STATE OF **REMOTE ACCESS** SECURITY REPORT

REALVNC®

TABLE OF CONTENTS

ABOUT THIS REPORT

It's no secret that cybercriminals make use of both externally- and internally-accessible Remote Access solutions during cyberattacks. It's also no secret that, when thinking about the use of Remote Access solutions, organizations' initial concerns are usually regarding performance, user experience, features, and functionality. Only after that do they realize it's important to also make certain there are security controls in place. And in the landscape of today's cyberthreats, it's no longer possible for organizations to make Remote Access' security stance an afterthought.

Today, Remote Access needs to be as secure as it is fast and feature-rich.

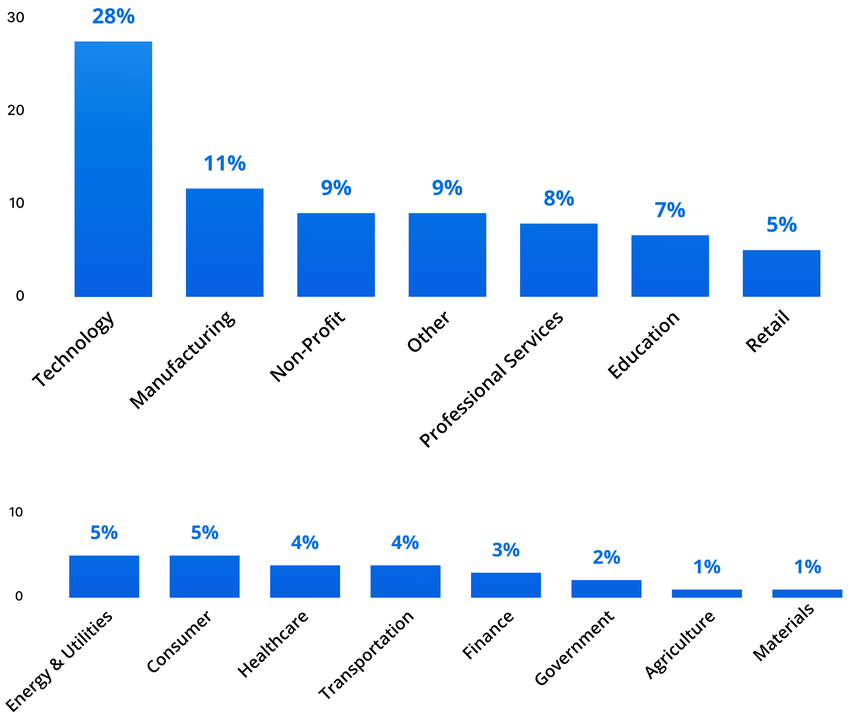
To provide context around the current state of Remote Access and its impact on organizations' cybersecurity stance, we surveyed over 450 IT professionals. We wanted to shed some light on what kinds of technologies are in use to both facilitate remote access and secure it, how those technologies are being practically used by organizations, how the remote access is being secured, and what the result of these choices is when faced with cyberattacks that commonly take advantage of Remote Access.

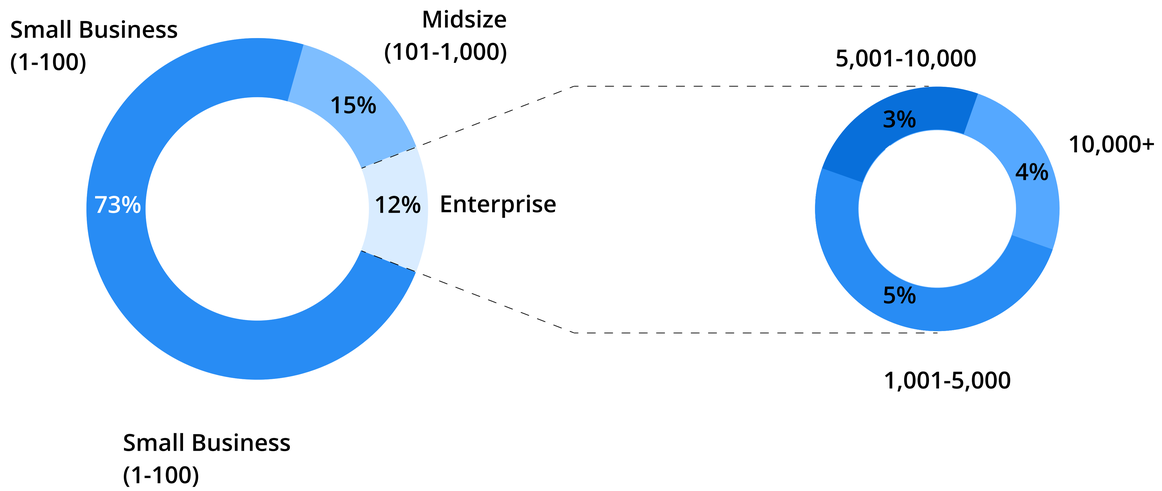
"...it's important to also make certain there are security controls in place"

ABOUT THE RESPONDENTS

We surveyed over **450 organizations from 62 countries** all over the planet, with the greatest number of respondents from the **United States (46% of respondents), Canada (8%), the United Kingdom (6%), and Australia (3%)** participating in this year's report.

Response by organization size (shown at right) provided us with a solid representation of organizations of every size using standard breakpoints for small, midsized, and enterprise organizations. Remote Access is used by every type of organization, regardless of industry, as demonstrated by the over 50 industry verticals represented in this report.





"Remote Access is used by every type of organization"

ABOUT THE CONTRIBUTORS

RealVNC®

RealVNC® Connect is the world's most secure remote access solution. Over 90,000 companies trust RealVNC® Connect as their solution for reliable, secure remote IT access. RealVNC® is the “no regrets” remote access platform for engineers looking for the most reliable and the most secure solution. Intentionally built different by the creators of VNC® technology. Over the last 25 years, as the inventors of VNC®, we've enabled a global workforce to work wherever works and created the remote access market.

Nick Cavalancia

Nick Cavalancia is a 4-time Microsoft Cloud and Datacenter MVP, has over 28 years of enterprise IT experience, is an accomplished consultant, speaker, trainer, writer, and columnist, and has achieved industry certifications including MCSE, MCT, Master CNE, and Master CNI. He has authored, co-authored and contributed to dozens of books on various technologies. Nick regularly speaks, writes, and blogs for some of the most recognized tech companies today on topics including cybersecurity, cloud adoption, business continuity, and compliance.

Conversational Geek

Conversational Geek is a publisher of content for the IT professional. Leveraging the expertise of its long bench of IT practitioner-experts. Conversational Geek creates educational content that assists IT pros to better understand the ever-changing nature of the IT landscape. For more educational content, visit conversationalgeek.com

20

STATE OF REMOTE ACCESS SECURITY REPORT

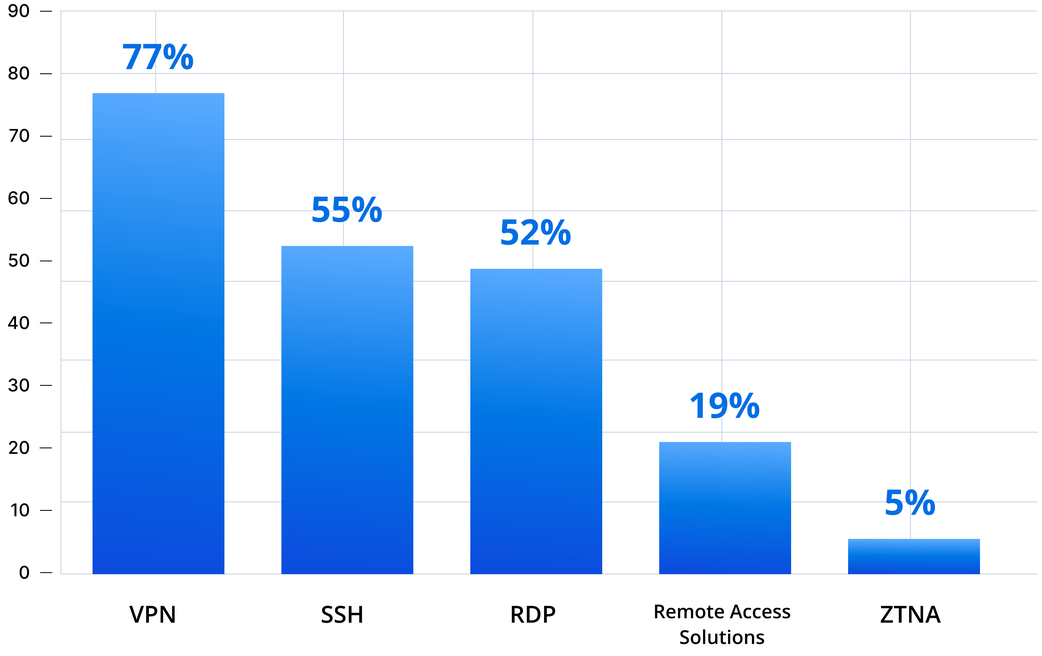
23

REALVNC®

WHAT TECHNOLOGIES ARE BEING USED TO PROVIDE REMOTE ACCESS?

Most organizations are either using a Remote Access solution to provide both the connectivity to the corporate network and remote desktop or are first connecting via VPN and then either leveraging their local apps or connecting to a virtual desktop. As shown below, over three-quarters (77%) of organizations are using a VPN. SSH is widely used, with more than half of organizations (55%) using it to connect to Unix/Linux systems.

Despite RDP playing a documented role in 95% of cyberattacks [1], its use persists in slightly more than half of organizations. Small business represents the lion's share of organizations indicating they still use RDP, while both the midmarket and enterprise are still at risk, given a rather unhealthy representation of RDP in each of those segments. About 1 in five organizations are using a third-party remote access solution, which comprised a wide range of products, including RealVNC®.



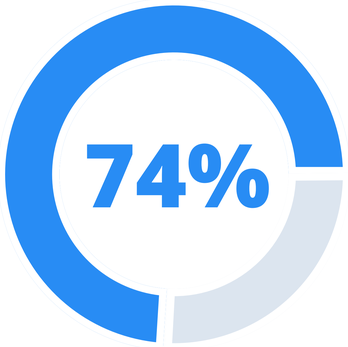
Zero Trust Network Access was predominantly found in use in the enterprise, with most less sizable organizations still relying on tried-and-true solutions to provide remote access.
It's important to note that organizations are using more than one technology and are likely taking advantage of the secure connections provided by VPNs and ZTNA solutions, and then using remote session products and platforms to provide remote access.

We also asked organizations to specify (if applicable) any remote access solutions they may be using. Solutions like TeamViewer, RealVNC® Connect, various open-source VNC solutions , and AnyDesk topped the list.

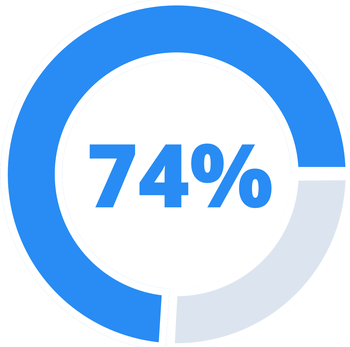
[1] Sophos, Active Adversary Report for Tech Leaders (2023)

WHO'S USING REMOTE ACCESS AND WHAT'S IT BEING USED FOR?

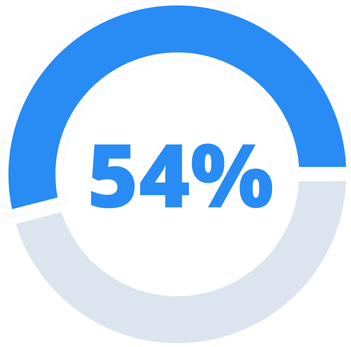
Nearly three-quarters (74%) of organizations said their IT users utilize some form of Remote Access, while 61% said non-IT users also utilize Remote Access. As shown below, the use cases for Remote Access are an even match between the remote use of internal resources by both external and internal users, while remotely accessing cloud resources from an internal user slightly outweighs their external counterpart. The Technology, Manufacturing, and Education sectors led the way for all four scenarios below.



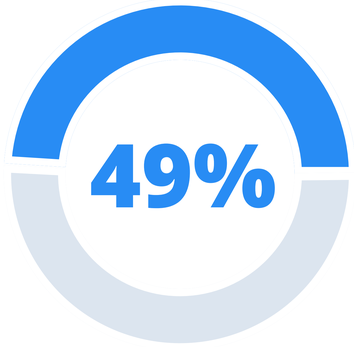
Externally-Remote User to Internal Resources



Internally-Remote User to Internal Resources



Internally-Remote User to Cloud-based Resources

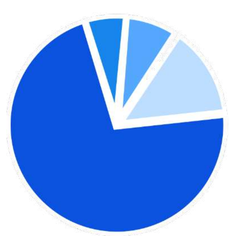


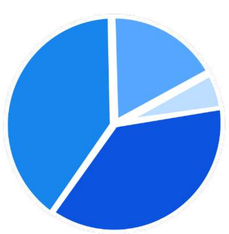
Externally-Remote User to Cloud-based Resources

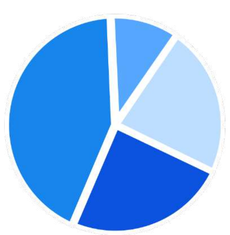
Organizations are using a wide range of operating systems to facilitate remote access as either the remote client, the remote host, or both. The following chart lists the operating systems used as client, host, or both, in descending order. It's no surprise Windows and Linux lead the charge as the most often used operating systems for remote access. Besides being used in tech, Raspberry Pi was surprisingly found most used in the smallest parts of the SMB, as well as in the Non-Profit, Consumer, Education, and Professional Services industries.

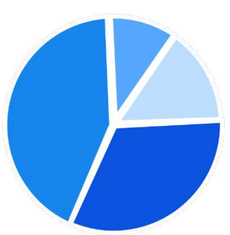
WHICH
OPERATING SYSTEMS
are used with remote access?

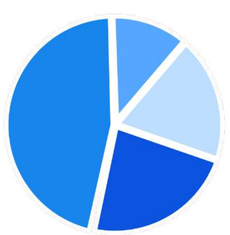
client, host, or both?

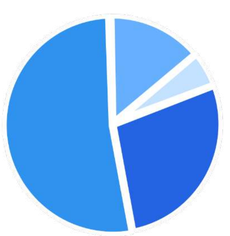










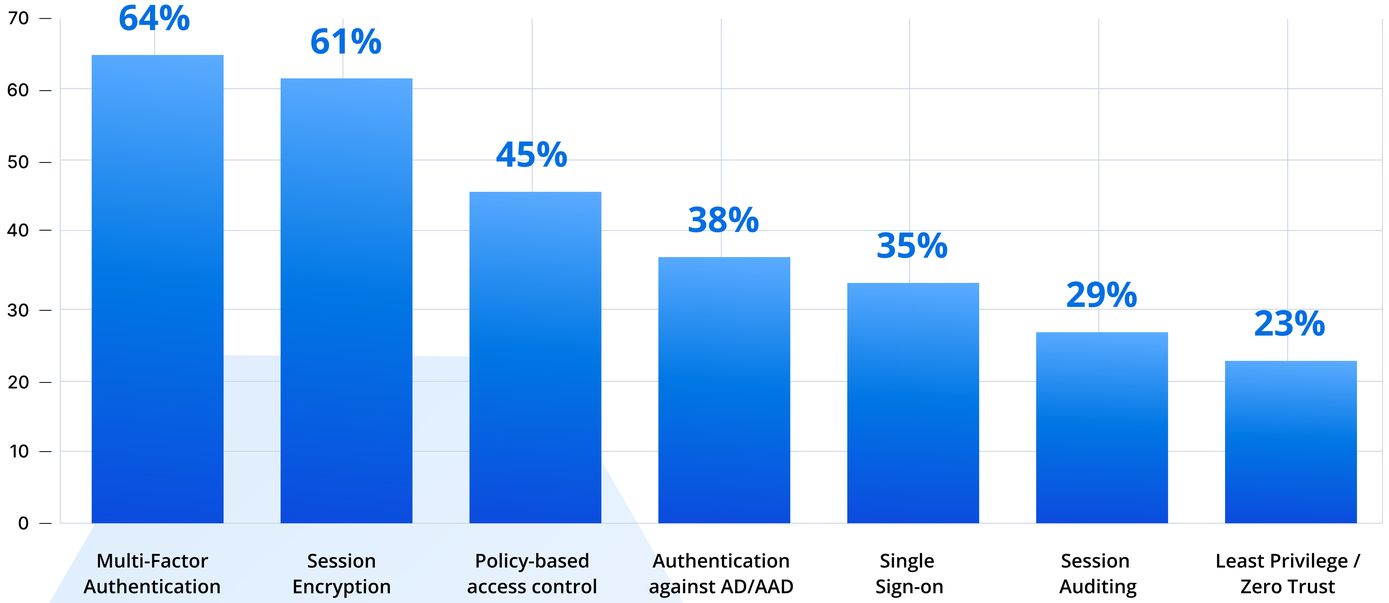


Host Client Both N/A

WHAT SECURITY CONTROLS ARE BEING USED OVER REMOTE ACCESS?

An organization's state of security is an ever-present concern, so the threat surface Remote Access presents requires that it be paired with one or more security controls layered on top of the Remote Access itself. Multi-factor authentication (MFA) and session encryption were the two most used security controls, providing organizations with assurance that the user of a credential is the owner of the credential, as well as that the session and its data remained secure. We were a little perplexed by the much lower usage of both authentication against AD and use of single sign-on solutions, as MFA needs to be paired with some authenticating authority.

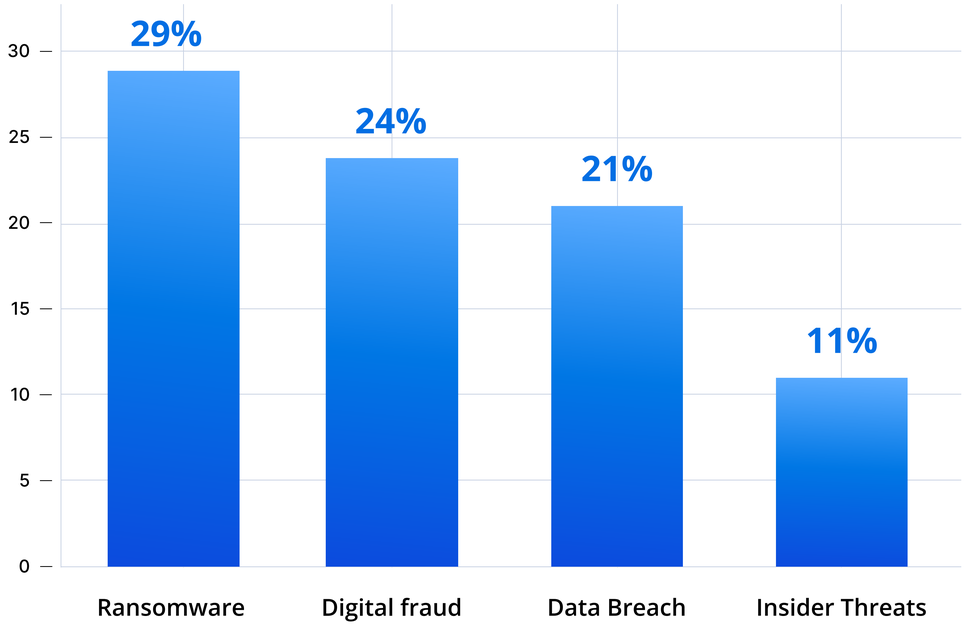
We were also a bit surprised to see less than half of organizations setting up access control policies to lock down the mix of remote users, the systems to be accessed, and the level of privilege to be exercised during a given session. This, mixed with MFA provides organizations with a good amount of control to reduce the cyberattack risk that Remote Access presents.



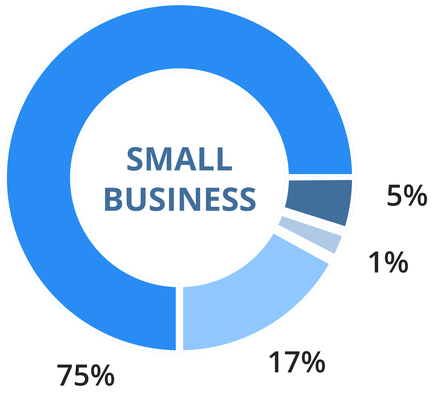
It should be no surprise that Enterprise-sized organizations used these security controls most, with an average of just under 3.5 controls in place. Small Business organizations used the controls the least, with an average of just over 2 controls in place. Industries with the most controls in place on average were Materials (5), Government (3.75), and Transportation (3.35).

WHO IS EXPERIENCING CYBERATTACKS?

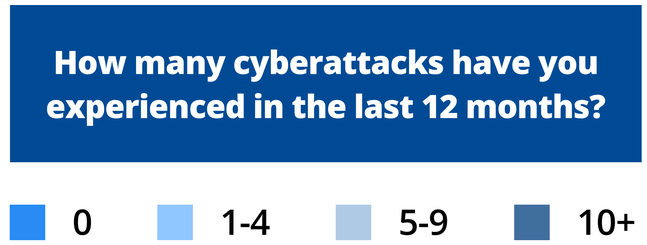
Let's first establish who is experiencing cyberattacks, followed by the types of attacks experienced, and then see if/how Remote Access played a role. As shown below, the Small Business sector has experienced the smallest number of cyberattacks (as a percentage) in the last 12 months in any of the segments below. Enterprise organizations, on the other hand, are experiencing the most cyberattacks across the board, with 15% of them experiencing ten or more attacks in a 12-month period.

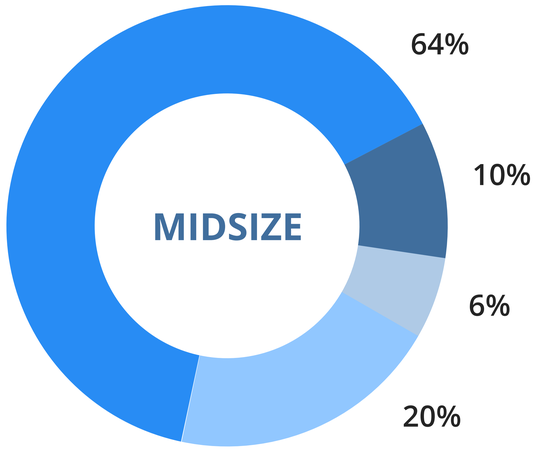


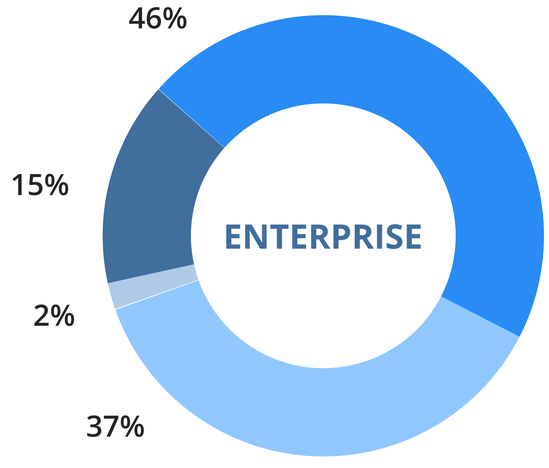
Of those experiencing one or more cyberattacks, we asked which types of attacks were ones in which remote access could have played a role. To no surprise, ransomware was the top cyberattack type experienced by organizations.



How many cyberattacks have you experienced in the last 12 months?

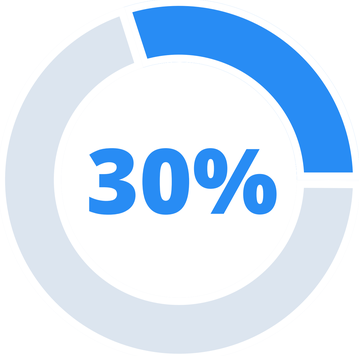




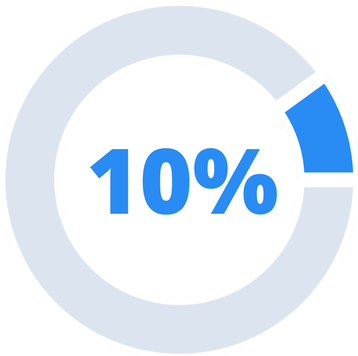


WHAT ROLE DOES REMOTE ACCESS PLAY IN CYBERATTACKS?

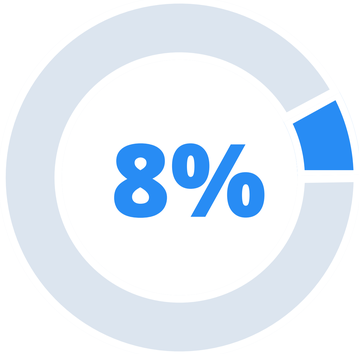
Of those organizations experiencing one or more cyberattacks in the last 12 months, 70% said Remote Access did not play a role. That seems a little low to us, given that industry data suggests that RDP-based remote access (something 52% of respondents say they use) has been (and remains) a top initial attack vector in ransomware attacks since 2018 through today[2], and used for internal access and lateral movement in 77% of all cyberattacks[1]. Of the other 30% that did see the organization's own Remote Access solution(s) involved in cyberattacks, it was used in the following ways:



Initial Access



Lateral movement



Data Exfiltration

It appears that the greatest concern here should be the misuse of Remote Access in the initial access portions of cyberattacks (something corroborated by previously mentioned industry data), keeping in mind that facilitating lateral movement and the exfiltration of data is equally harmful to the organization (and, again, is something demonstrated to be a valid concern based in industry data).

Of the organizations that saw Remote Access playing any of the three roles above:

- **45% of them were using RDP as their Remote Access**
- **25% of them had no security controls layered over their Remote Access solution**
- **40% had no MFA implemented, and**
- **63% had no policy-based access control in place.**

It's evident from the data above that Remote Access, in addition to providing a robust remote experience for the end-user, also needs to be far more secure to align with the organization's cybersecurity goals.

[2] Coveware, Quarterly Ransomware Reports (2018-2023)

REMOTE ACCESS RECOMMENDATIONS

Remote Access in and of itself is a productivity play; it's designed, first and foremost, to provide a user with an ability to remotely access the systems, applications, and data they need to accomplish their job. But today's organization cannot responsibly provide users – whether internal or external – with an ability to remotely access systems without considering how Remote Access will impact the organization's cybersecurity stance. To assist in better securing your Remote Access, we offer the following recommendations:

Be Wary of RDP!

Just over half of organizations indicated they were using RDP. If your organization is using the Remote Desktop service and RDP client built into the Windows OS without having also implemented the enterprise Remote Desktop Services (which can employ additional security controls) to facilitate remote access (especially if for external users, but also even if RDP is strictly used for internal access), it's time to stop doing so and look for a Remote Access solution with better security controls.

MFA, MFA, and More MFA

With credential harvesting being the leading goal for most phishing attacks today, it makes sense that the largest use of Remote Access during a cyberattack was during Initial Access; stolen credentials mixed with an externally accessible RDP connection equates to network access.

So, it becomes critical that authentication to any part of the corporate network requires additional factors (regardless of how privileged or low-level a user is) to thwart misuse of compromised credentials or even dictionary attacks. In short, everyone should be required to use MFA at logon.

With Remote Access, Make Security as High a Priority as Functionality

Each of the security controls mentioned in this report add to the organization's cybersecurity posture when it comes to reducing the Remote Access threat surface. The Remote Access solution you choose to use should inherently offer as many of the previously mentioned controls as possible, including authentication against a central identity/single sign-on platform, support for multi-factor authentication, policy-based access control, auditing of privileged sessions, encryption of the remote session communications, and – as organizations move towards establishing and maintaining a state of Zero Trust – added controls the support the Zero Trust initiatives.

Use a Single Solution

While not detailed as part of this report, many organizations are leveraging different solutions for external and internal remote access scenarios. While this may meet the need from a productivity standpoint, it's imperative from a cybersecurity standpoint that organizations use a centralized single solution so that every remote access session is subject to the same sets of security configurations, policies, workflows, approvals, etc.

Find out more and get a free trial of RealVNC® Connect here!