2020

Cybersecurity INSIDERS

REMOTE WORKFORCE SECURITY REPORT

bitglass

OVERVIEW

Securing the remote workforce has become a critical priority for organizations affected by the closing of offices and workplaces in the wake of the COVID-19 pandemic.

Conducted during the height of the 2020 COVID-19 pandemic, this Remote Workforce Security Report reveals the state of securing the new remote workforce, key challenges and unique security threats faced by organizations, technology gaps and preferences, investment priorities, and more.

Key findings include:

- 84% of organizations consider it at least somewhat likely (44% of them very likely) that they will continue increased work from home capabilities in the future due to increased productivity benefits.
- 65% allow access from personal, unmanaged devices, while 55% see this scenario as a significant security risk.
- 54% confirm that the COVID epidemic accelerated migration of workflows to cloud-based apps.
- Of the organizations that expanded secure access capacity, the most frequent motion was to purchase more user licenses for existing apps (39%), followed by adding new vendors / solutions (26%), and purchasing more hardware (18%).

We would like to thank Bitglass for supporting this important industry research project. We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats and during challenging times.

Thank you,

Holger Schulze

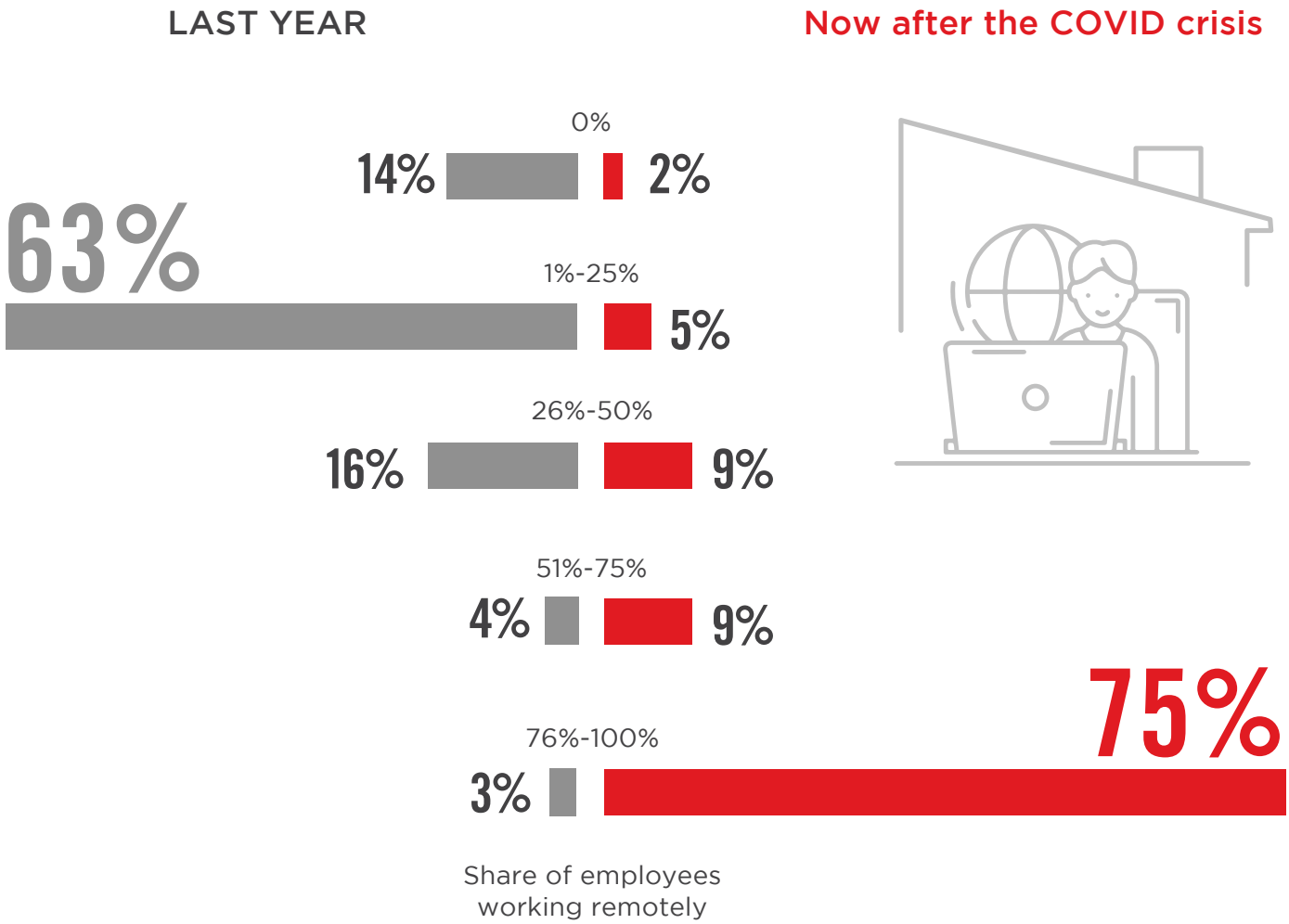
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

DRAMATIC INCREASE IN REMOTE WORKFORCE

The survey reveals a massive shift toward remote and homebased work environments due to the COVID-19 pandemic. While a majority of 63% of organizations had less than one-quarter of employees working in remote/at-home environments before the crisis, a whopping three quarters of the same organizations report that over 75% of their workforce is now working from home.

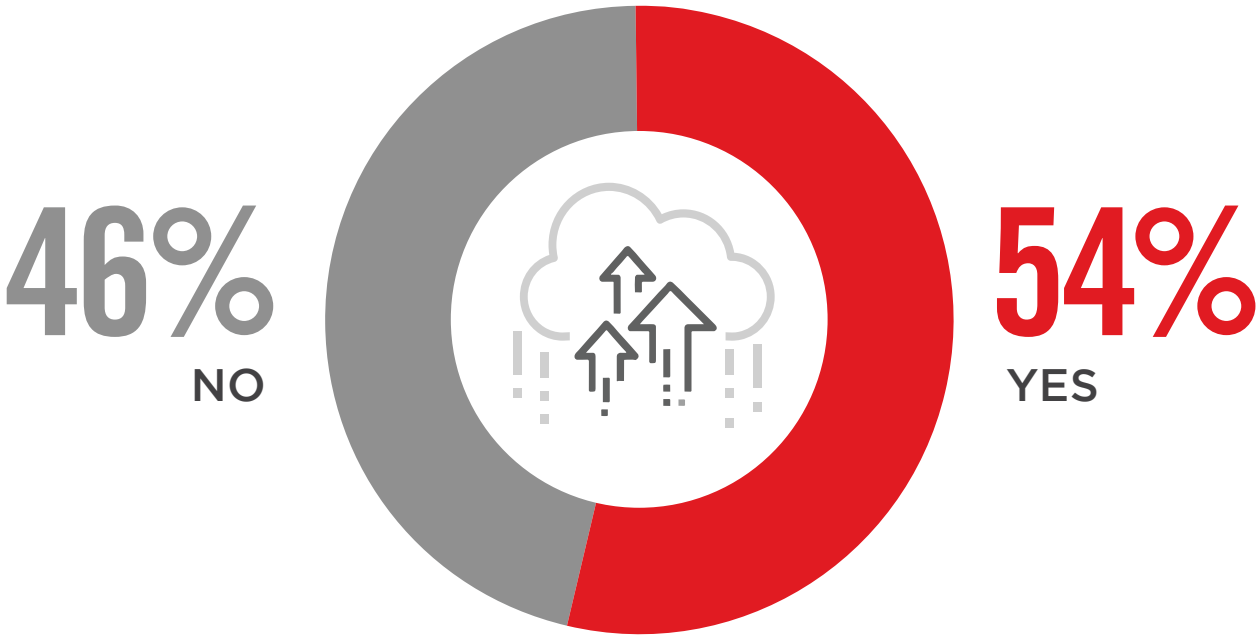
What percentage of your workforce was working remotely/at-home LAST YEAR compared to NOW during the COVID crisis?



MIGRATION TO CLOUD

A majority (54%) confirm that the COVID pandemic accelerated the migration of user workflows to cloud-based applications. As applications migrate to the cloud, companies need to consider how securing applications in the cloud is different than on-premises solutions.

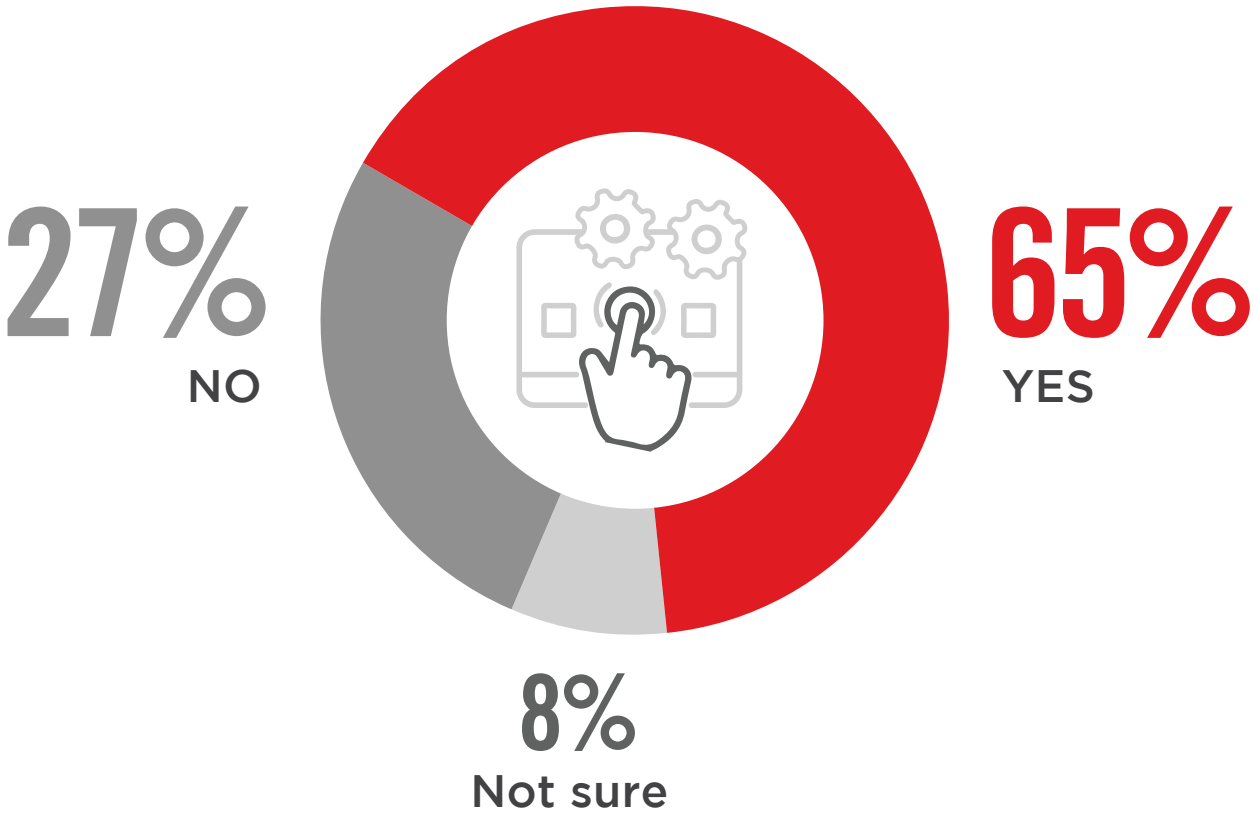
Has COVID accelerated migration of additional user workflows or applications to cloud-based applications?



ACCESS FROM PERSONAL DEVICES

A total of 65% allow access from personal, unmanaged devices, while 55% see this scenario as a significant security risk. Securing bring your own device (BYOD) requires a different approach to security than securing managed devices. For example, agents may not be the ideal model for monitoring all traffic on personal devices.

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



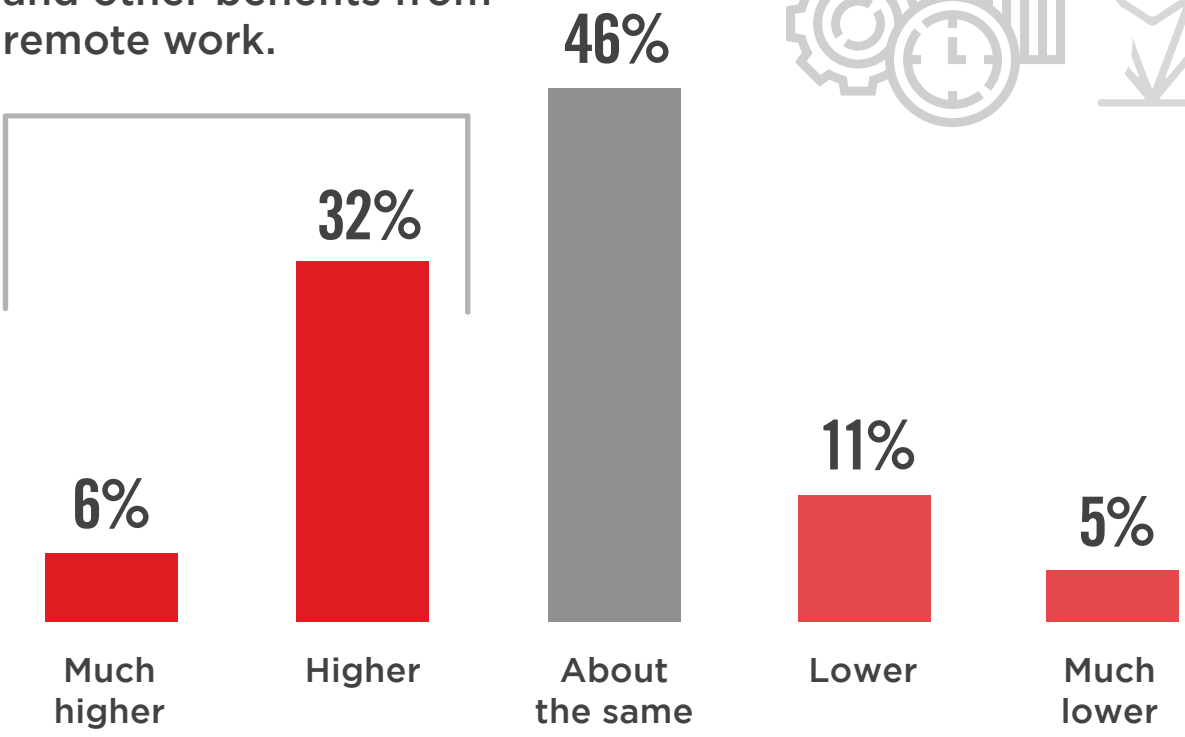
PRODUCTIVITY EFFECTS

Thirty-eight percent of organizations expressed they see higher productivity and other benefits from remote work. Only 16% see lower productivity.

Is your organization seeing higher productivity and other benefits from remote work?

38%

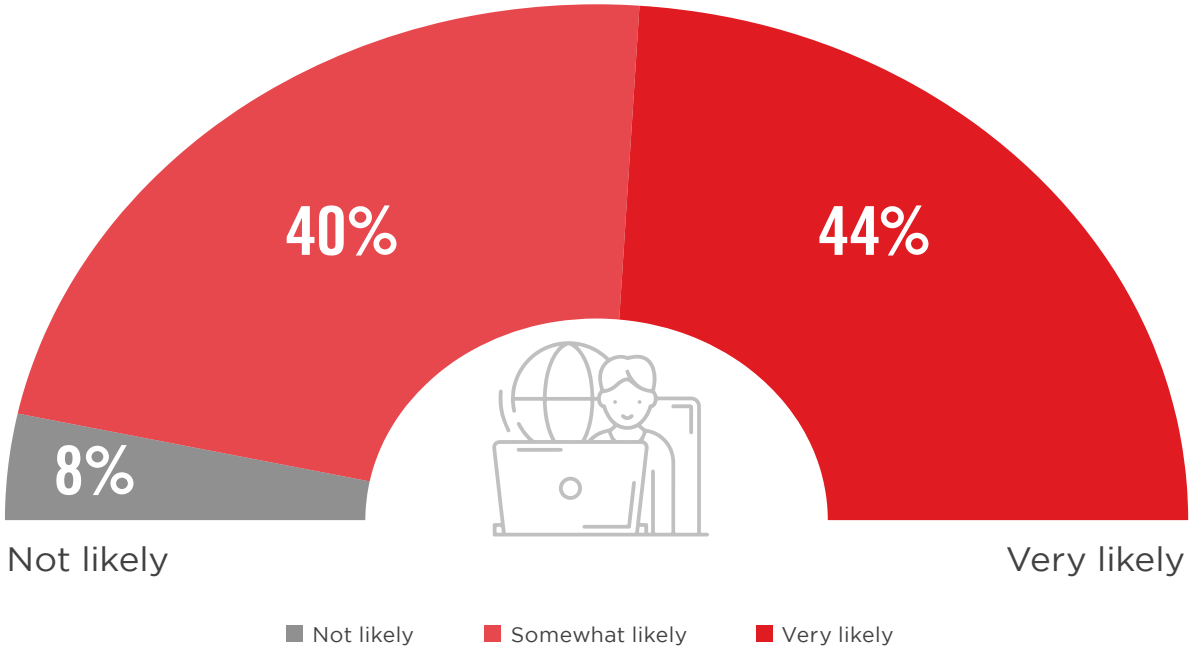
See higher productivity and other benefits from remote work.



FUTURE REMOTE WORK

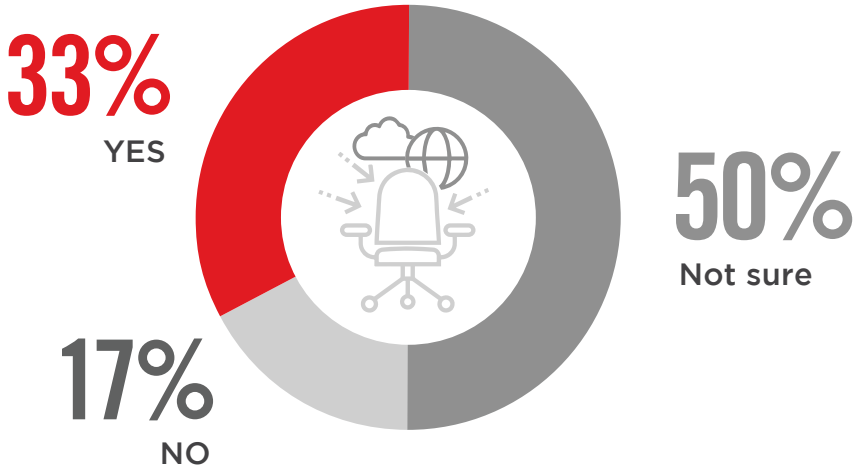
Similarly, a majority of organizations consider it at least somewhat likely (44% of them very likely) they will continue increased work from home capabilities in the future due to increased productivity benefits. In fact, 33% are looking at making some positions permanently remote after the COVID crisis ends.

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



Other 8%

Is your organization considering to make some positions permanently remote (that used to be on-site) after the COVID crisis ends?

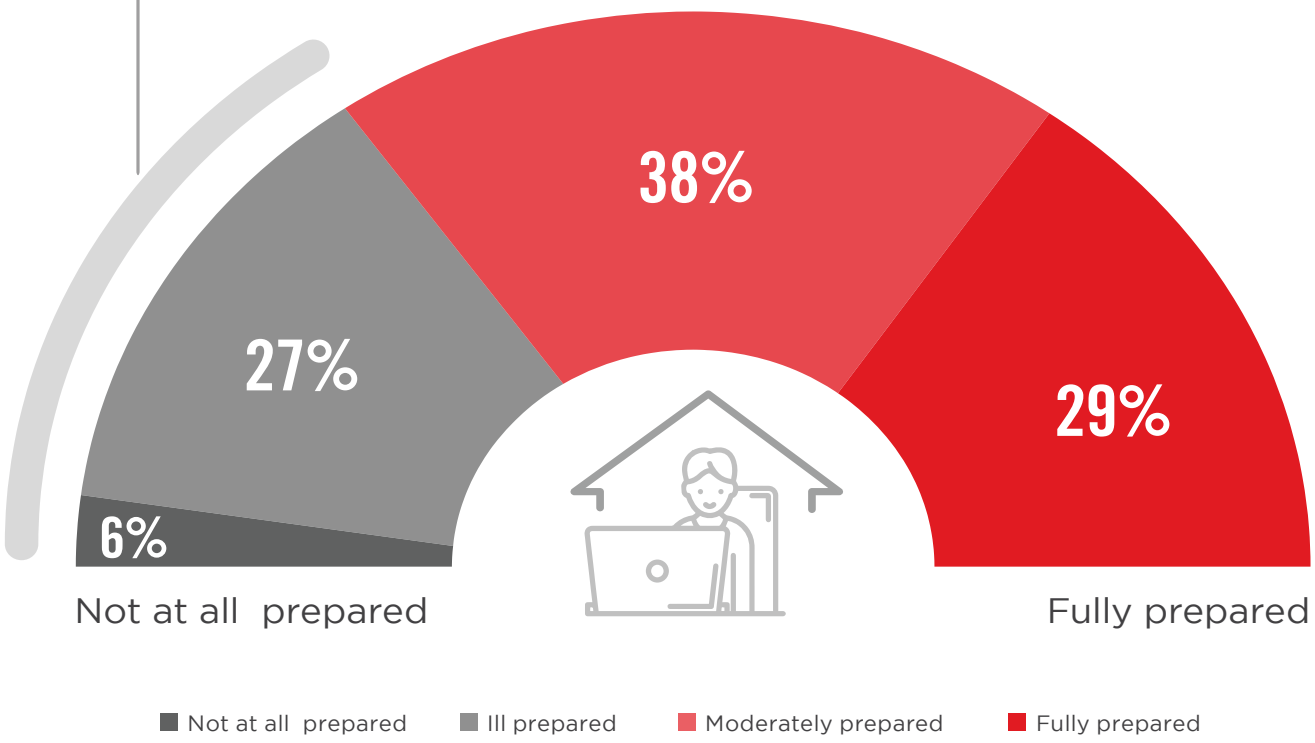


READINESS FOR REMOTE WORK

A third of organizations report they were not sufficiently prepared for the rapid shift from on-premises to remote work scenarios.

Prior to the COVID-19 pandemic, how prepared was your organization with a business continuity/disaster recovery plan that included a rapid shift from on-premises work to a remote workforce?

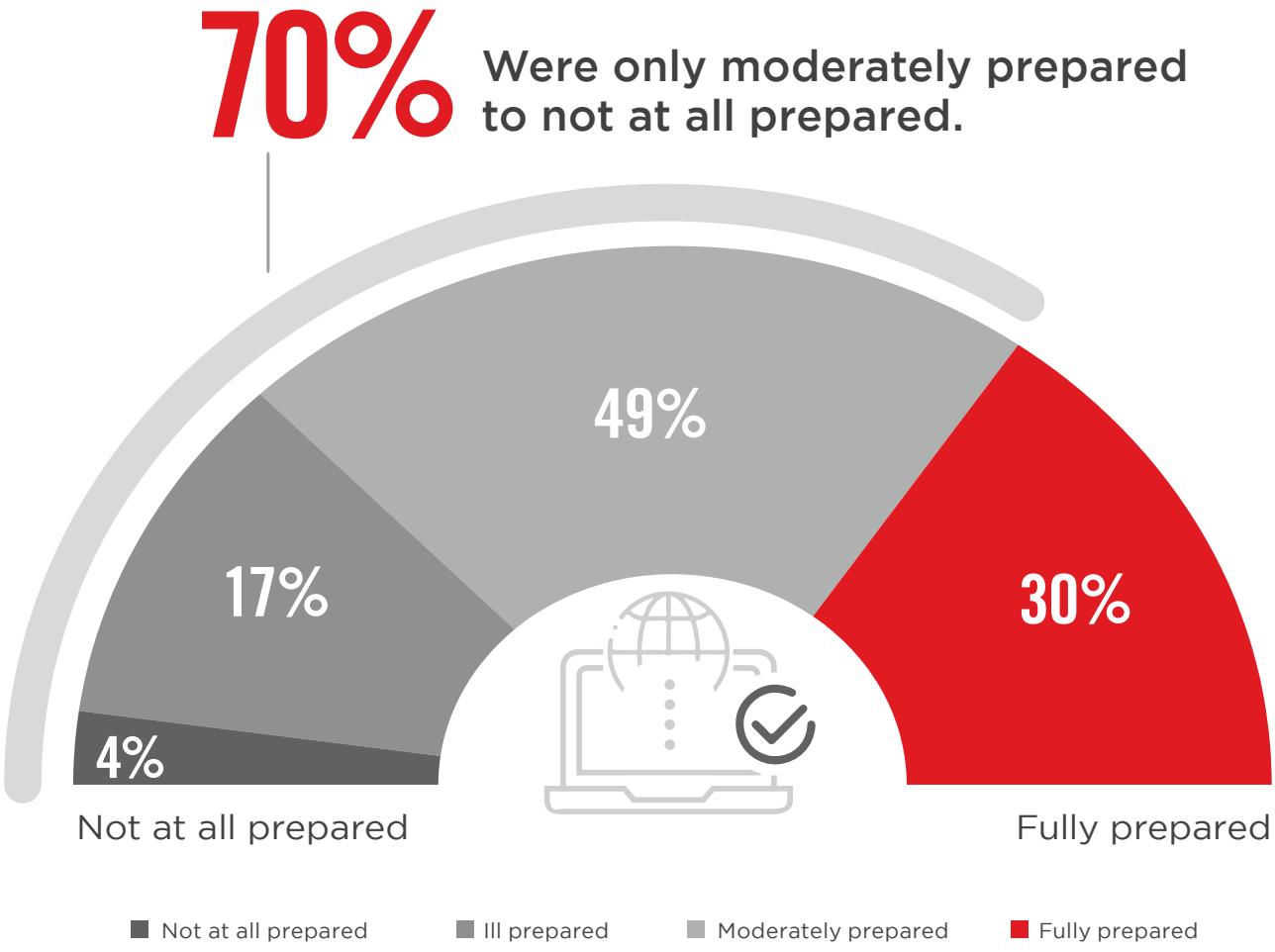
33% Of organizations report they were not sufficiently prepared.



SECURITY PERSPECTIVE

The COVID pandemic highlighted how ill-prepared organizations were for the complete shift to remote working. Seventy percent confirm that they were either not prepared at all or only moderately prepared.

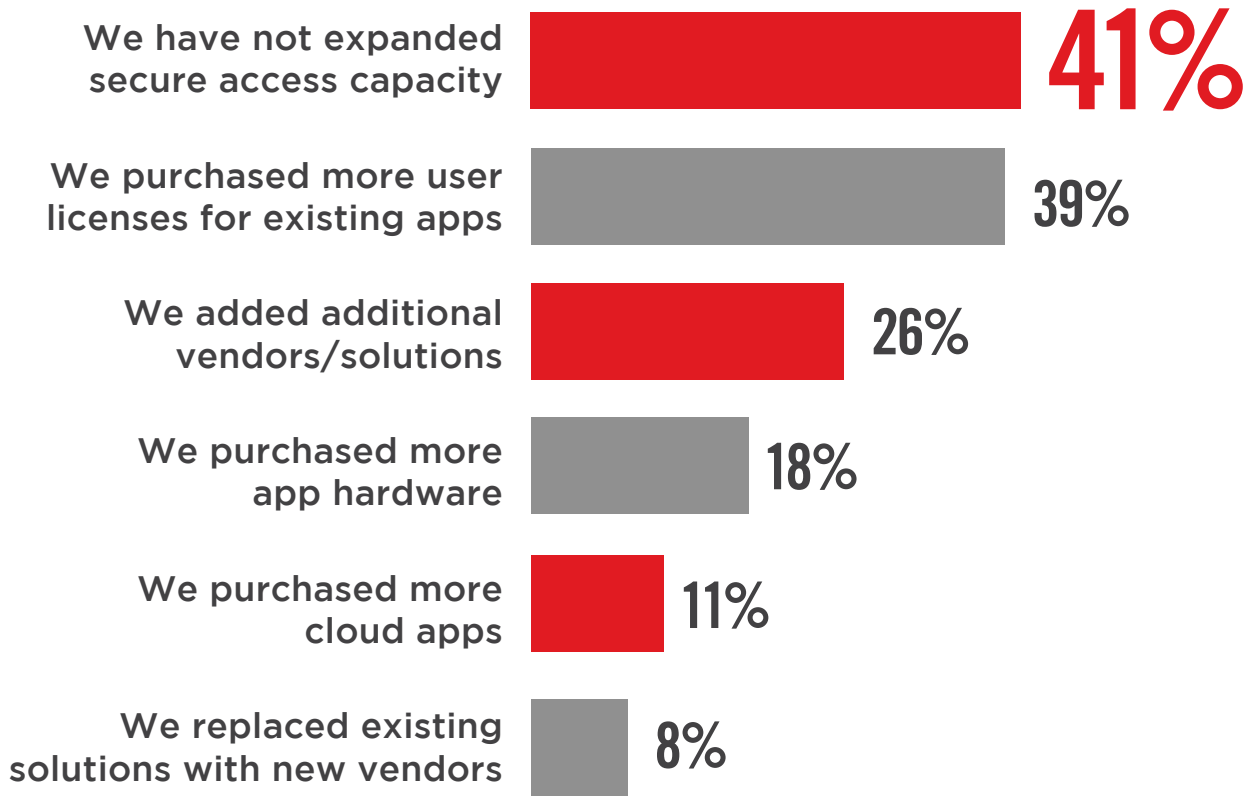
How prepared was your organization for the shift to remote work from a security perspective?



WORKFORCE EXPANSION PATHS

Forty-one percent of respondents did not expand security access capabilities. Of the organizations that expanded secure access capacity, the most frequent motion was to purchase more user licenses for existing apps (39%), followed by adding new vendors/solutions (26%), and purchasing more hardware (18%).

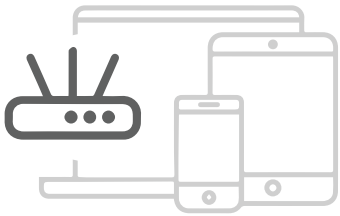
How did you expand secure access capacity?



BARRIERS TO SECURING REMOTE WORK

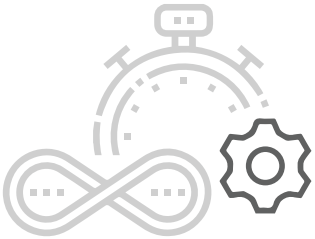
When asked about the biggest impediments to scaling security for remote workforces, organizations named remote work equipment (50%), bandwidth restrictions (37%) and not enough software licenses (26%) as the key barriers.

What have been the biggest impediments to scaling security for your remote workforce?



50%

Equipment for remote work (devices, cameras, accessories, etc.)

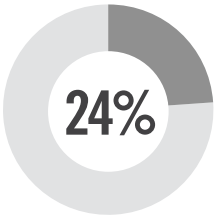


37%

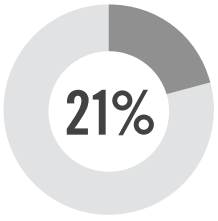
Bandwidth restrictions impacting productivity

26%

Not enough licenses



Logistics of installing agents on employees' personal devices



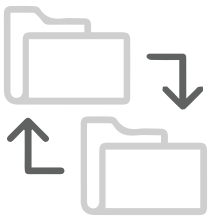
We have not experienced security scaling issues

Other 3%

RISKY APPS

Of the apps used by remote workers, organizations are most concerned with file sharing (68%), web applications (47%), and video conferencing (45%) from a security perspective. This is not surprising, as they are the fundamental business applications that all organizations rely upon.

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



68%

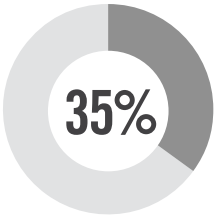
File sharing

47%

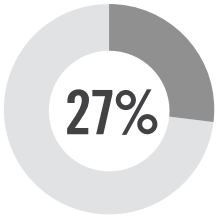
Web applications

45%

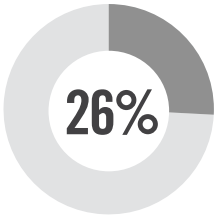
Video conferencing



Messaging



Social media



Websites

Other 2%

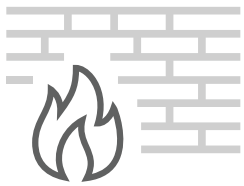
SECURITY CONTROLS IN PLACE

When we asked organizations about security controls, only 34% report to have any endpoint compliance, and 18% have cloud DLP. When organizations enable cloud, BYOD, and remote work, they must deploy the proper security tools to do so safely. Consequently, these numbers, as well as those of solutions like CASB, UEBA, ZTNA, and web filtering, ought to be higher.

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

77%

Anti virus/ anti-malware



77%

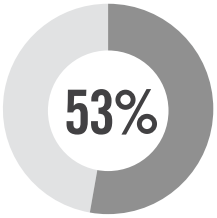
Firewalls

66%

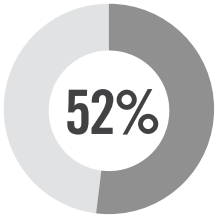
Virtual Private Network
(VPN/SSL-VPN)

66%

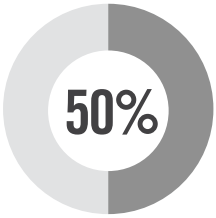
Multi-Factor Authentication
(MFA)



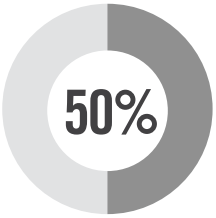
Backup and recovery



Password management



File encryption



Endpoint security (EDR)

Anti-phishing 47% | Single sign-on 45% | Endpoint compliance 34% | Mobile Device Management (MDM) 34% | Web Application Firewall (WAF) 29% | Virtual Desktop Infrastructure (VDI) 26% | Load balancing/Application Delivery Controller (ADC) 24% | Web proxy/web filtering 23% | Cloud Data Loss Prevention (DLP) 18% | Cloud Access Security Brokers (CASB) 16% | User and Entity Behavior Monitoring (UEBA) 11% | Software-Defined Perimeter (SDP) 10% | Zero Trust Network Access (ZTNA) 8% | Other 3%

THREAT VECTORS

The most concerning threat vectors facing remote work environments are malware (72%), phishing (67%) and unauthorized or excessive access privileges (59%).

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

72%

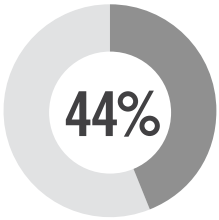
Malware

67%

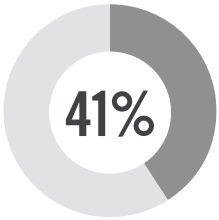
Phishing

59%

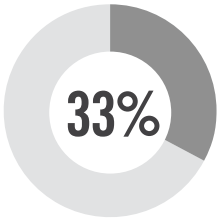
Unauthorized user/ privileged access



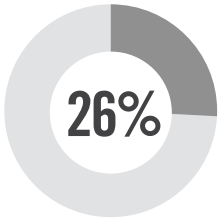
Unpatched systems/ vulnerability exploits



Identity theft



Malicious websites



Insider attacks

Other 5%

KEY SECURITY CHALLENGES

User awareness and training ranks highest (59%) on the list of key security challenges facing organizations that are increasing their remote workforces. This is followed by accessing networks through home or unsecure public WiFi networks (56%) and the use of personal devices (43%).

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

59%

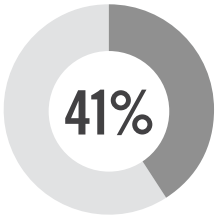
User awareness and training

56%

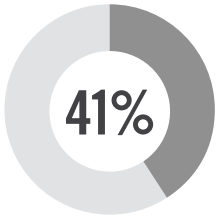
Home/public WiFi network security

43%

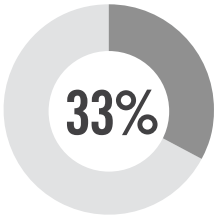
Use of personal devices/BYOD



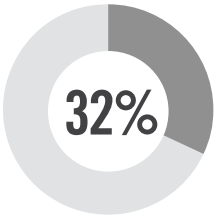
Sensitive data leaving perimeter



Increased security risks



Lack of visibility



Additional cost of security solutions

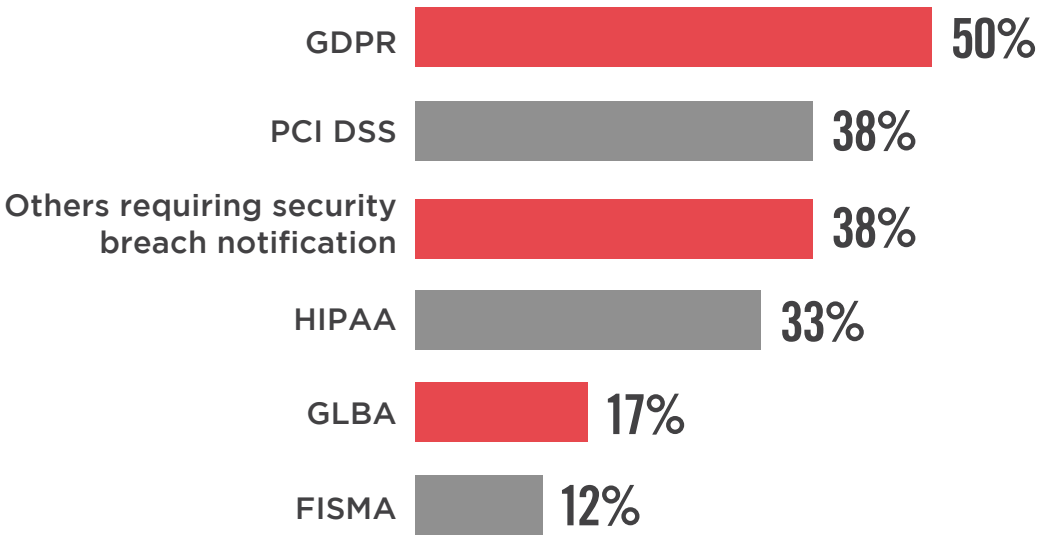
Availability/user experience 30% | Adding capacity 24% | Unsanctioned use of cloud apps 21% | Accountability/audit gaps 21% | None 5% | Other 2%

IMPACT ON COMPLIANCE

Two-thirds of organizations see remote work environments having an impact on their compliance posture (63%). GDPR tops the list of compliance mandates (50%).

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

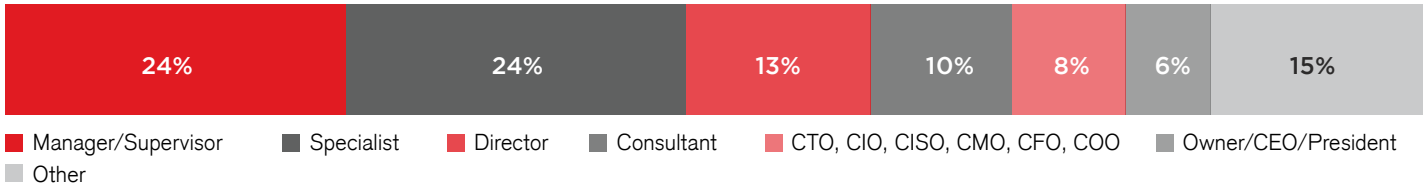
If so, which ones?



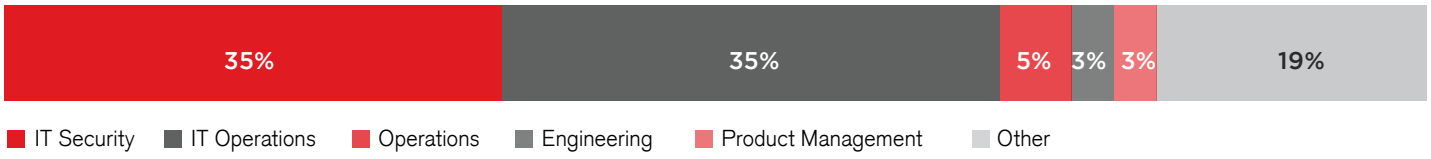
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 413 IT and cybersecurity professionals in the US, conducted in May 2020 to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences for remote workforces in the wake of the 2020 COVID-19 pandemic. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

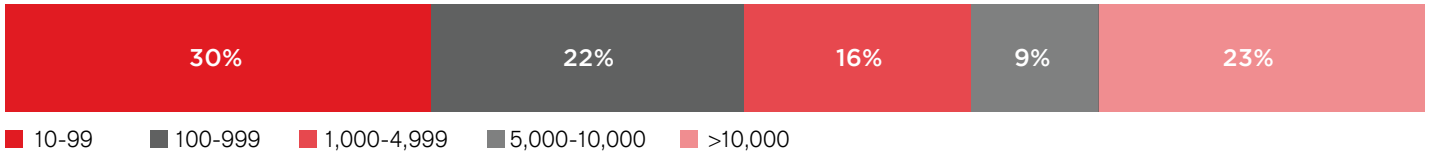
CAREER LEVEL



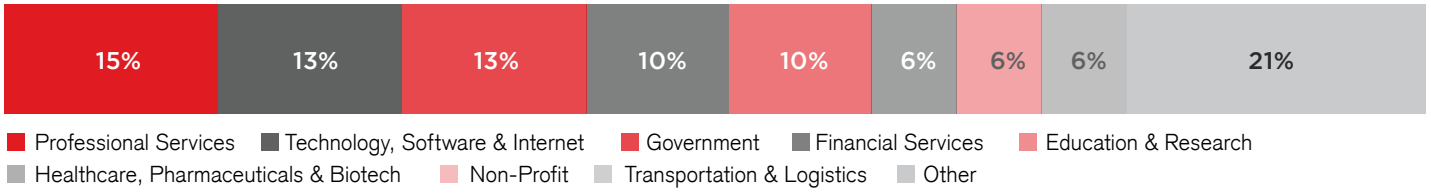
DEPARTMENT



COMPANY SIZE



INDUSTRY



Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

www.bitglass.com