute-force attacks, and secure network access with advanced password controls and multi-factor authentication (MFA).

Steps to develop immunity against the imminent cyber pandemic

In this section, we'll cover the steps IT admins could follow to secure remote access to sensitive network resources with ADSelfService Plus.

STEP 1:
Enforce MFA for major operating systems

Credential-based attacks like brute-force on RDPs are successful when IT admins only use AD domain credentials to secure access to their employees' machines. With ADSelfService Plus, IT admins can ensure employees first authenticate themselves with their AD password, and then through any of the supported authenticators like biometrics or YubiKey before they can access their machine. ADSelfService Plus supports endpoint MFA for Windows, macOS, and Linux local and remote endpoints to effectively thwart all credential-based attacks.

SUPPORTED AUTHENTICATORS:

- Security questions and answers
- SMS and email verification codes
- Google Authenticator
- Duo Security
- RSA SecurID
- RADIUS
- YubiKey Authenticator
- Push notifications
- Fingerprint authentication
- QR code-based authentication
- Time-based one-time password (TOTP)
- AD-based security questions
- Microsoft Authenticator

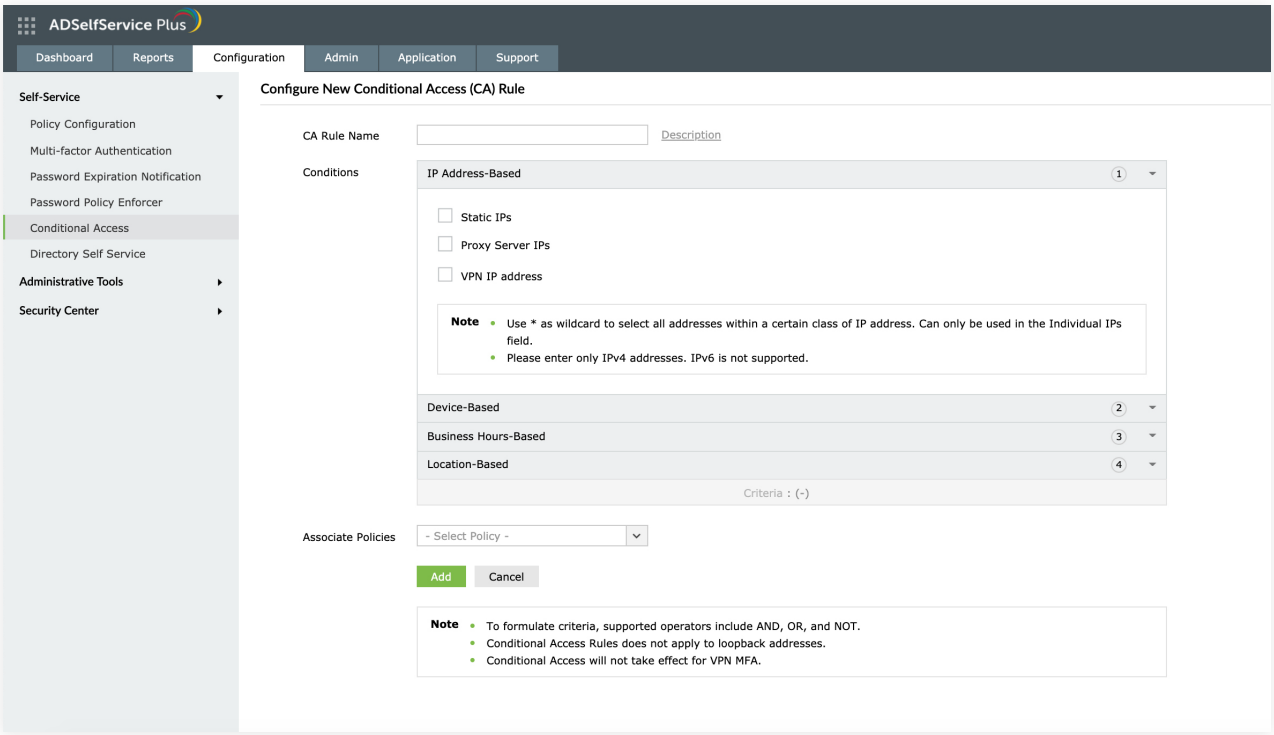
STEP 2:
Enforce conditional access to resources

ADSelfService Plus' Conditional Access Rules ensure only authorized users have access to workstations, applications, and various features that are available in ADSelfService Plus, including Change Password and Directory Self-Update.

ADSelfService Plus' Conditional Access feature also considers risk factors such as:

- **IP address:** Controls access based on the IP address of the user. IT admins can configure static IPs, proxy server IPs, and VPN IPs.
- **Device:** Controls access based on the computer object and the platform (Windows, macOS, Linux, mobile web app, or mobile native app) they run on.
- **Business hours:** Controls access based on business hours or non-business hours.
- **Geolocation:** Controls access based on the location from where the request originated.

For example, say the entire finance team is located in one particular part of the city in a country. IT admins can create a Conditional Access Rule to ensure that access to finance-related applications are only from the country the finance team is located, and only during the defined business hours. Put simply, ADSelfService Plus helps admins differentiate between high risk and low risk resource access requests by enforcing access policies based on the supported risk factors.

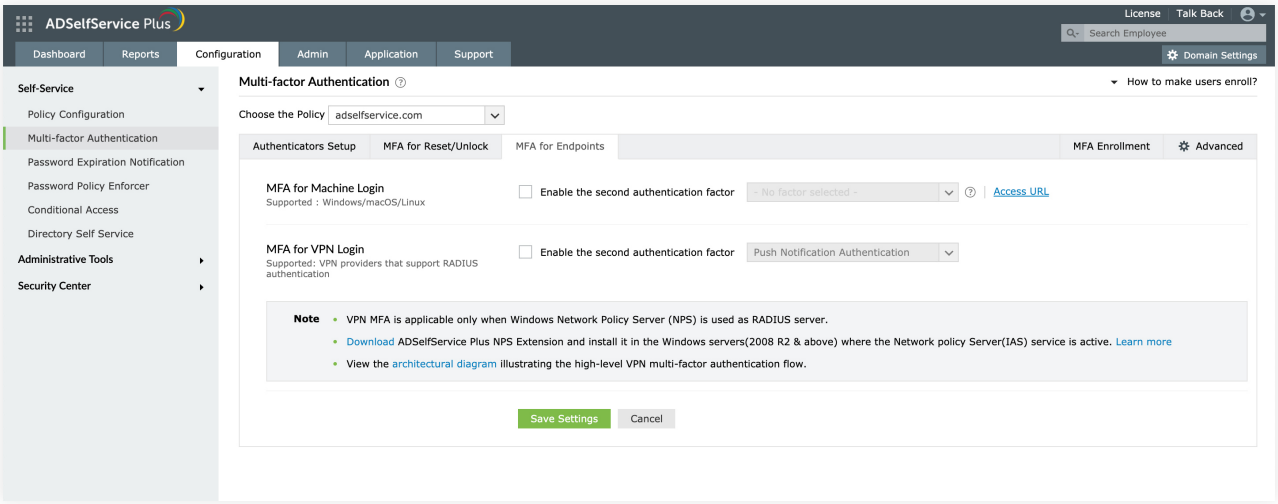


STEP 3:
Enforce VPN MFA

In compliance with the US Department of Homeland Security recommendations, ADSelfService Plus helps prevent attackers from using compromised credentials to access VPN servers with MFA. Only after the employee first proves their identity by entering their password, and next through the enforced authenticator techniques, are they granted access to the VPN server to establish an encrypted tunnel to the internal network.

SUPPORTED VPN AUTHENTICATION METHODS:

- Push notification
- Biometric authentication
- Time-based one-time password (TOTP) authentication
- Google Authenticator
- Microsoft Authenticator
- YubiKey Authenticator

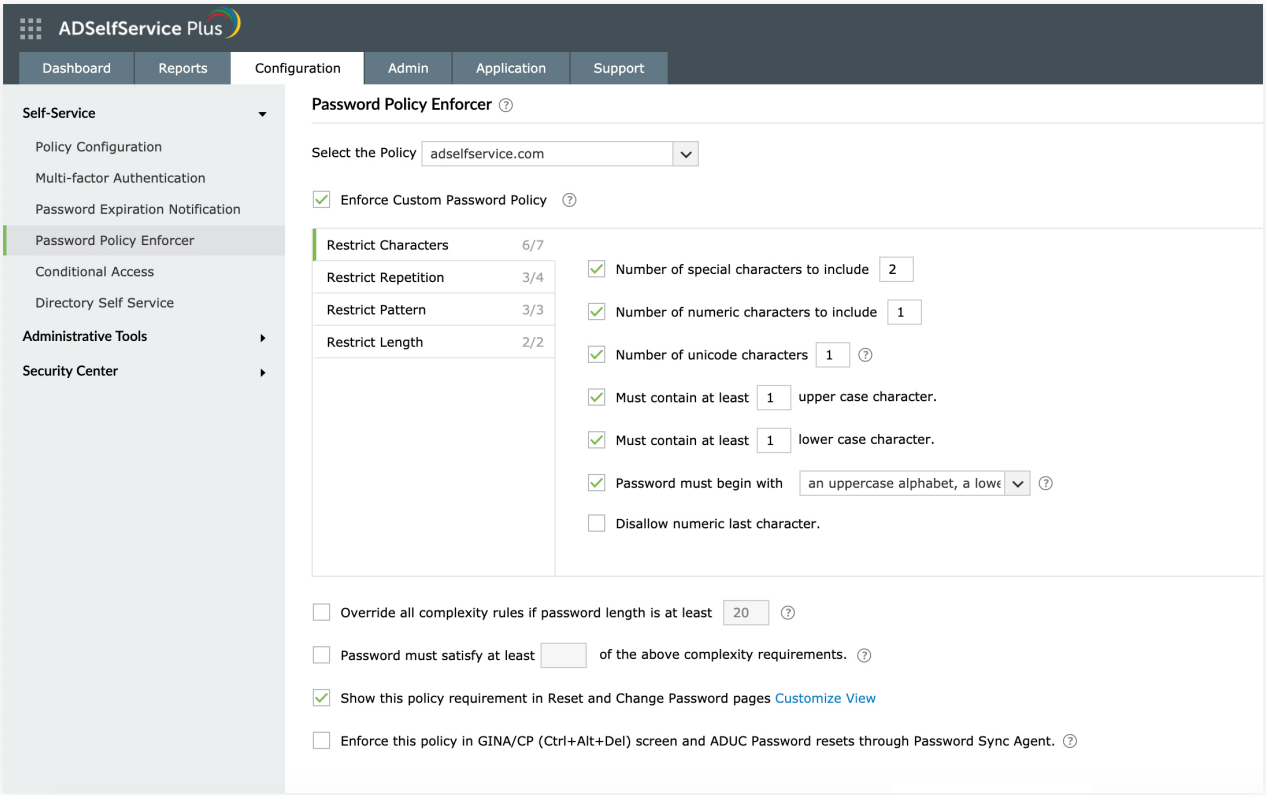


STEP 4:

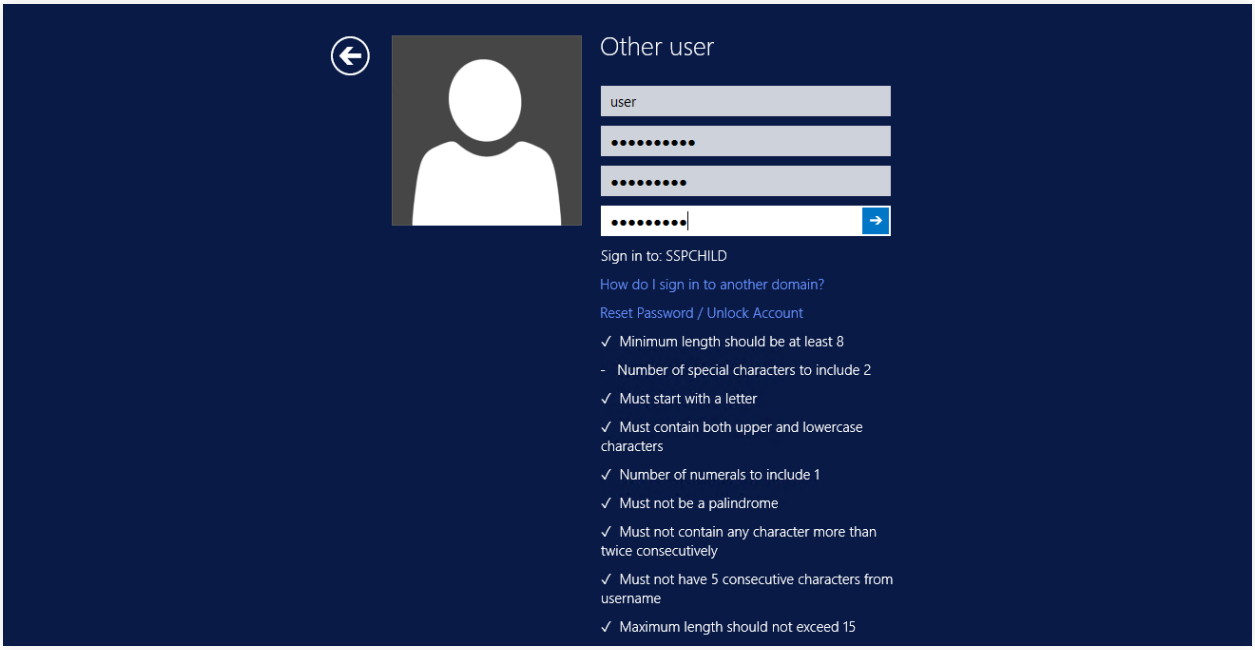
Ensure usage of strong user passwords

Passwords are the first line of defense for most organizations. However, due to password fatigue, employees are prone to use weak passwords or reuse their old passwords across multiple applications.

To help users practice password hygiene, ADSelfService Plus allows admins to enforce advanced password policy controls like banning weak passwords, dictionary words, palindromes, breached passwords (on integration with Have I been Pwned API service), keyboard sequences, old passwords, encourage passphrase usage, and more.

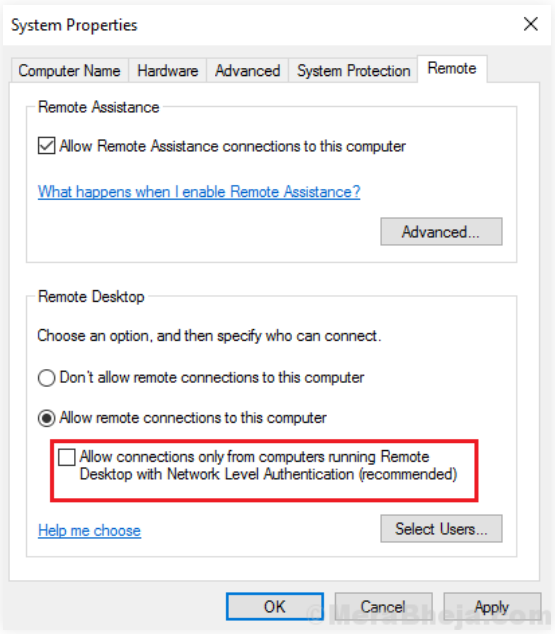


Admins can also enforce custom password policies for users' AD and cloud applications accounts, based on their organization unit (OU), group, or domain membership.



STEP 5:
Other considerations

1. Implement an account lockout policy that differentiates user logins from hackers during password login and password reset to tackle brute-force attacks.
2. Ensure that you disable the RDP services unless required.
3. Install patches for any affected machine as quickly as possible.
4. Enable Network Level Authentication (NLA).



5. Change the RDP port number from the default port value (TCP 3389).
6. To limit the number of services that can be accessed via the internal network, place the RDP servers behind a demilitarized zone (DMZ) or other restricted area of the network.

Conclusion: Post the corona outbreak, organizations are still adjusting to radical changes like large-scale remote work. Using RDP and VPN enables agility, but with cybercriminals actively seeking to exploit vulnerabilities, IT teams must be extremely aware of their pitfalls and effectively work to mitigate threats they introduce to the business.

Footnotes

1. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/
2. https://www.us-cert.gov/ncas/alerts/aa20-099a
3. https://inside.com/campaigns/inside-security-2020-08-05-23996/sections/202280
4. https://www.gartner.com/en/newsroom/press-releases/2020-03-10-gartner-business-continuity-survey-shows-just-twelve-percernt-of-organizations-are-highly-prepared-for-coronavirsu
5. https://www.fema.gov/media-library-data/1441212988001-1aa7fa978c5f999ed088dcaa815cb8cd/3a_BusinessInfographic-1.pdf