REMOTE ACCESS PREDICTIONS REPORT 2024

REALVNC®

TABLE OF CONTENTS

ABOUT THIS REPORT

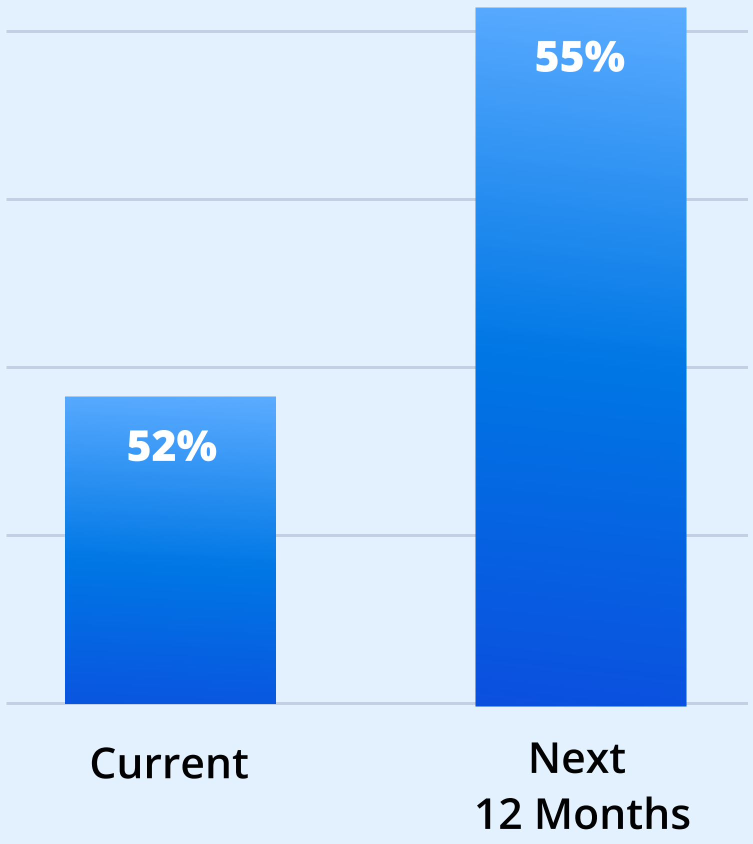
Remote Access has become an essential tool (in various degrees), in every organization. Whether used to provide external users with access to internal or cloud resources, or to elevate the productivity of IT, Remote Access solutions are a necessity in a modern network. At the same time, cybercriminals are well aware of this continual reliance on such solutions and are constantly looking for ways to take advantage of them. This makes ensuring the security of the Remote Access solution just as necessary as is it is to offer the functionality in the first place.

Now that we've established that Remote Access security is a must, what does its future look like?

To provide context around the future of Remote Access security and its impact on the organization's cybersecurity stance, we surveyed over 450 IT professionals, and released the RealVNC 2023 State of Remote Access Report a little while ago. This was designed to shed some light on the kinds of technologies which are in use to both facilitate remote access and secure it, how those technologies are being used in practice by organizations, how the remote access is being secured, as well as what the result of these choices is when faced with cyberattacks that commonly take advantage of Remote Access. We also included some additional questions in that same survey that focus on what organizations see the future of their Remote Access security looking like and why.

Percentage of organisations

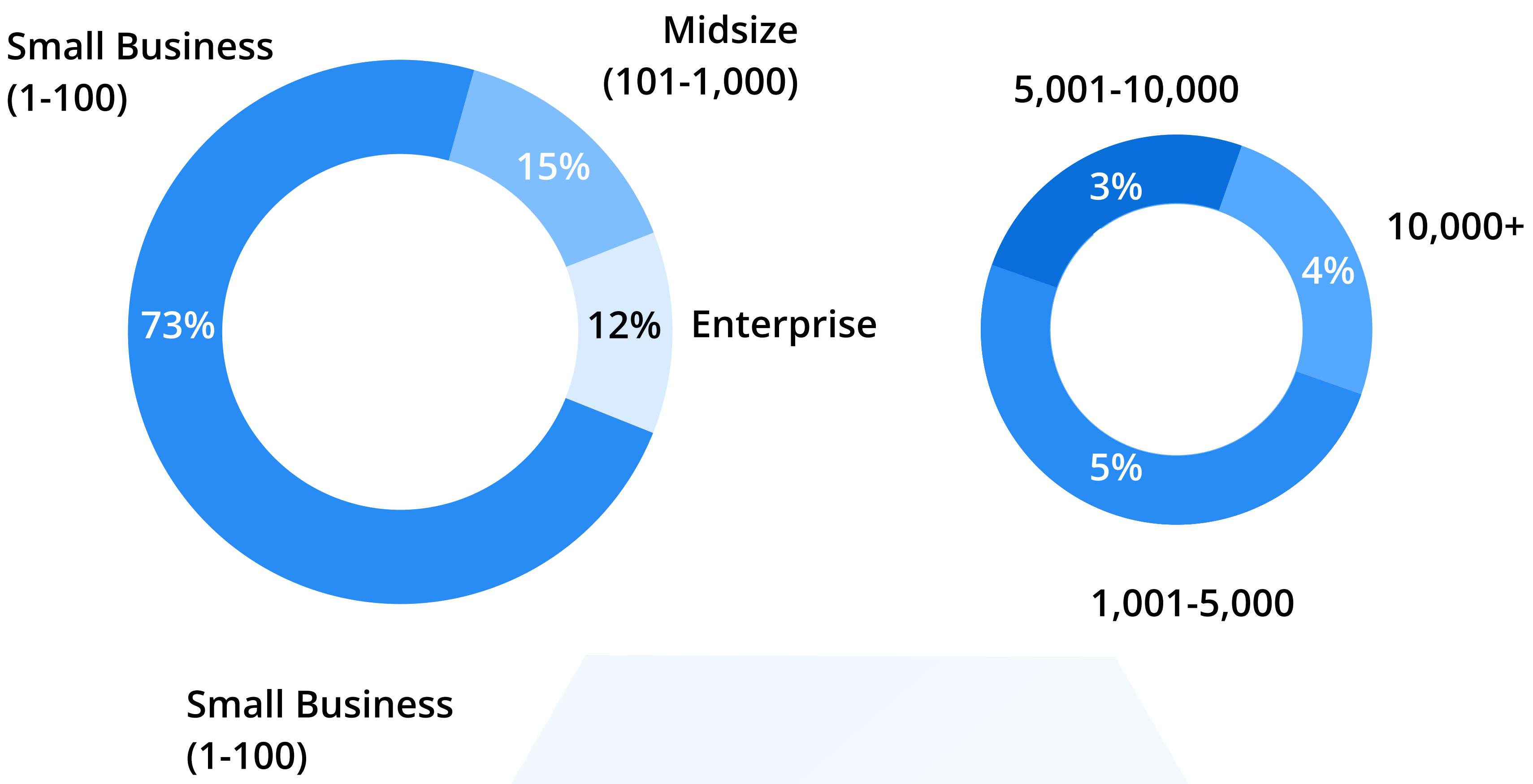
using RDP for Remote Access



NOTE: Most of the charts in this report show what organizations are currently doing and what they are planning in 12 months, as demonstrated below, giving you a point of reference (the current state) to better evaluate the future state of Remote Access (within the next 12 months).

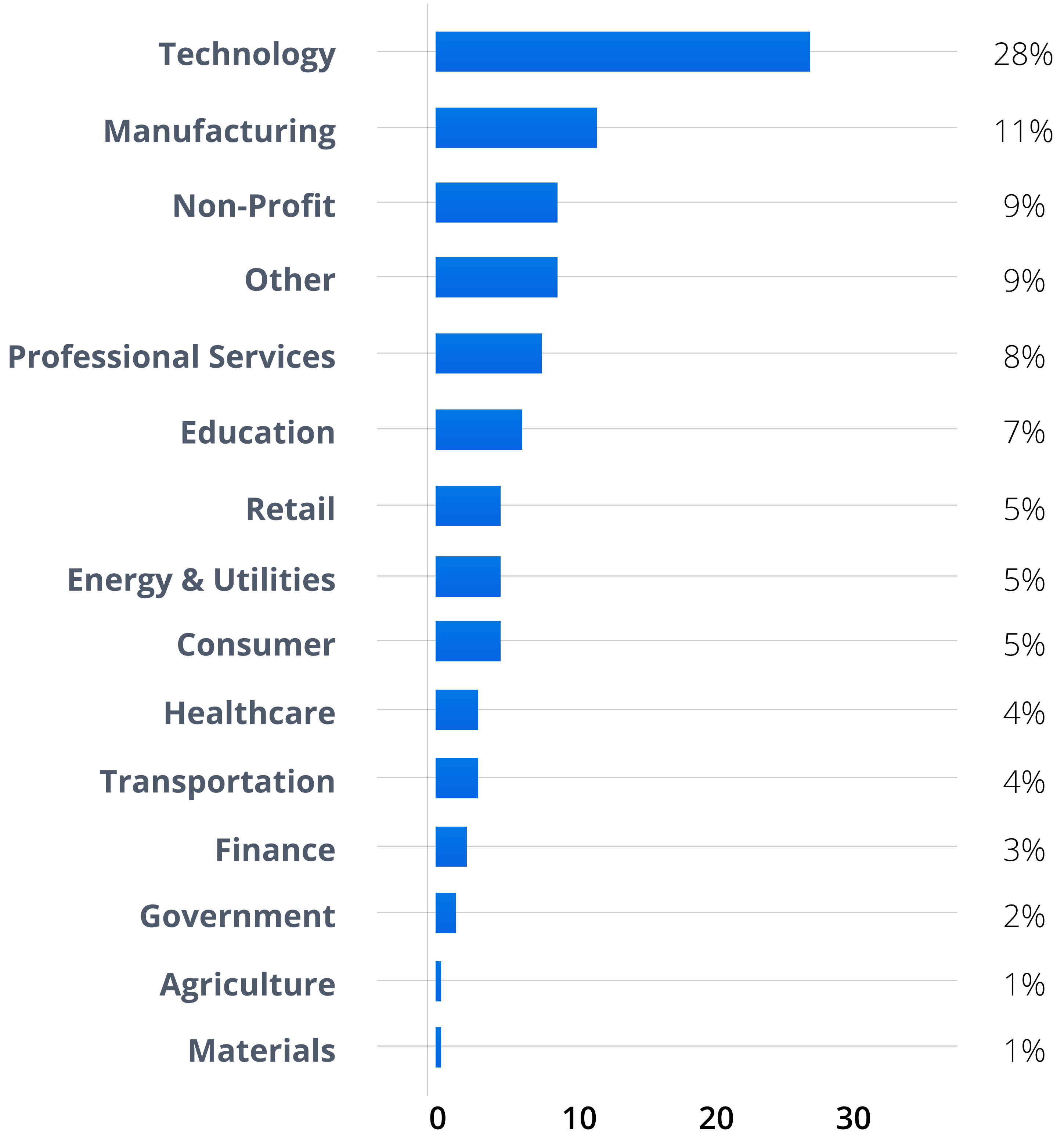
ABOUT THE RESPONDENTS

We surveyed over 450 organizations from 62 countries throughout the globe, 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 below) provided us with a solid representation of organizations of every size using standard breakpoints for small, midsized, and enterprise organizations.



Breakdown of respondents by organization size

Remote Access is used by every organization, regardless of industry – as demonstrated by the over 50 industry verticals represented in this report.



The industry verticals represented in this report

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 quarter of a century, 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

REMOTE ACCESS PREDICTIONS REPORT 2024

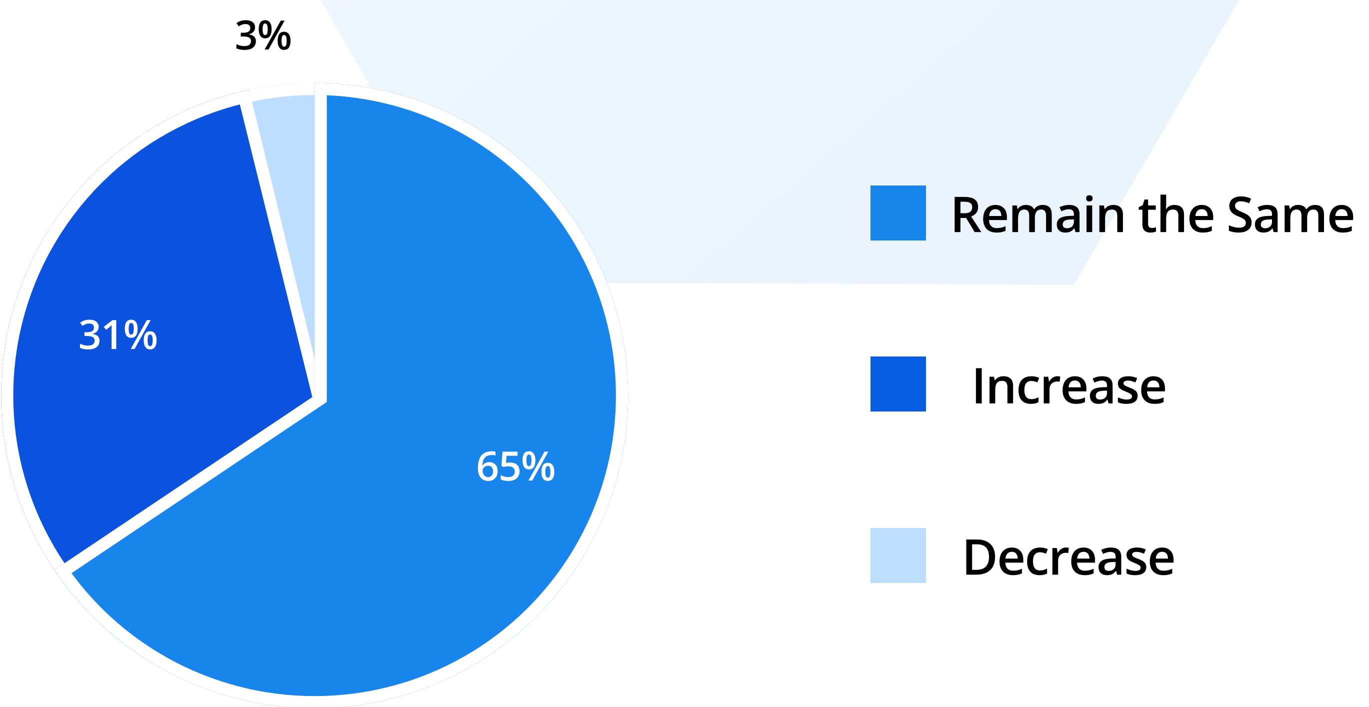
HOW WILL REMOTE ACCESS BE PROVIDED IN 2024?

Let's take a look at the way organizations plan on using remote access this year.

In 2024, nearly one-third (31%) of organizations plan on increasing their use of Remote Access (shown at right), with the vast majority – nearly two-thirds (65%) - planning for their usage to remain at the same levels as today.

So, how will organizations provide Remote Access compared to today?

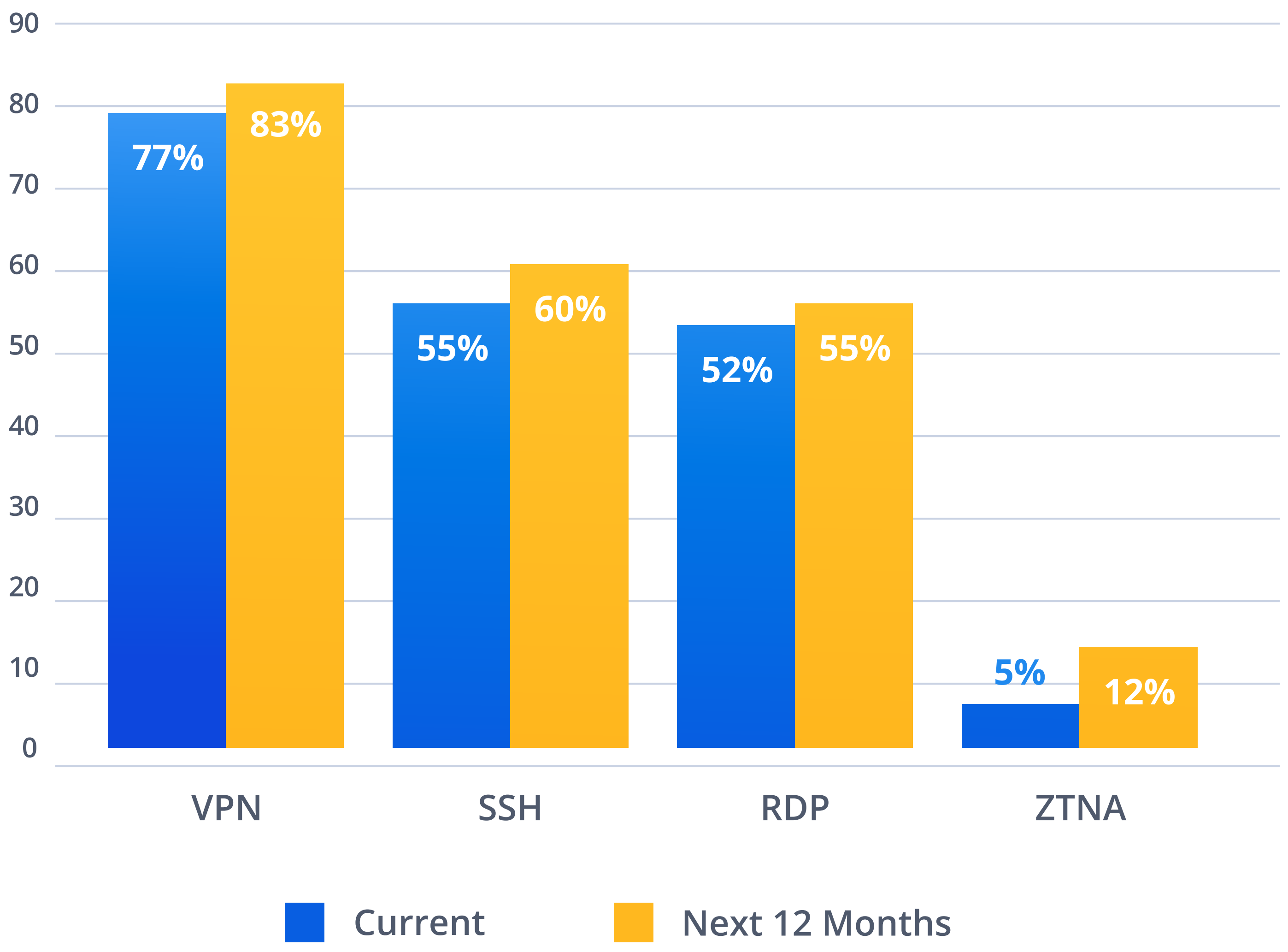
Organizations across all industry verticals are generally planning on doing "more of the same". As shown below, they plan to increase the use of whatever remote access technologies they currently have in place.



How will your use of Remote Access change in the next 12 months?

Not surprising are the increases seen in the use of VPNs and SSH. But, given the documented rising misuse of RDP in both initial access and lateral movement actions within cyberattacks, it's surprising to see the use of RDP not just continue, but actually see the reliance on it increase in 2024.

The largest planned increase (based on percentage growth) is that of Zero Trust Network Access. Found increasing primarily in Enterprise organizations, the growth represents more than a doubling of the number of organizations that currently use it today versus those that plan on implementing it within the following 12 months.



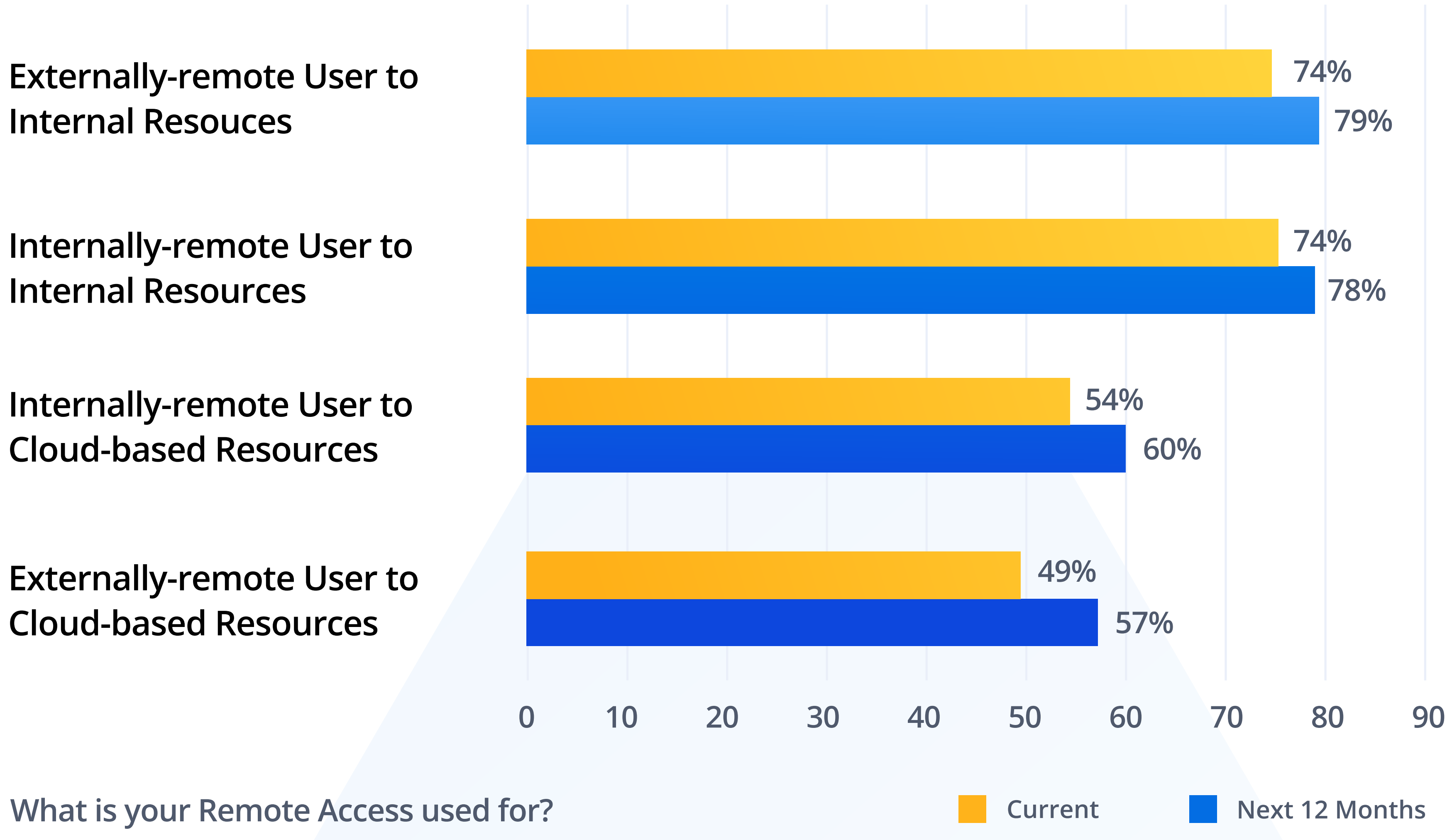
What type(s) of remote access do you currently rely on?

This "doubling down" of using the same technologies – particularly RDP and VPN – may actually increase an organization's cybersecurity risk, as 70% of initial access being sold on the Dark Web are credentials to be used over either VPN or RDP[1].

[1] Group-IB, Hi-Tech Crime Trends 2022-2023 (2023)

WHO WILL BE USING REMOTE ACCESS AND WHAT WILL IT BE USED FOR?

More than three-quarters (77%) of organizations said they plan for their IT users to utilize some form of Remote Access in the next 12 months. At the same time, 65% said non-IT users will also utilize Remote Access. The previously mentioned planned increase in the use of Remote Access is demonstrated by the chart below, as more organizations plan on leveraging it for all four of the use cases we presented.

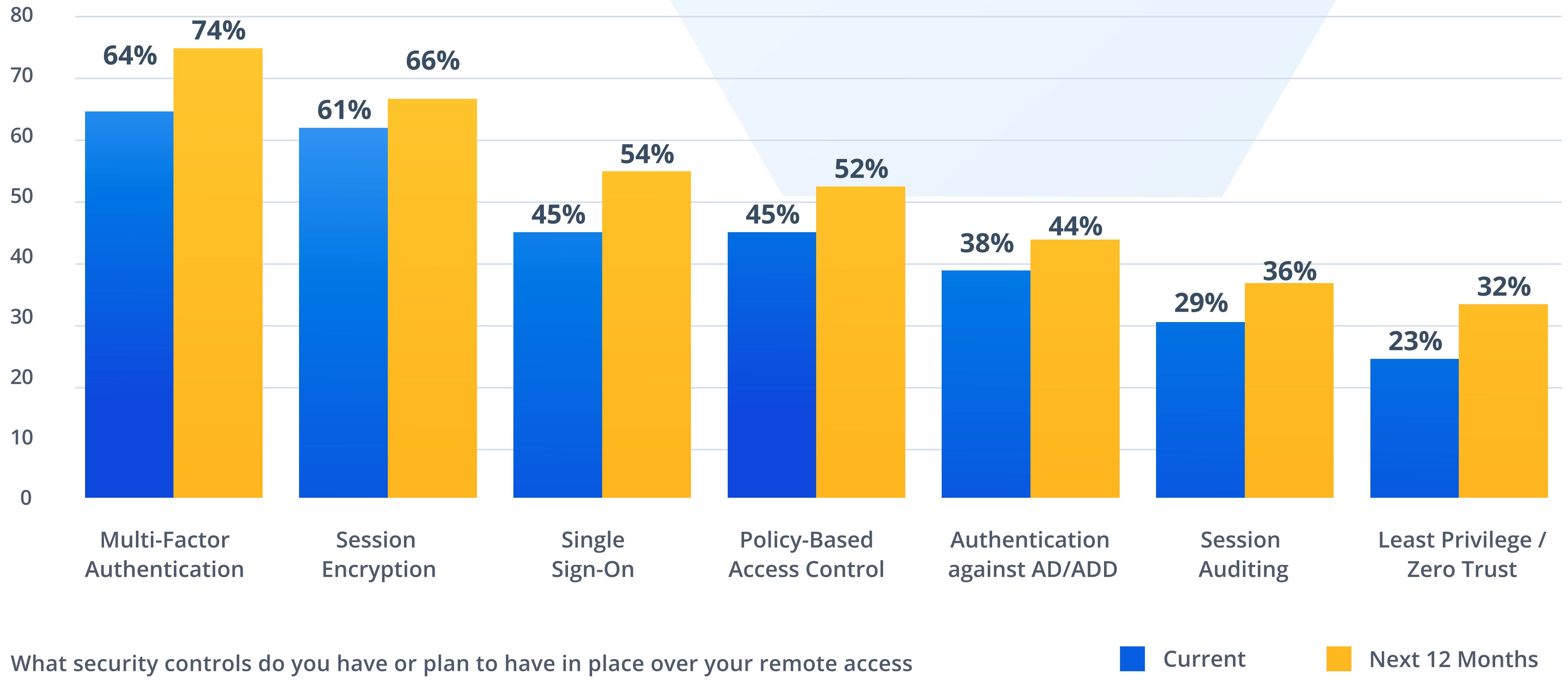


The Small Business segment represents the lion's share of the growth in all the use cases above, with nearly all Midmarket and Enterprise organizations continuing to use Remote Access to support the same uses they do today. Given that in all four use cases Remote Access will continue to be used to provide users with access to either internal or cloud resources, it's imperative that we see security controls used in increasing measure – especially in "Externally-Remote User" scenarios, as the amount of credentials being sold on the Dark Web providing threat actors with initial access from outside the organization's network has grown by 146% in the last 12 months[1]. The addition of security controls around Remote Access will help to ensure that cybercriminals have as little a chance of successfully misusing Remote Access for either external or internal use as possible.

[1] Group-IB, Hi-Tech Crime Trends 2022-2023 (2023)

WHAT SECURITY CONTROLS WILL BE USED OVER REMOTE ACCESS?

Due to the risk of misuse, Remote Access can't exist in a bubble. It needs to be paired with a layered security strategy; this is evident from the presence of several types of security controls used to ensure all aspects of a Remote Access session are secure. As shown at right, organizations plan on increasing the use of security controls with their Remote Access. Multi-factor authentication (MFA) remains a number one priority for organizations, although about one-quarter of organizations still don't see the value in this absolutely "must-have" control that should be implemented for every user within the organization (regardless of use of Remote Access).



What security controls do you have or plan to have in place over your remote access

One unexpected increase was that of the use of Single Sign-On (SSO) solutions across all sizes of organizations. If the SSO solution is merely a productivity play to make accessing a remote session easier, this may put more organizations at risk. This is because of the potential lack of validation resulting from the user of the credential also being its owner. Because of the nature of these solutions providing access to multiple applications and resources, they should be utilizing some form of monitoring of access requests to look for anomalous behavior that could be a leading indicator of a cyberattack. Otherwise, this increase can't be good for organizations.

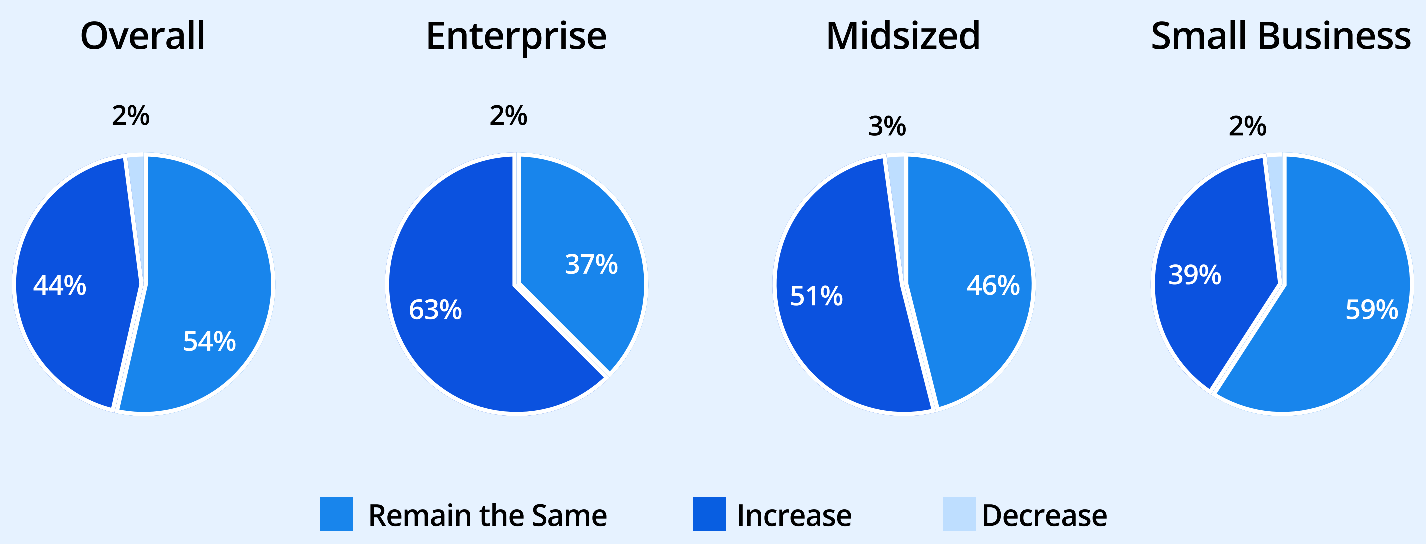
The increase in SSO use could also be related to the largest percentage increase found in the adding of Least Privilege/Zero Trust, seeing as SSO solutions are including such monitoring features to be more security-centric.

In nearly every category, the Midmarket showed the largest percentage of organizations adding on solutions (the exception was Least Privilege / Zero Trust, where the Enterprise dominated).

WILL THE FUTURE OF REMOTE ACCESS ACTUALLY BE MORE SECURE?

While over half (54%) of organizations (shown below) believe that the security state of their Remote Access will remain the same in the near future, a very material 44% feel that, with the added controls and shifts in use of specific Remote Access technologies, the security state of their Remote Access will actually be improved.

How will your changes to Remote Access impact your organization's state of cybersecurity?



As also shown above, it's the Enterprise sector that is most confident in their future state of cybersecurity around Remote Access. 63% of those organizations are stating that their Remote Access security will increase in 12 months.

Just over half of Midmarket businesses are also planning to be more secure (which we'd expect to see, given their previously demonstrated intent to continue to augment security around Remote Access in the previous year). The Small Business sector mostly believes that their Remote Access security stance will remain the same as it is today (and these businesses are doing little to improve it, despite being the largest segment to plan on increasing its use of Remote Access) – a recipe for an increased risk of cyberattack.

So, what steps can you take to mimic the Enterprise and Midmarket organizations that believe their Remote Access will be more secure in 12 months' time?

- Adding at least one additional security control to your Remote Access not currently in use. The two most popular security controls planned to be added onto Remote Access within both market segments are Single Sign-On capabilities, and Policy-based access control, with the Enterprise also adding Least Privilege/ Zero Trust and the Midmarket adding Session Auditing.
- Not increasing the use of RDP as a Remote Access technology. The organizations planning to be more secure have no plans to use more RDP.

IMPROVING REMOTE ACCESS SECURITY TODAY AND TOMORROW

Cybercriminals continue to leverage both built-in Remote Access tools, as well as unsecured third-party Remote Access solutions, during cyberattacks. It, therefore, becomes essential that organizations take steps to increase the state of their Remote Access security for either internal or external use. To assist in better securing the future of your Remote Access, we have the following recommendations:

Seriously, it's Time to Kill RDP

If you don't believe RDP is a security issue, you're not paying attention. RDP has and continues to be a material asset to threat actors in Ransomware attacks[2] (as well as every other type of cyberattack that requires access to a victim network), so seeing that more organizations are planning to use it is downright irresponsible. RDP needs to be replaced for both internal and (especially) external use immediately and replaced with a solution that, by default, includes several of the security controls mentioned in this report.

Continually Augment Your Remote Access Security

The organizations that felt the most confident about the future of their Remote Access security were those that were actively planning on augmenting the security controls that revolve around Remote Access. There are two possibilities for you here:

- You add on security controls that integrate with your current solution
- You need to go shopping for a new solution that offers those controls.

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

IMPROVING REMOTE ACCESS SECURITY TODAY AND TOMORROW (CONTINUED)

Make Security a Priority

This one may seem a little odd, given the demonstrated increases in security control usage documented in this report. While not detailed in this report, we also asked the very same respondents about what criteria they look for in a Remote Access solution. Out of ten presented criteria (one of which was 'Security Features'), guess where security ranked? Third behind 'Speed and Reliability' and 'Ease of Use'. While, yes, a solution that delivers Remote Access needs to provide a great user experience, it also needs to be considered that the offering of such a solution inherently creates risk – risk that needs to be acknowledged, identified, and mitigated before the solution is ever put into production. So, should you find yourself in the position of needing to look for a new Remote Access solution, make sure that security is of equal priority to the solution's actual remote access functionality.

Make Remote Access Happen Using a Single Solution

Many organizations are leveraging different solutions for external and internal remote access scenarios (and even multiple solutions for each use case!). 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.

If you found this report interesting, make sure you Download the 2023 State of Remote Access Security Report for Key Industry Insights!