2021
Remote Workforce Security Report

SpyCloud

Cybersecurity
INSIDERS

Overview

Following the dramatic rise in work-from-home in the wake of the COVID-19 pandemic, securing the expanding remote workforce has become a critical priority for organizations.

The 2021 Remote Workforce Security Report reveals the current state of protecting the new workforce of widely distributed organizations. The report explores their key challenges, along with the new security threats they face, technology gaps and preferences, investment priorities, and more.

Key findings include:

- A majority of organizations (79%) are at least moderately concerned about the security risks introduced by users working from home
- Only 22% of organizations confirm that they were fully prepared for the massive shift to remote work from a security perspective
- Organizations are primarily concerned with securing network access (69%), followed by BYOD/personal devices (60%), and managed/corporate devices (51%)

We would like to thank SpyCloud 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

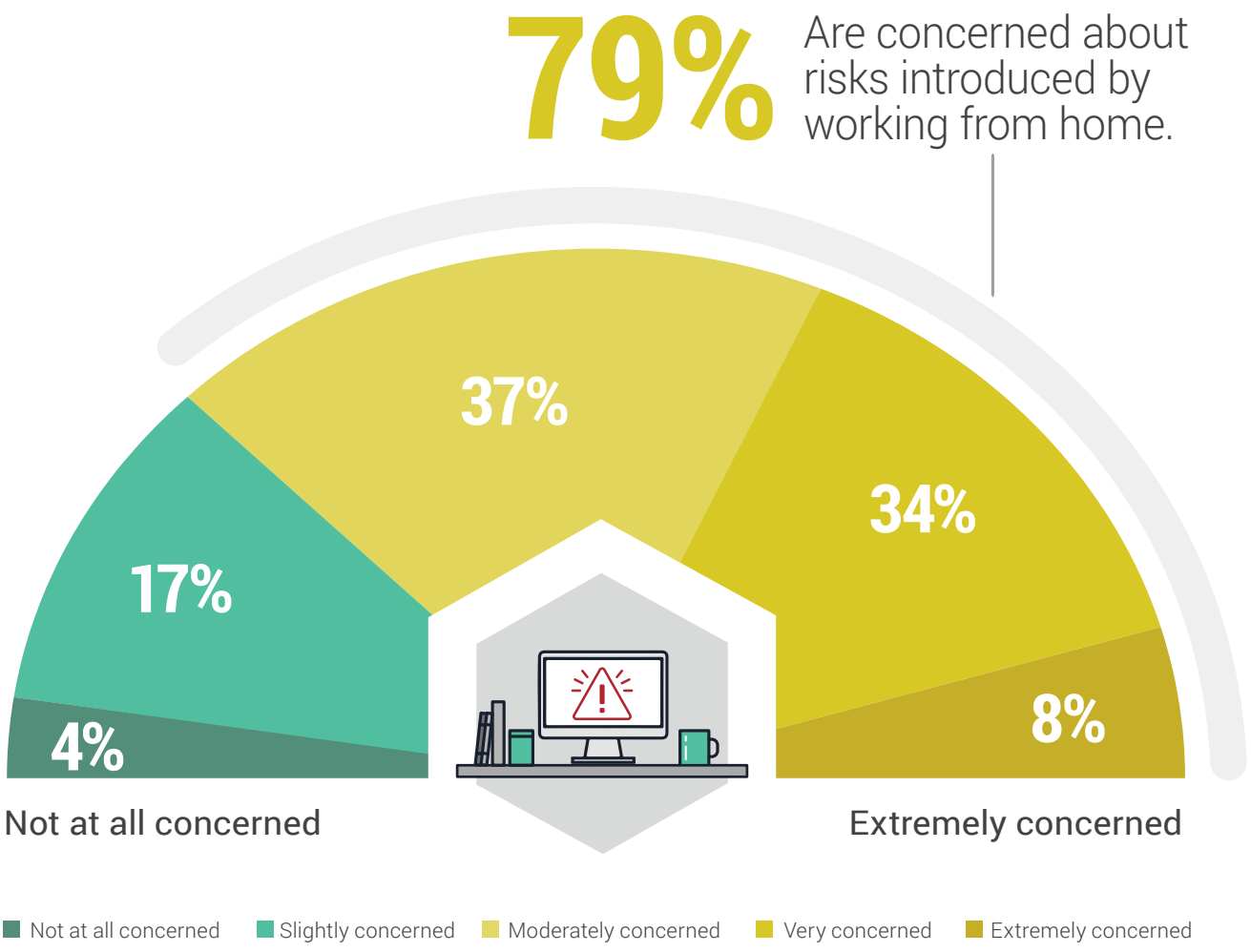
Contents

INTRODUCTION

Security Risk

Eight out of ten organizations are at least moderately concerned about the security risks introduced by users working from home.

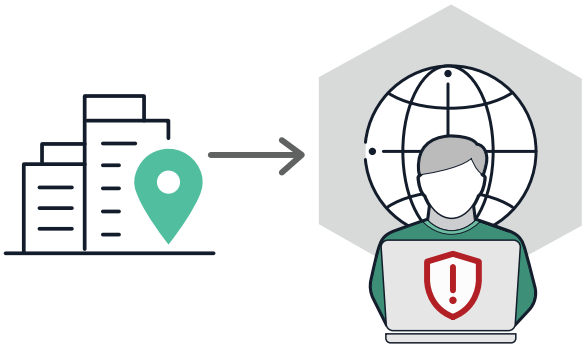
How concerned are you about the security risks introduced by users working from home?

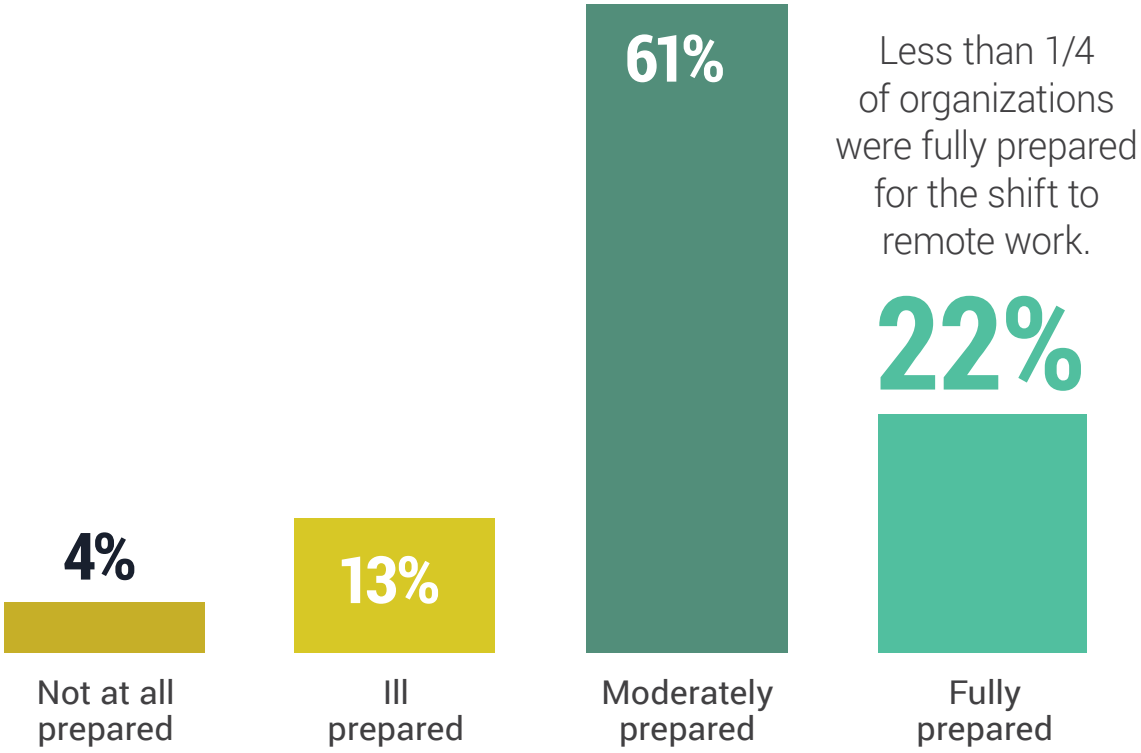


Security Preparedness

The COVID pandemic highlighted how prepared organizations were for the complete shift to remote working, but only 22% confirmed that they were fully prepared from a security perspective.

How prepared was your organization for the shift to remote work from a security perspective?





Less than 1/4 of organizations were fully prepared for the shift to remote work.

Security Concerns

Organizations shared a myriad of concerns regarding securing remote employees, with network access and device security at the top of the list.

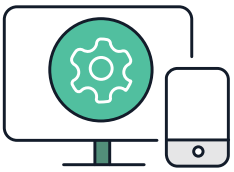
What is your organization primarily concerned with security while employees work remotely?

69%

Corporate network access

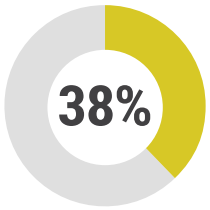
60%

BYOD/ personal devices

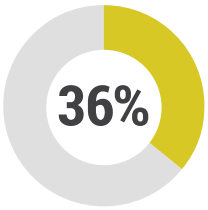


51%

Managed devices



SaaS apps
(Zoom, Slack, Salesforce, GSuite, HR platforms, etc.)



On-premises apps

Custom apps

the Web 16% | IaaS instances 10%

PERCEPTIONS OF REMOTE WORKFORCE SECURITY

What Makes Remote Work Less Secure

When drilling down into what makes remote work less secure, the most common responses can be grouped into user behavior and lack of visibility. More than half of the respondents believe that employees are more likely to use corporate devices for personal and family activities, where just over a third of respondents believe that remote employees operating outside the corporate network makes remote work less secure.

What makes remote work less secure?

61%

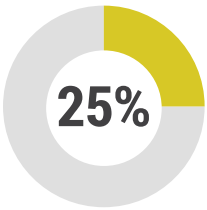
Users are more likely to use corporate devices for personal and family activities

50%

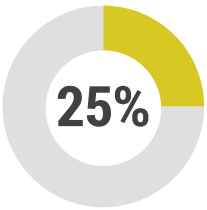
Users are more susceptible to phishing attacks at home

38%

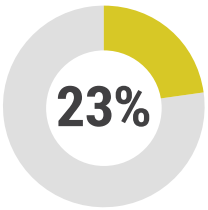
Lack of visibility, since most remote workers operate outside the corporate network



Users that are furloughed pose an increased risk of data theft



Employees are using personal devices where the organization has less control



Users are more likely to reuse passwords across work and personal accounts

Users are more likely to access corporate resources using unmanaged personal or family devices 22% | Users are less likely to comply with new or existing corporate security policies 12% | Our security solutions are not designed to secure a fully remote workforce 9% | Other 3%

Remote Security Risk

Many of the factors that respondents say make remote work less secure tie back to user behavior. Thirty-nine percent of respondents believe that users are more at risk of malware, phishing, or other exploit, concerns that are amplified when employees use personal devices that are outside of corporate control.

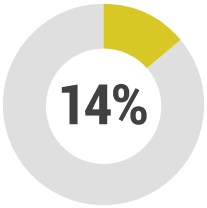
What is the primary risk you're concerned with as your users connect remotely?

39%

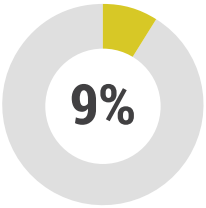
Exposure to malware, phishing, or other exploit

36%

Protection of my data, especially when accessed by unmanaged endpoints



Audit and oversight of employees conducting work from unmanaged resources



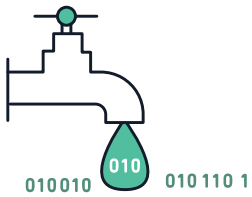
Ensure compliance of my regulated users

Other 2%

New Security Risks

When looking at the new security risks posed by remote workers, user behavior remains top of mind, with users connecting via unmanaged devices taking the number two spot. However, only 18% view password reuse across personal devices as a new risk.

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



68%

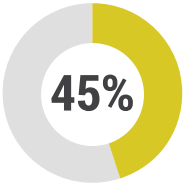
Data leakage to endpoints

59%

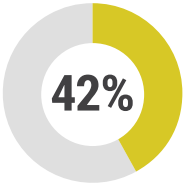
Users connecting with unmanaged devices

56%

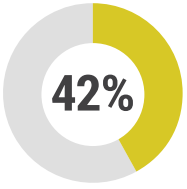
Access from outside the perimeter, meaning less anti-malware protection



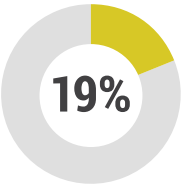
Maintaining compliance with regulatory requirements



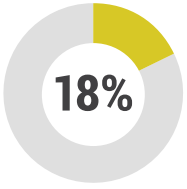
Remote access to core business apps (such as, email and collaboration)



Loss of visibility of user activity



Direct access to cloud-based applications around our IDP



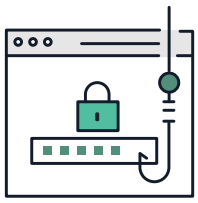
Password reuse across personal devices

Other 4%

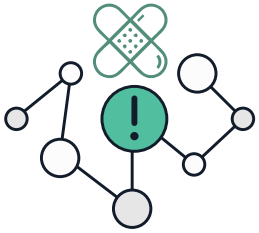
Threat Vectors

Last year, malware (72%) and phishing (67%) topped the list of the most concerning threat vectors facing remote work environments. This year, 72% of respondents believe phishing to be the most concerning threat vector. By tapping into strong emotions around the COVID-19 pandemic, cybercriminals are luring people into taking risky actions without considering the consequences.

What specific threat vectors are you most concerned about with employees working from home?

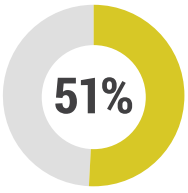


72%
Phishing



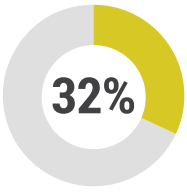
60%
Unpatched systems/ vulnerability exploits

59%
Malware

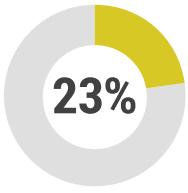


Unauthorized user/privileged access

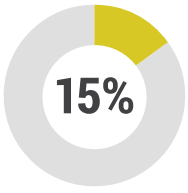
Malicious websites



Identity theft



Insider attacks



Account takeover

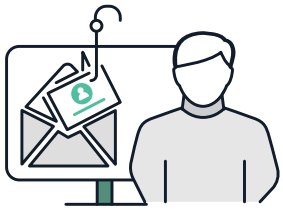
Other 1%

WHAT USERS REPORT

Security Support Issues

We asked organizations which security related support questions they are increasingly seeing. By far the most frequently mentioned topic is phishing attempts (63%); this is followed by suspicious authentication attempts (31%) and issues with backing up devices (28%).

Since going remote, which of the following have you received increased security support questions about?



63%

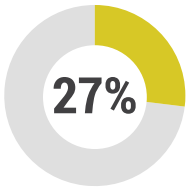
Reported phishing attempts

31%

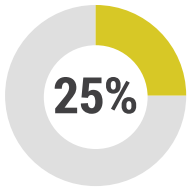
Suspicious two-factor authentication attempts

28%

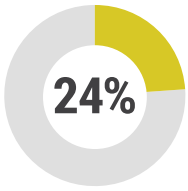
Unable to share/backup from certain device types



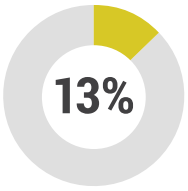
Reports of malware on devices



Concerns over connecting personal IoT to same internet network used for work



Reporting breaches of third-party tools



Concerns about terms of service of certain apps

Other 6%

WHAT ARE YOU DOING ABOUT IT?

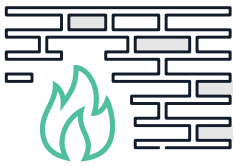
Security Controls

When we asked organizations about security controls to protect remote work scenarios, anti-virus/malware jumped three points over last year to 80%, while anti-phishing jumped seven points to 54%. This increase in anti-phishing controls could reflect adjustments organizations made in light of COVID-related scams.

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

80%

Anti-virus/ malware

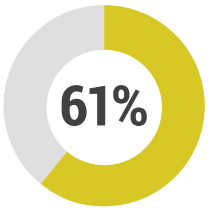


72%

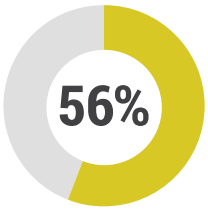
Firewalls

70%

Virtual Private Network (VPN/SSL-VPN)



Multi-Factor Authentication (MFA)



Endpoint security (EDR)

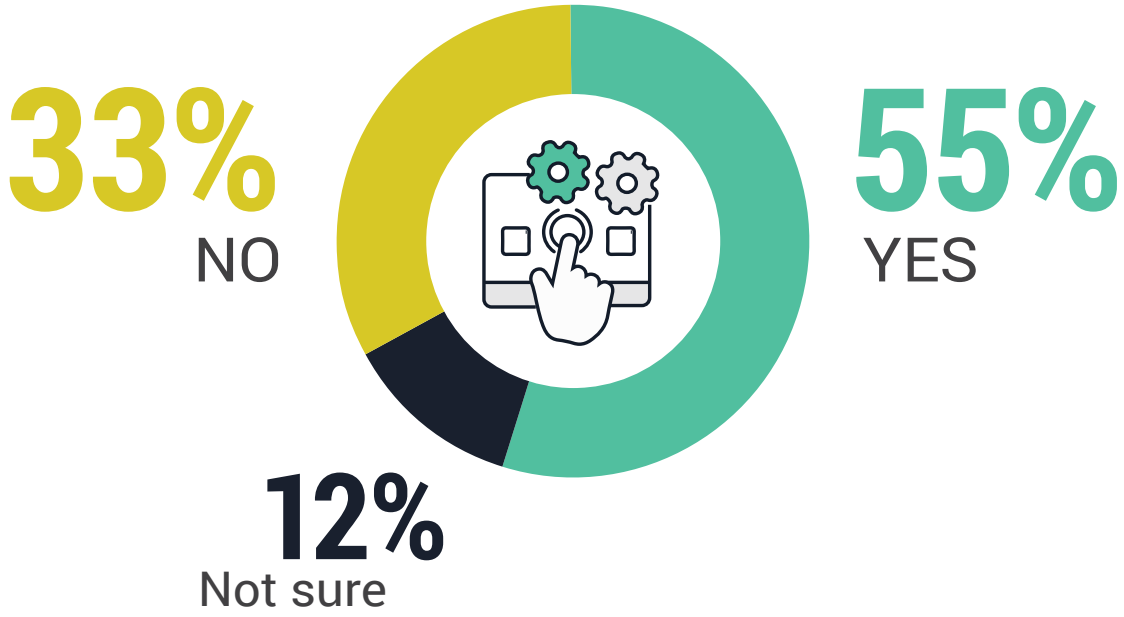
Anti-phishing

Password management 50% | Backup and recovery 50% | File encryption 49% | Single sign-on 49% | Endpoint compliance 46% | Mobile Device Management (MDM) 46% | Secure Web Gateway (web proxy/filtering) (SWG) 44% | Web Application Firewall (WAF) 35% | Virtual Desktop Infrastructure (VDI) 35% | Load balancing/Application Delivery Controller (ADC) 30% | User and entity behavior monitoring (UEBA) 20% | Zero Trust Network Access (ZTNA) 20% | Cloud DLP 20% | Cloud Access Security Brokers (CASB) 18% | Software-Defined Perimeter (SDP) 13% | Credential exposure monitoring/dark web monitoring 12% | Account takeover prevention 9% | None 1%

Access Through Personal Devices

A huge risk to organizations is undetected malware on personal devices. Organizations are being more stringent about employee's access of corporate applications from personal, unmanaged devices since working from home. Last year, 27% of respondents said that employees aren't allowed to access managed applications from personal devices. This year, the number jumped 6 points to 33%.

Are employees able to access managed applications from personal, unmanaged devices?



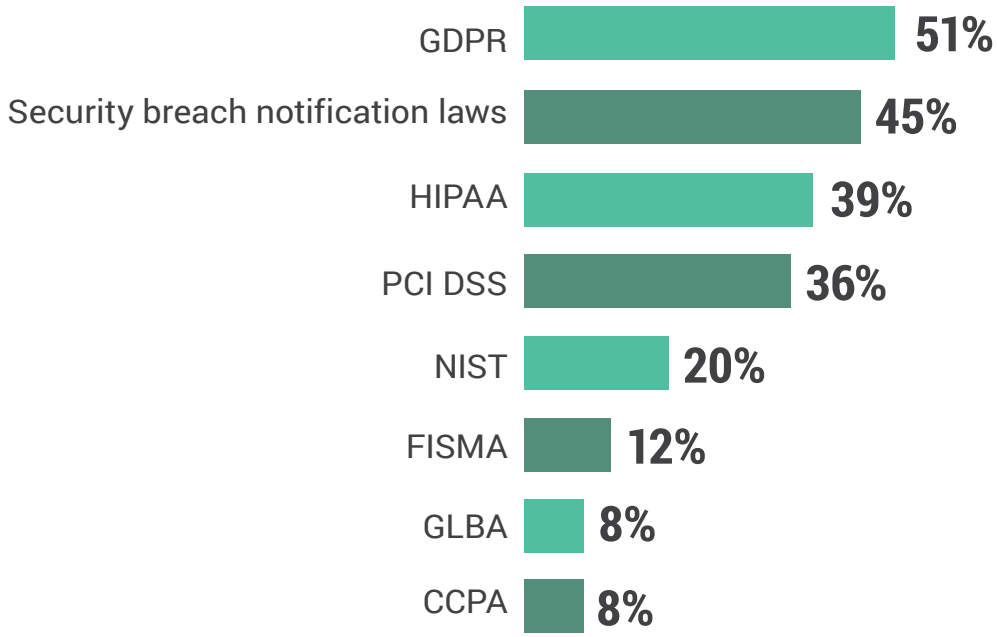
POLICIES & REGULATIONS

Impact on Compliance

Seventy percent of organizations see remote work environments having a negative impact on their compliance posture, which is a seven point increase from last year. GDPR tops the list of affected compliance mandates (51%), followed by security breach notification laws (45%) and HIPAA (39%).

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

If so, which ones?

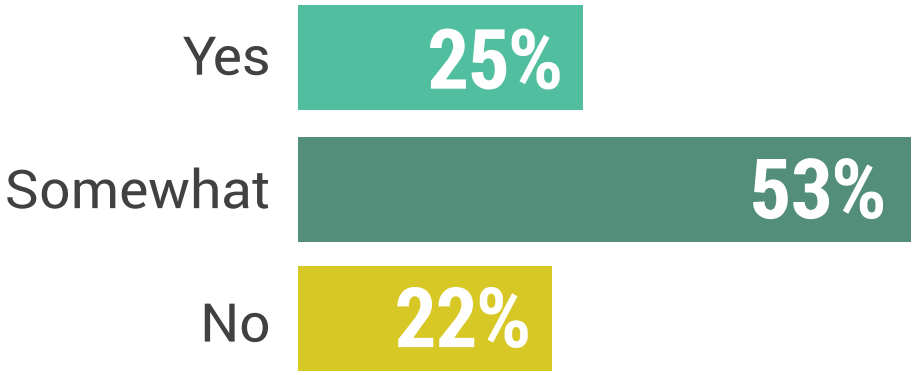


SECURITY IS A SHARED RESPONSIBILITY

Shifting Security Burden

When asked whether much of the burden for securing a remote workplace is shifting from the IT security team to the individual employee, 53% believe that it should be a shared responsibility.

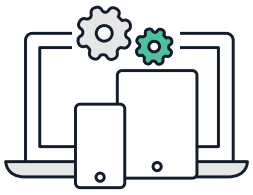
Do you agree with the following statement: Much of the burden of responsibility for securing the remote workplace is shifting from the IT security team to the individual employee?



Security Compliance by Employees

When it comes to adhering to security policies and protocols, employees most commonly comply with Mobile Device Management (MDM) (32%), followed by multi-factor authentication (30%) and Virtual Private Networks (VPN) (26%).

Which of the following security protocols are individuals most resistant to adhering to or maintaining?



32%

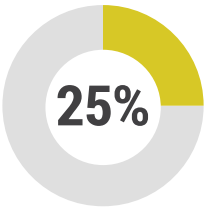
Mobile Device Management (MDM)

30%

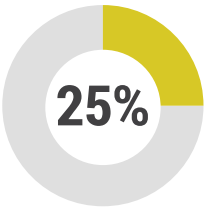
Multi-Factor Authentication (MFA)

26%

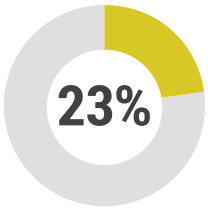
Virtual Private Network (VPN/SSL-VPN)



File encryption



Password managers



Anti-phishing

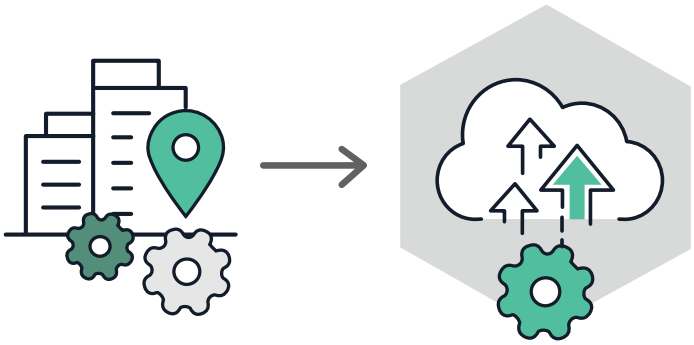
Web proxy/web filtering 22% | Backup and recovery 22% | Endpoint Security (EDR) 22% | Virtual Desktop Infrastructure (VDI) 20% | Anti-virus/malware 19% | Single sign-on 17% | User and entity behavior monitoring (UEBA) 17% | Zero Trust Network Access (ZTNA) 17% | Account takeover prevention 16% | Endpoint compliance firewalls 16% | Web Application Firewall (WAF) 13% | Cloud Access Security Brokers (CASB) 12% | Cloud DLP 10% | Other 15%

THE FUTURE OF REMOTE WORK

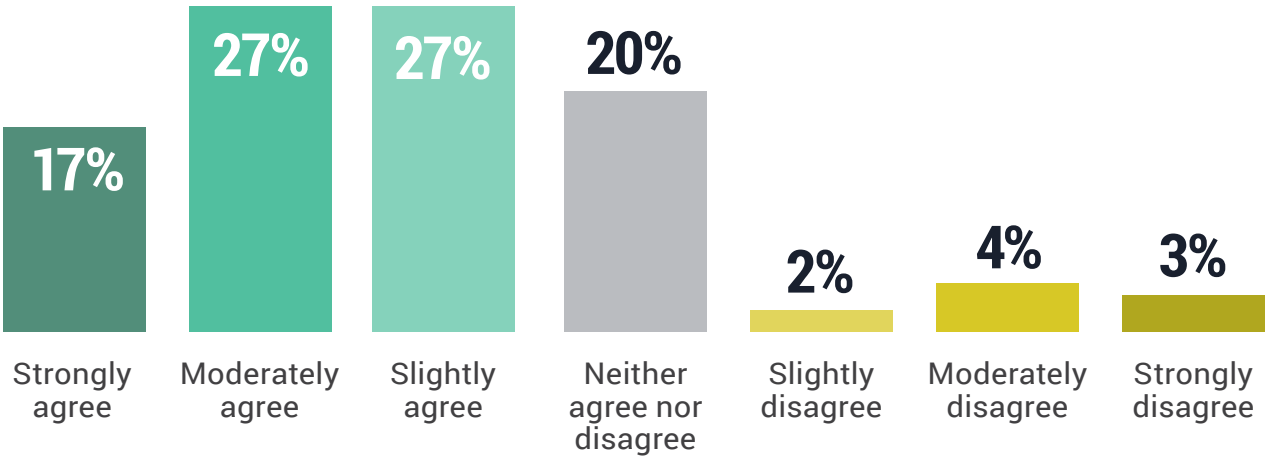
Shift To Cloud

Cloud computing has emerged as the backbone of remote work; survey respondents agree, with the vast majority reporting a continued transition from on-premises applications to the cloud.

To what degree do you agree with this statement: Going forward: your organization will shift away from on-premises applications and tools in favor of the cloud for enabling remote work.



71% Agree with organizations shifting away from on-premises applications and tools in favor of the cloud for enabling remote work.

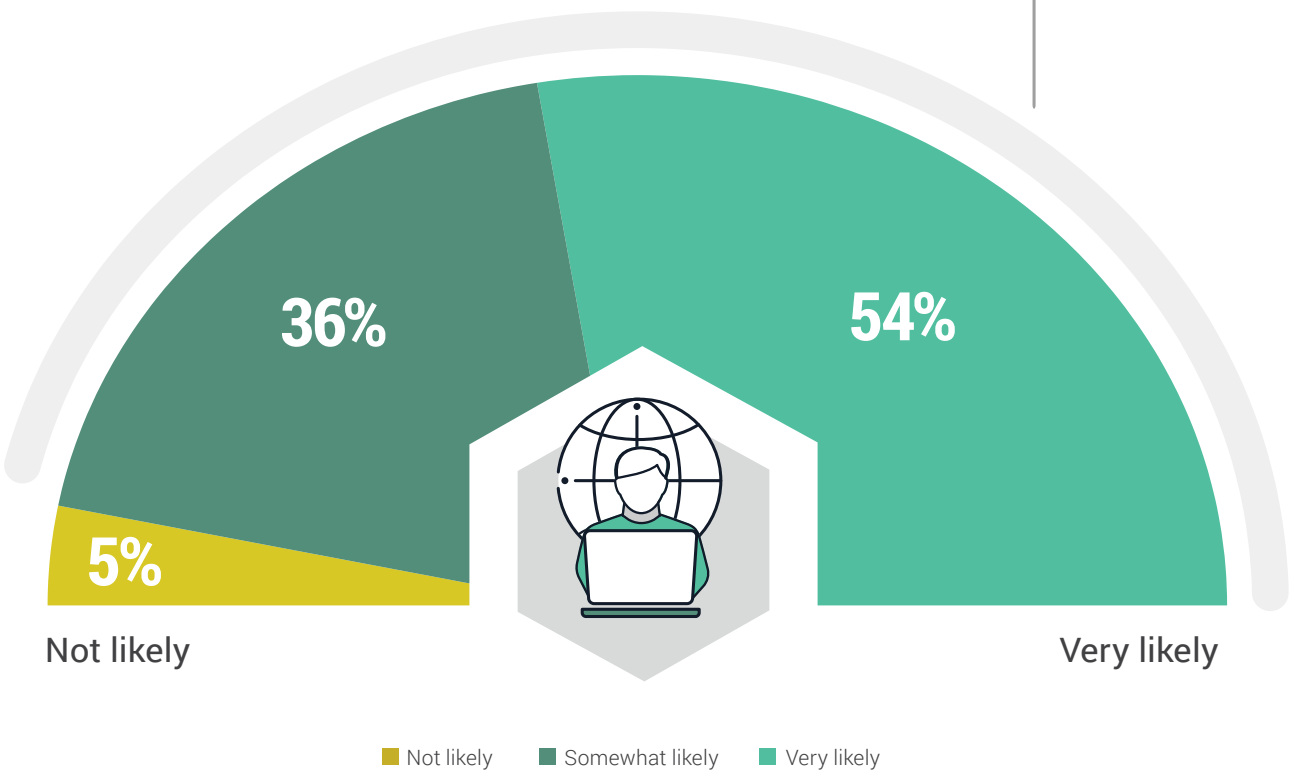


Future WFH Support

Organizations have seen increased productivity and other benefits with remote working, meaning security teams will need to continue to support this trend, even after the world returns to some sense of normalcy.

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 consider that they will likely continue increased work from home capabilities in the future.

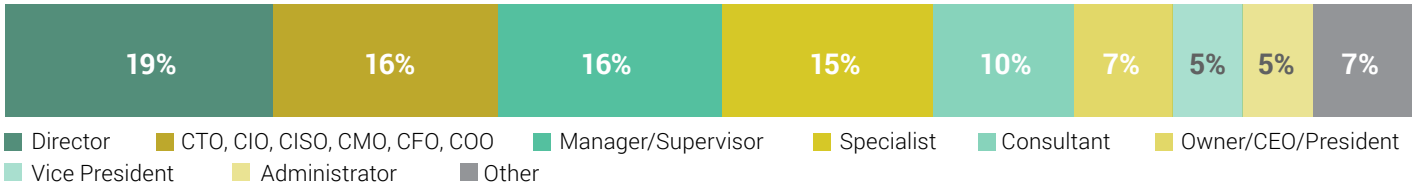


Other 5%

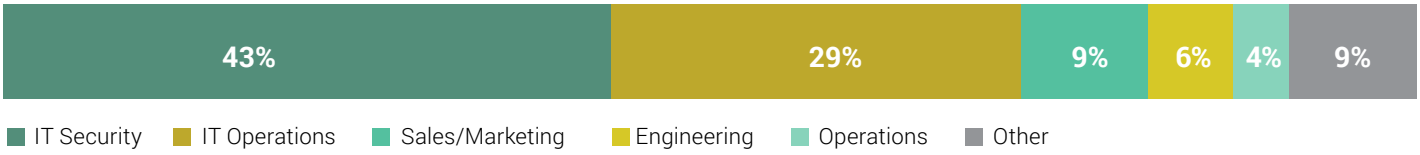
Methodology & Demographics

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.

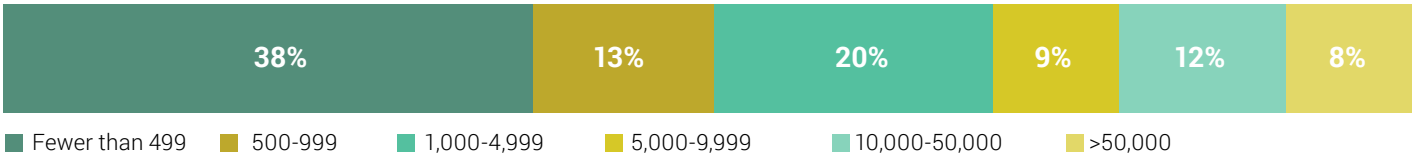
CAREER LEVEL



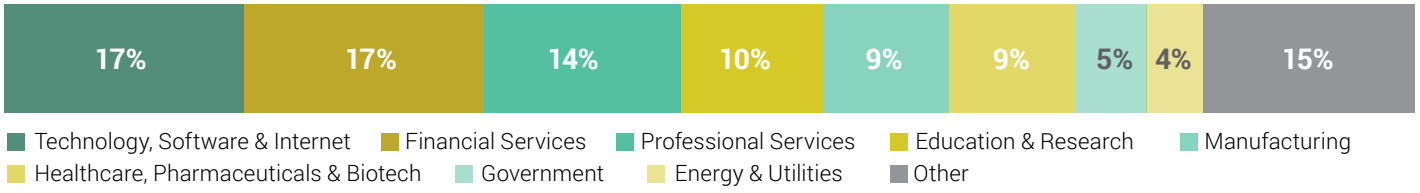
DEPARTMENT



COMPANY SIZE



INDUSTRY



Why SpyCloud Cares

Our collective shift to remote life, from work to school to grocery shopping, has substantially expanded the attack surface for both individuals and organizations. Shared devices, increased online activity, and newly-created accounts have provided threat actors with a plethora of targets, especially as users put themselves and their employers at risk by reusing passwords across work applications and personal accounts.

SpyCloud is in the business of preventing account takeover that occurs when bad actors leverage stolen credentials – usually obtained in data breaches or malware campaigns – to log into accounts and steal data, files, and funds. Even when in-person activities resume, the many extra accounts created to navigate online life will remain, and a data breach of one forgotten app or website can continue to endanger users and their employers.

The proven way to ensure that those logging into your systems are who they say they are – and not criminals using stolen credentials – is to detect and reset compromised passwords early, before criminals have a chance to use them. SpyCloud protects over two billion employee and consumer accounts, with solutions powered by the world's largest collection of breach and botnet data.

Learn more and see how many of your users' credentials have been exposed in data breaches at **spycloud.com.**