2021

Cybersecurity
INSIDERS

THE STATE OF REMOTE WORK SECURITY

archTIS

Nucleus Cyber

OVERVIEW

The need to secure the remote workforce has never been more critical. A year into the pandemic, organizations are still grappling with how to protect their assets.

The State of Remote Work Security Report reveals the status of organizations' efforts to secure the new workforce, key challenges, and unique security threats faced by organizations, technology gaps and preferences, investment priorities, and more.

Key findings include:

- Almost three-quarters of organizations are concerned about the security risks introduced by users working from home; despite these challenges, 86% are likely to continue supporting remote work in the future.
- Key security challenges cited include user awareness and training (57%), home/public WiFi network security (52%), and sensitive data leaving the perimeter (46%).
- The applications that organizations are most concerned with securing include, file sharing (68%), the web (47%), video conferencing (45%), and messaging (35%).
- More than half of organizations see remote work environments having an impact on their compliance posture (70%). GDPR tops the list of compliance mandates (51%).
- Organizations prioritize human-centric visibility into remote employee activity (34%), followed by next-generation anti-virus and endpoint detection and response (23%), improved network analysis and next-gen firewalls (22%), and Zero Trust Network Access (19%).

We would like to thank archTIS and Nucleus Cyber for supporting this important cybersecurity research project.

We hope you find this report informative and helpful as you continue your efforts in protecting your organization against evolving threats and during challenging times.

Thank you,

Holger Schulze

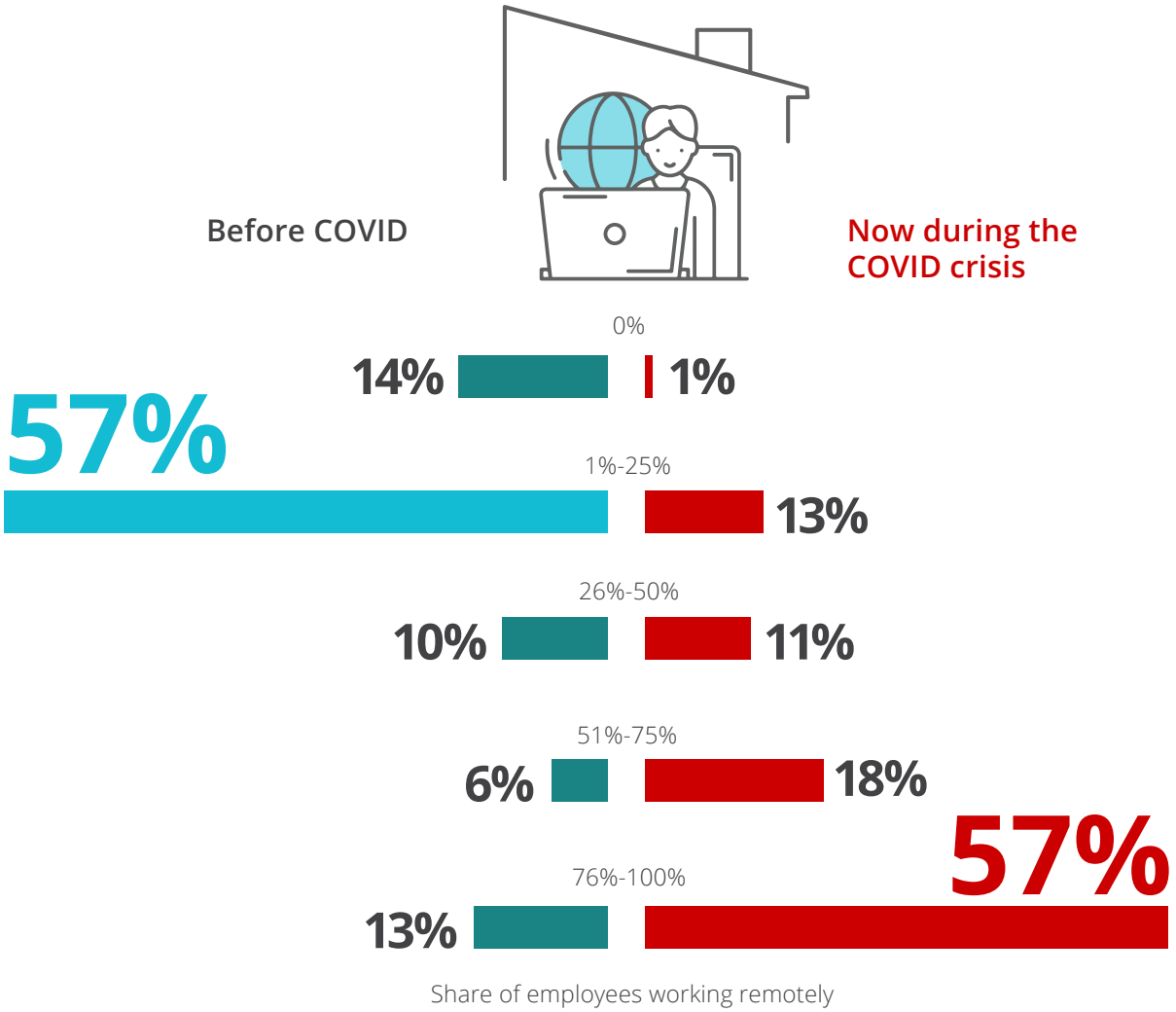
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

DRAMATIC INCREASE IN REMOTE WORKFORCE

It is no surprise that in the last year many organizations have made the shift to a remote workforce. One year into the pandemic, 57% of organizations have over 75% of their workforce remote. A year ago, 57% of organizations report that 25% or less were remote.

What percentage of your workforce is working remotely/at home NOW during the COVID crisis compared to before (on average)?

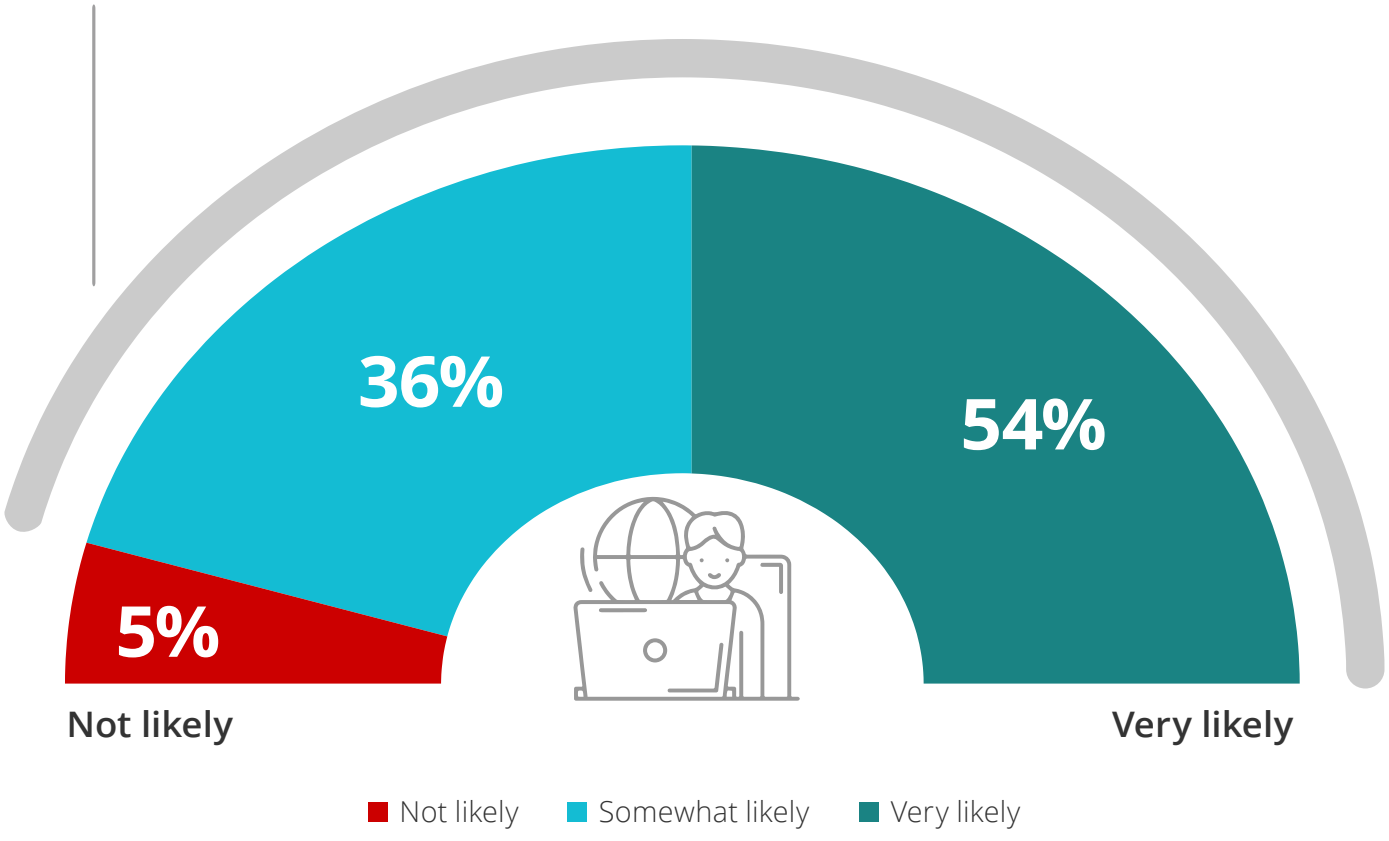


FUTURE OF REMOTE WORK

Many organizations are seeing the benefits of having a remote workforce. Ninety percent of organizations are likely to continue remote working in the future.

Do you expect to continue to support increased work from home capabilities in the future (due to increased productivity and other business benefits)?

90% Of organizations are likely to maintain a remote workforce.

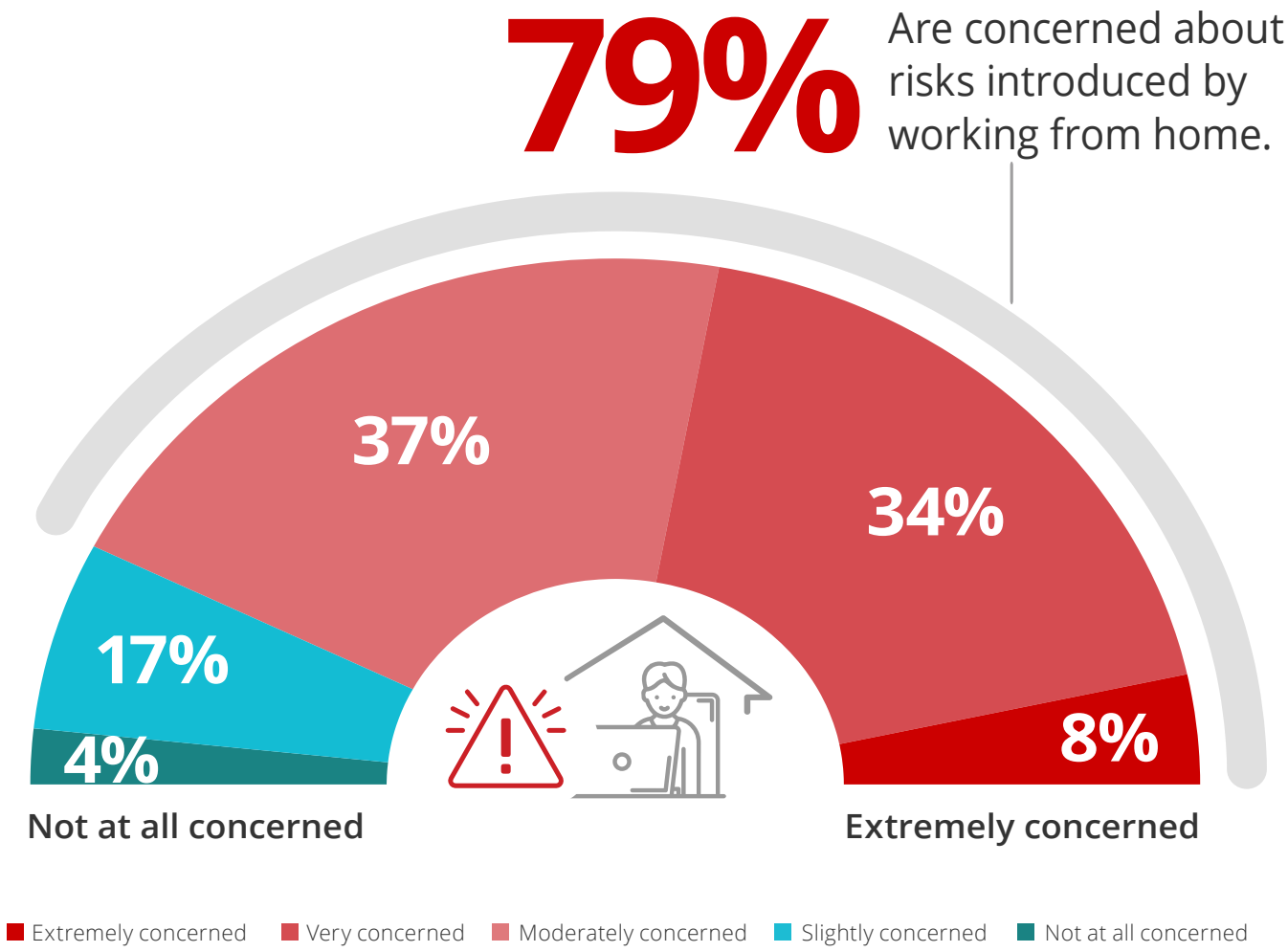


Not sure 5%

SECURITY RISK CONCERNS

More than three-quarters of organizations are moderately or more concerned about the security risks introduced by users working from home.

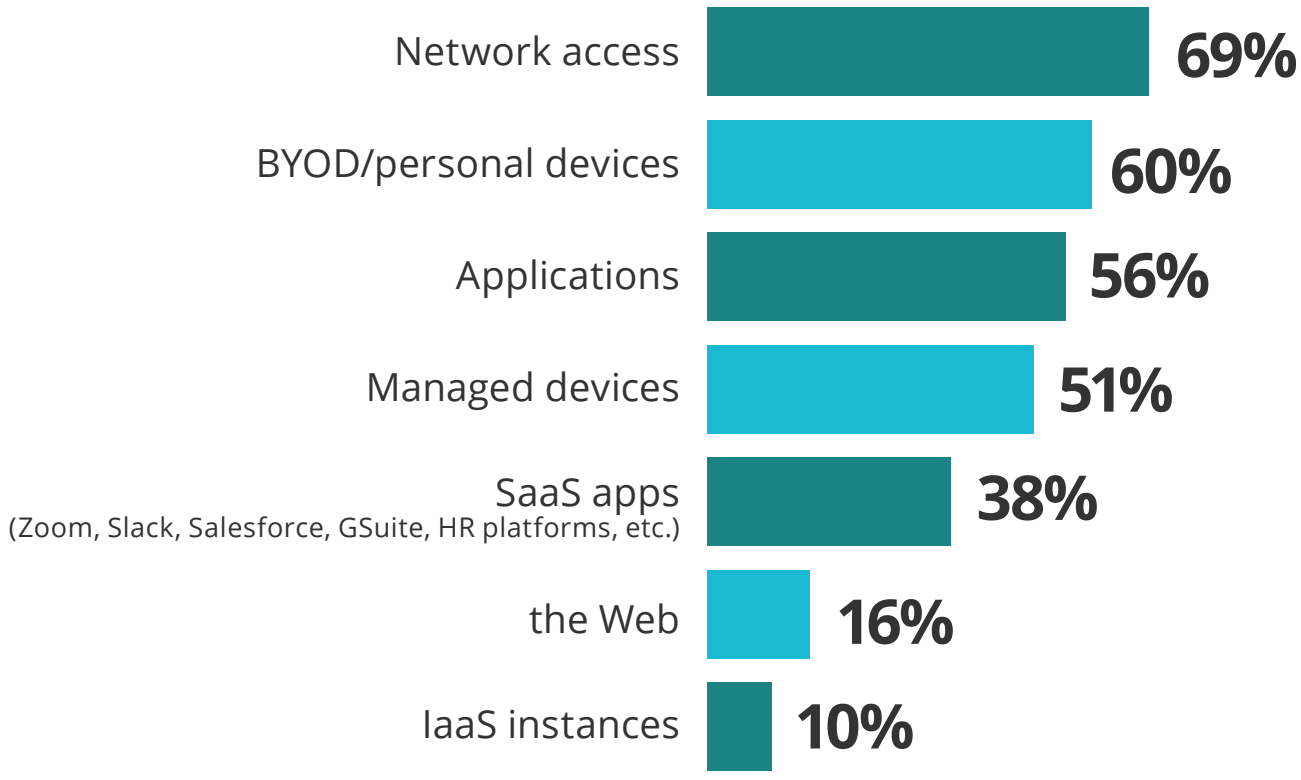
How concerned are you about the security risks introduced by users working from home?



SECURITY CONCERNS

Network access (69%) tops the list of concerns when it comes to securing remote employees. Bring Your Own Devices (BYOD) and personal devices (60%), applications (56%), and managed devices (51%) are also a concern for a majority of organizations.

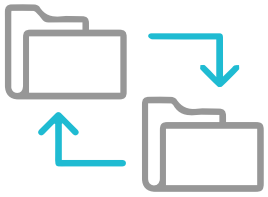
What is your organization primarily concerned with securing while employees work remotely?



RISKY APPS

The applications that organizations are most concerned with securing include file sharing (68%), the web (47%), video conferencing (45%), and messaging (35%). This is not surprising, as these are fundamental business applications that all organizations rely upon for a productive workforce.

What work applications used by remote workers are you most concerned about from a security perspective?



68%

File sharing

47%

Web applications

45%

Video conferencing

35%

Messaging

27%

Social media

26%

Websites

Other 2%

REMOTE SECURITY

Security breaches at the endpoints are a source of concern for many organizations as they look for securing their corporate assets. Therefore it is no surprise that organizations are most concerned with exposure to malware or phishing risks (39%) followed by protection of data, especially when accessed by unmanaged endpoints (36%).

What is the primary risk you're concerned with as your users connect remotely?

39%

Exposure to malware and phishing risks

36%

Protection of my data, especially when accessed by unmanaged endpoints

14%

Audit and oversight of employees conducting work from unmanaged resources

9%

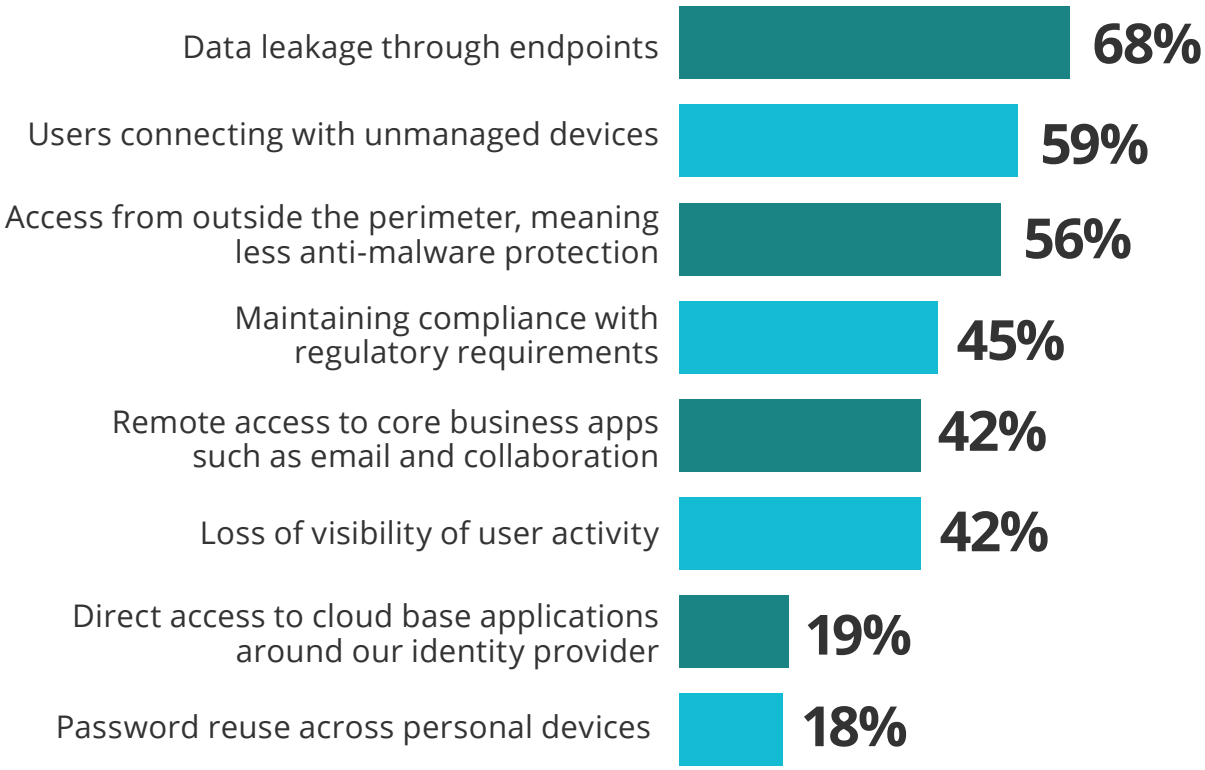
Ensure compliance of my regulated users

Other 2%

NEW SECURITY RISKS

The biggest security concerns due to the shift in the numbers of remote workers include data leaking through endpoints (68%), users connecting with unmanaged devices (59%), and access from outside the perimeter (56%). This is followed by maintaining compliance with regulatory requirements (45%), remote access to core business apps (42%), and loss of visibility of user activity (42%).

What are your concerns about the security risks introduced by new classes of remote users while working from home?

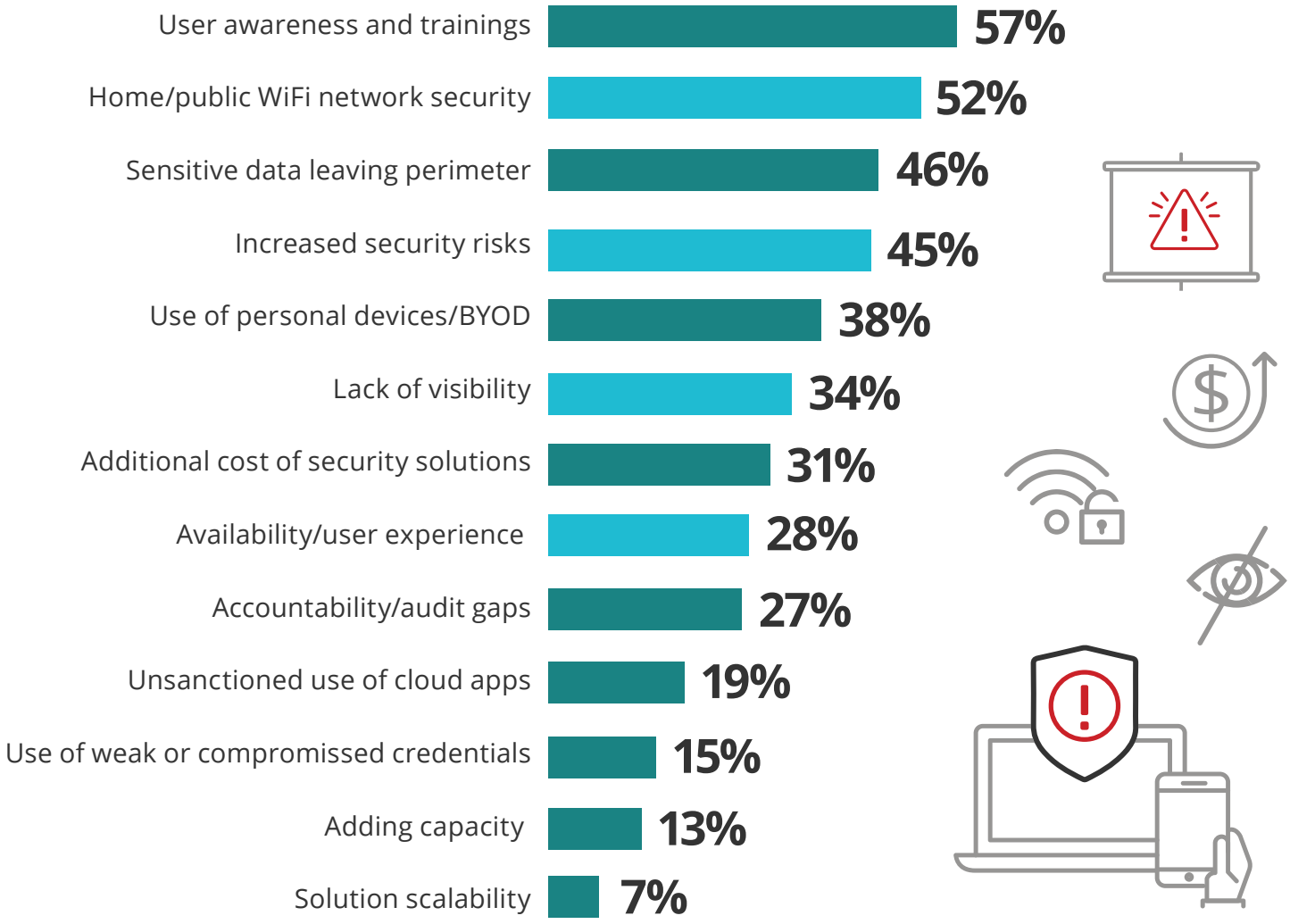


Other 4%

KEY SECURITY CHALLENGES

Key security challenges cited include user awareness and training (57%), home/public WiFi network security (52%), and sensitive data leaving the perimeter (46%).

What would you consider your organization's biggest security challenge regarding increasing the remote workforce?

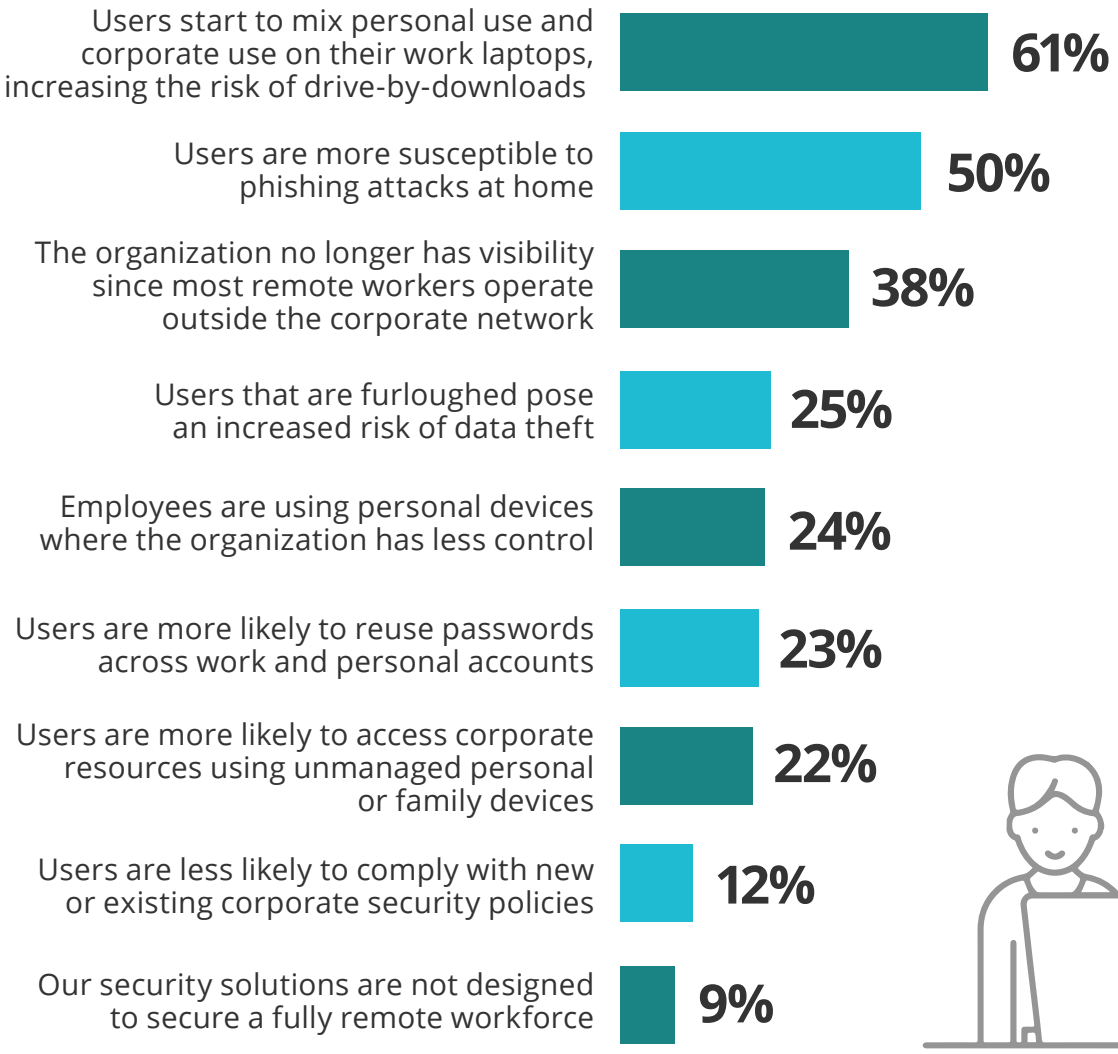


None 3% | Other 3%

WHAT MAKES REMOTE WORK LESS SECURE

The main reasons that make remote work less secure are: users start to mix personal use and corporate use on their work laptops, increasing the risk of drive-by-downloads (61%), users are more susceptible to phishing attacks at home (50%), the organization no longer has visibility since most remote workers operate outside the corporate network (38%), and users that are furloughed pose an increased risk of data theft (25%).

What makes remote work less secure?



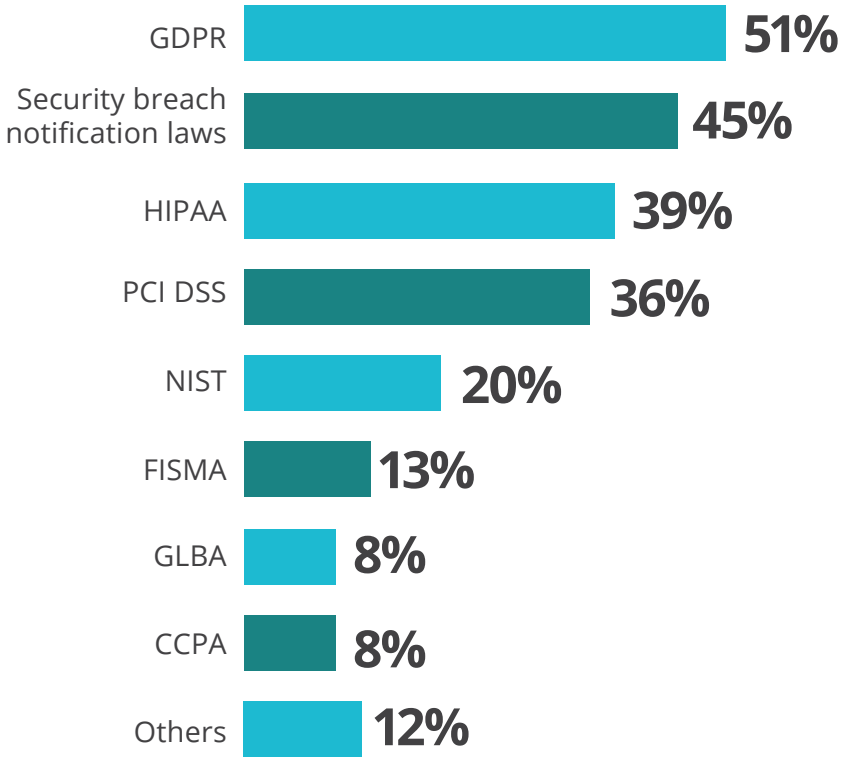
Other 3%

IMPACT ON COMPLIANCE

Just about three-quarter of organizations see remote work environments having an impact on their compliance posture (70%). GDPR tops the list of compliance mandates (51%).

Could remote work impact compliance mandates that apply to your organization?

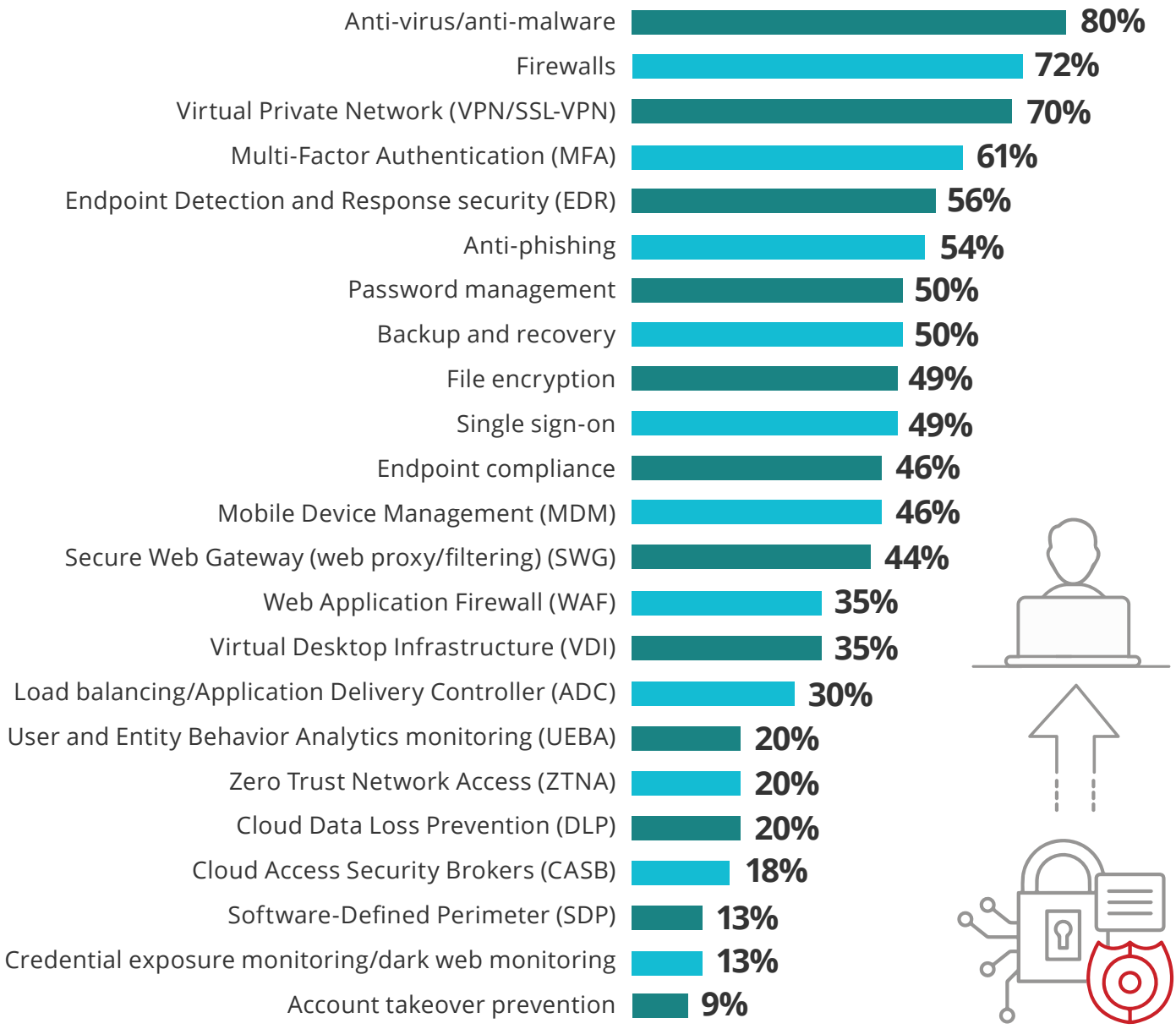
If so, which ones?



SECURITY CONTROLS IN PLACE

When we asked organizations about security controls, most are using a variety of security controls to protect remote work scenarios. A majority of respondents (80%) use anti-virus/anti-malware, firewalls (72%) and virtual private networks (70%) to propery secure remote work-from-home. Those to follow directly are multi-factor authentication (61%), endpoint detection and response (56%), and anti-phishing (54%), among others.

What security controls do you currently deploy to secure remote work-home office scenarios?



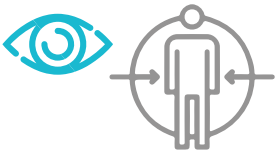
None 1%

CYBER TECHNOLOGY PRIORITIES

In order to better protect against new threats, organizations prioritize human-centric visibility into remote employee activity (34%), followed by next-generation anti-virus and endpoint detection and response (23%), improved network analysis and next-gen firewalls (22%), and zero trust network access (19%).

Please rank the importance of the following cyber technologies to protect the organization from these new threat vectors?

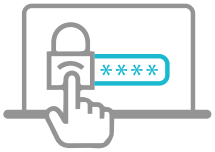
1 | **34%** Human-centric visibility



2 | **23%** Next-gen AV or EDR

3 | **22%** Improved network analysis and next-gen firewalls

4 | **19%** Zero Trust Network Access (ZTNA)



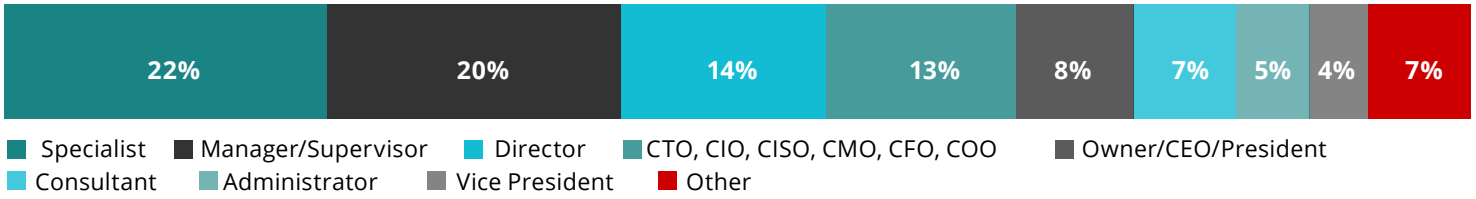
5 | **10%** Next-gen SIEM

6 | **6%** Cloud Access Security Broker (CASB)

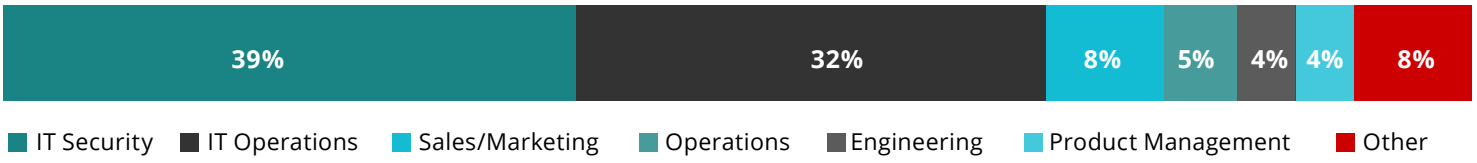
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 287 IT and cybersecurity professionals in the US, conducted in January 2021, to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences for remote work security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

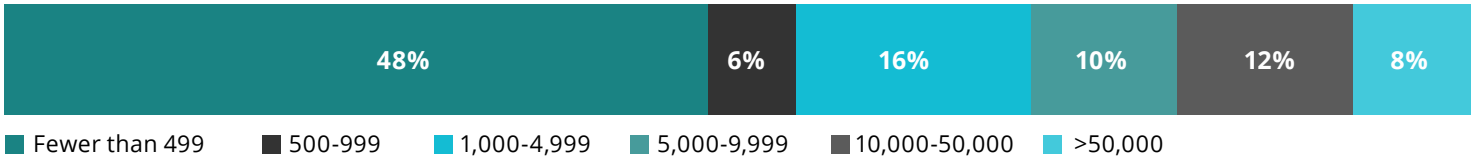
CAREER LEVEL



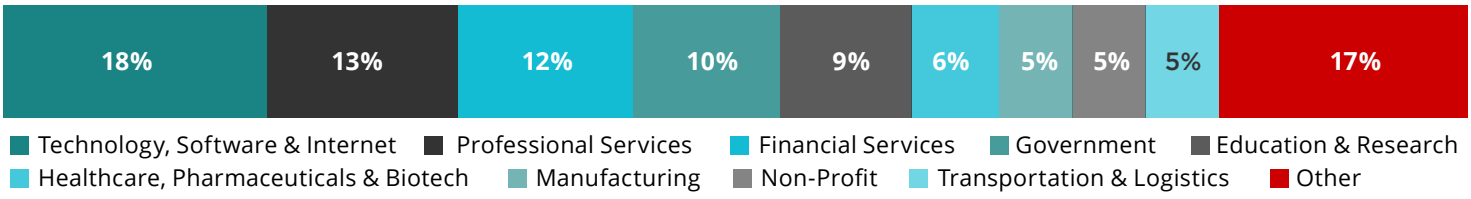
DEPARTMENT



COMPANY SIZE



INDUSTRY



About archTIS

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute-based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit **archtis.com** or follow **@arch_tis.**

About Nucleus Cyber

Nucleus Cyber, an archTIS Limited company (ASX:AR9), is a provider of advanced information protection solutions that prevent data loss and protect against insider threats. The company's NC Protect solution leverages existing technology investments to provide a simpler, faster and cheaper solution to tailor information protection for file sharing, messaging and chat across collaboration tools. For midsize to large enterprises and regulated industries it protects business-critical content in cloud collaboration tools Microsoft Office 365—SharePoint, Teams, OneDrive, Exchange and Yammer, plus Dropbox, Nutanix Files and Windows file shares. For more information visit **nucleuscyber.com** or follow **@nucleuscyber.**