2021

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 ongoing COVID-19 pandemic.

This Remote Workforce Security Report reveals the state of securing the new workforce. The report explores key challenges and unique security threats faced by organizations, technology gaps and preferences, investment priorities, and more.

Key findings include:

- While some organizations are having workers return to the office, the majority (57%) of organizations still have over three quarters of their teams working remotely a year into the pandemic.
- Organizations are highly focused on the network, as network access was the leading concern (69%) related to securing remote workers.
- 55% of organizations agree that relying upon VPN proved challenging throughout the shift to remote work. Using VPN frustrates users, is challenging to scale, and doesn't provide zero-trust security.
- The remote state of operations for organizations calls for an increasingly cloud-centric IT ecosystem. A majority, at 71%, are in agreement that their organization will shift away from on-premises appliances and tools in favor of the cloud for enabling remote work. Timing for this shift is critical and should happen sooner versus later, especially in light of the pressures imposed by the COVID-19 pandemic.

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

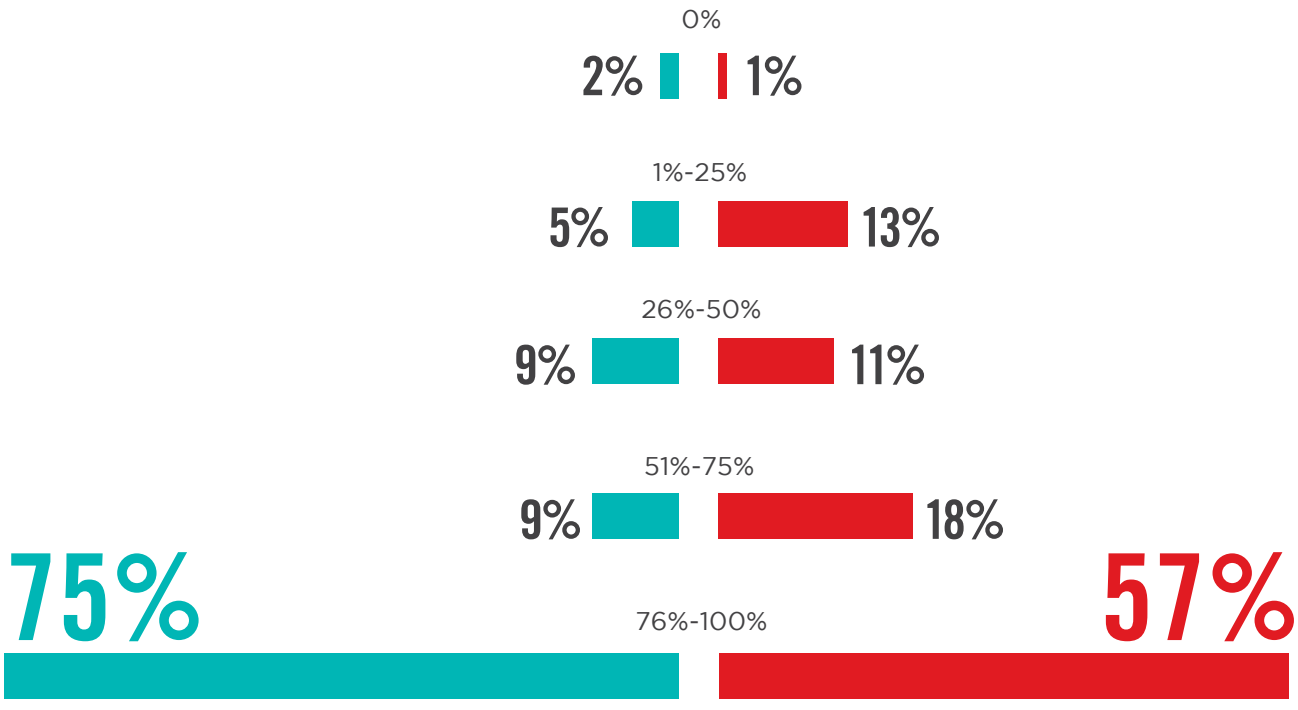
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

DRAMATIC INCREASE IN REMOTE WORKFORCE

Moving forward, there will be a need for a mixed IT and security environment as people will work on and off-premises. While some organizations are having workers return to the office, the majority (57%) of organizations still have over three-quarters of their teams working remotely a year into the pandemic.

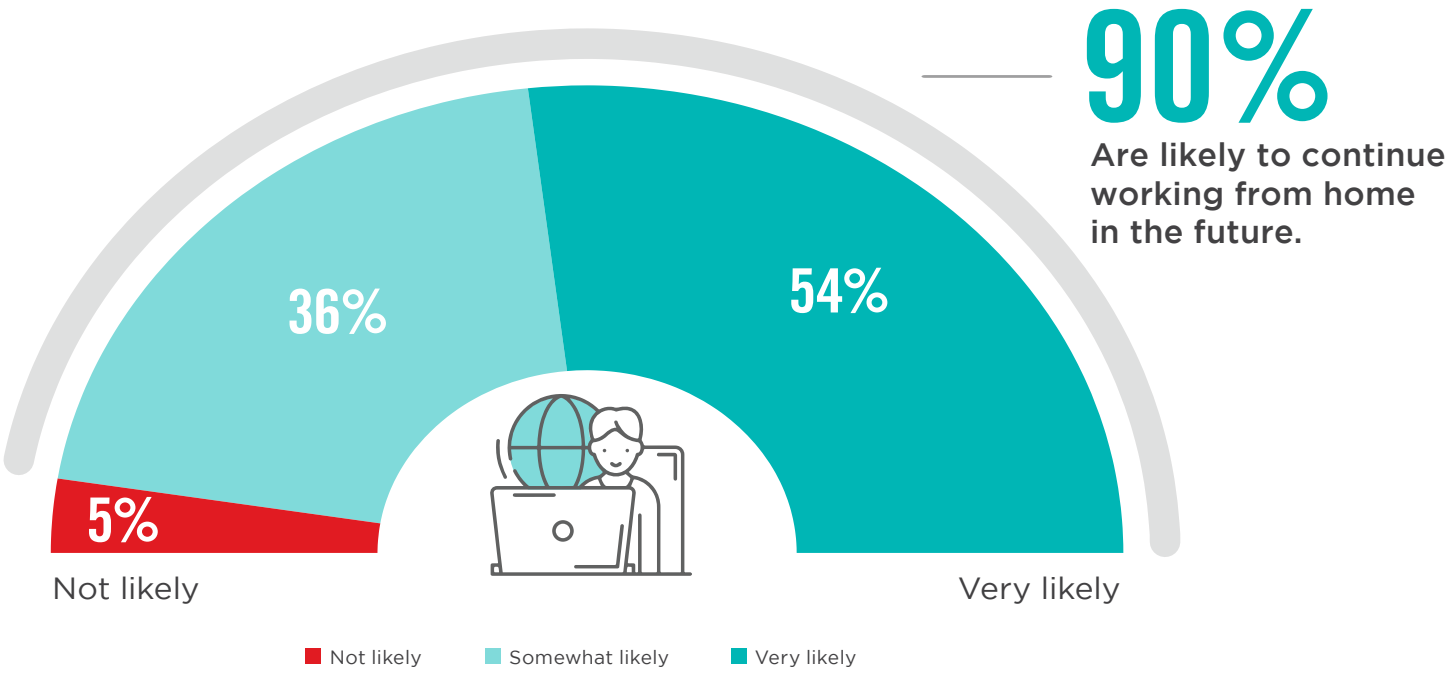
What percentage of your workforce is working remotely/at home NOW during the COVID crisis (on average)?



FUTURE REMOTE WORK

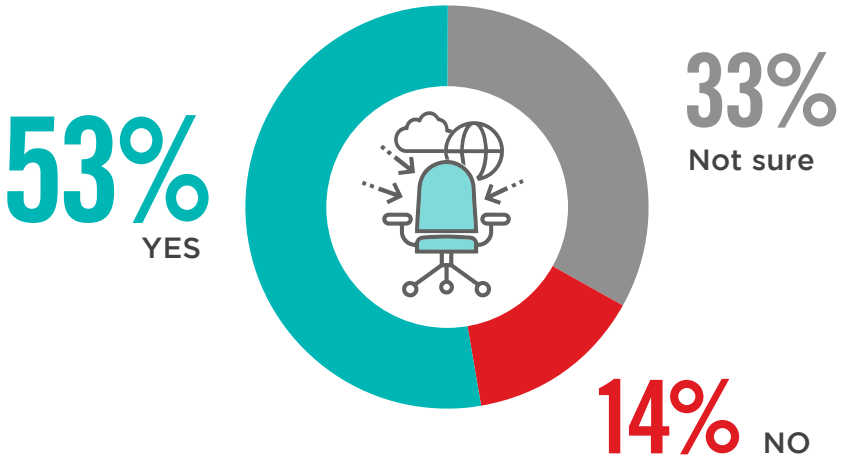
Similarly, a majority of organizations (90%) are likely to continue working from home in the future due to increased productivity benefits. In fact, 53% are looking at making some positions permanently remote after the COVID crisis ends, about 20 percentage points higher than it was when the pandemic started. A mixture of remote and on-premises workers will abound for some time.

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



Not sure 5%

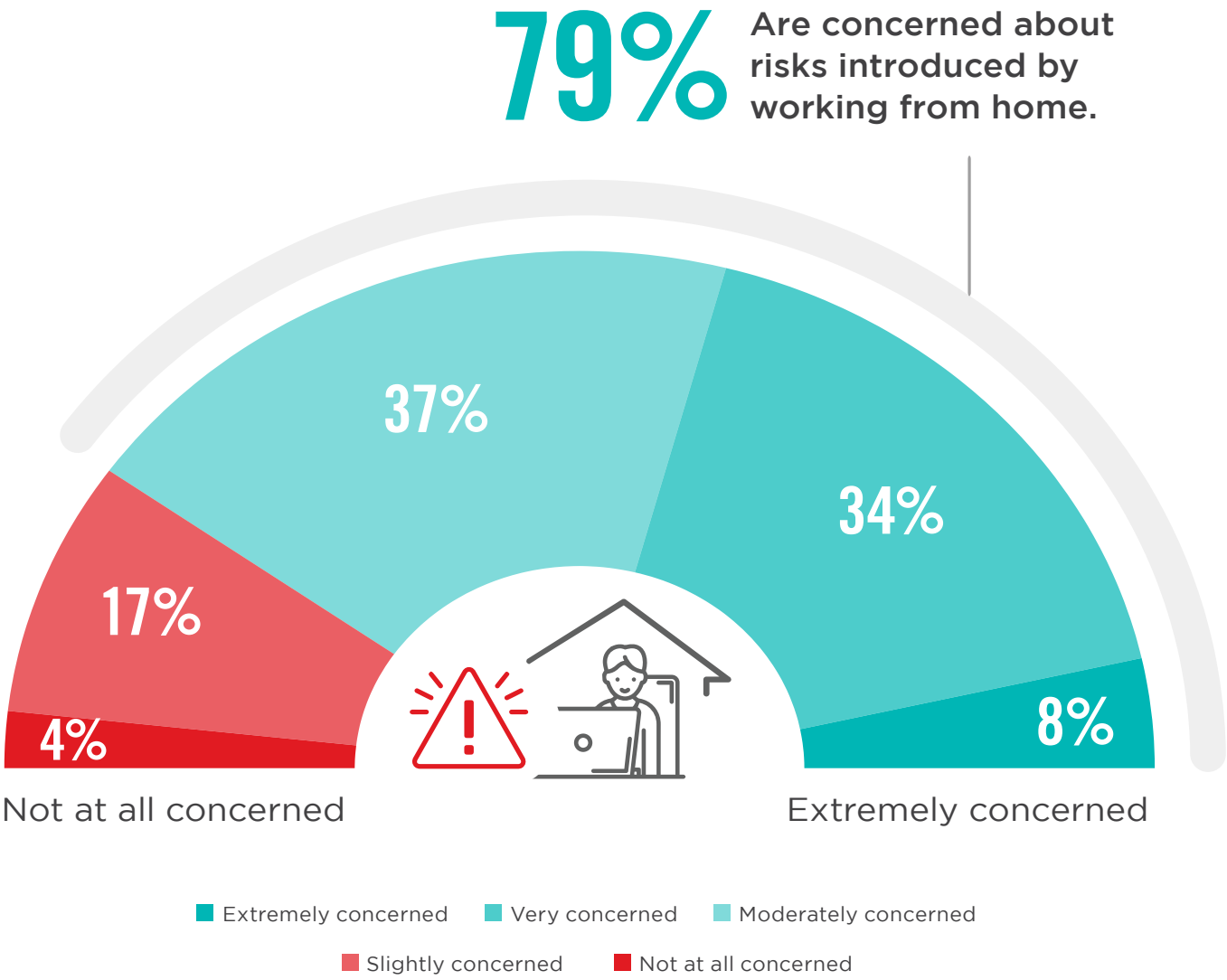
Is your organization considering to make some positions permanently remote (that used to be on-site) after the COVID crisis ends?



SECURITY RISKS CONCERNS

More than three-quarters of organizations are concerned about the security risks introduced by users working from home. Despite experiencing a full year of remote work in response to the global pandemic, organizations are still feeling worried and unprepared when it comes to securing off-premises users.

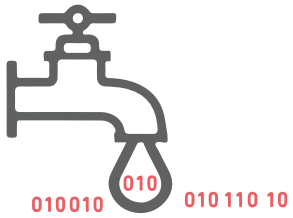
How concerned are you about the security risks introduced by users working from home?



NEW SECURITY RISKS

The biggest remote work security concerns stem from data leaking through endpoints (68%), users connecting with unmanaged devices (59%), and access from outside the perimeter, meaning less anti-malware protection (56%). These concerns are followed by maintaining compliance with regulatory requirements (45%), remote access to core business apps (42%), and loss of visibility of user activity (42%). In other words, there is a wide variety of cybersecurity use cases and concerns that must be addressed by modern organizations.

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



68%

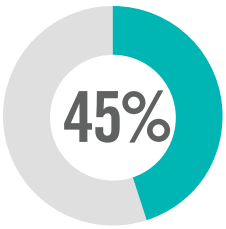
Data leakage to endpoints

59%

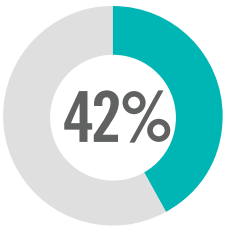
Users connecting with unmanaged devices

56%

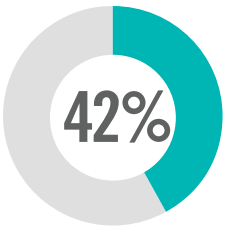
Access from outside the perimeter, meaning less anti-malware protection



Maintaining compliance with regulatory requirements



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



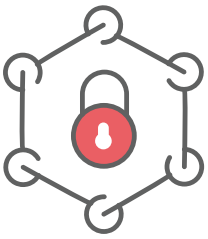
Loss of visibility of user activity

Direct access to cloud-based applications around our IDP 19% | Password reuse across personal devices 18% | Other 4%

SECURITY PERSPECTIVE

Organizations are primarily focused on securing their networks (69%) while employees work remotely. While it's good that 60% of respondents referenced BYOD as a top priority, there appears to be too little concern around securing cloud resources like SaaS apps (38%), which are frequently used to house, process, and share sensitive corporate data.

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

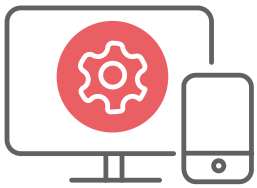


69%

Network access

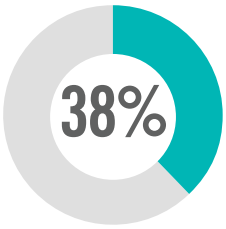
60%

BYOD/ personal devices

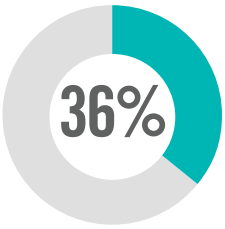


51%

Managed devices



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



On-premises apps

Custom apps

The web 16% | IaaS instances 10%

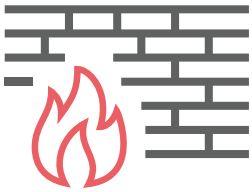
SECURITY CONTROLS IN PLACE

Organizations are using a variety of security controls to secure remote work but most are still thinking solely in terms of legacy tools that are not well suited for the modern enterprise. The top three controls were endpoint anti-virus (80%), firewalls (72%), and VPN (70%), while more appropriate tools like ZTNA (20%), cloud DLP (20%), and CASB (18%) were far less common.

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

80%

Anti-virus/ anti-malware

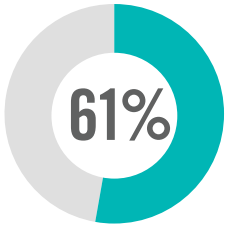


72%

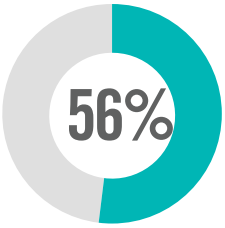
Firewalls

70%

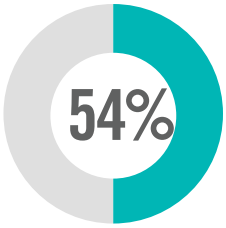
Virtual Private Network (VPN/SSL-VPN)



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%

ADHERENCE TO SECURITY POLICIES AND PROTOCOLS

The three top policies and protocols that employees are most resistant to complying with include Mobile Device Management (MDM) (32%), followed by multi-factor authentication (30%) and Virtual Private Networks (VPN) (26%). Despite being one of the three controls that employees resist the most, VPN is still one of the most commonly used tools, as mentioned on the previous page.

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

32%

Mobile Device Management (MDM)

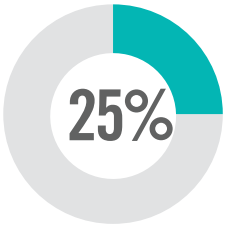
30%

Multi-Factor Authentication (MFA)

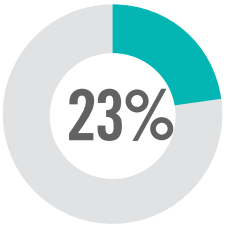
26%

Virtual Private Network (VPN/SSL-VPN)

File encryption



Password managers



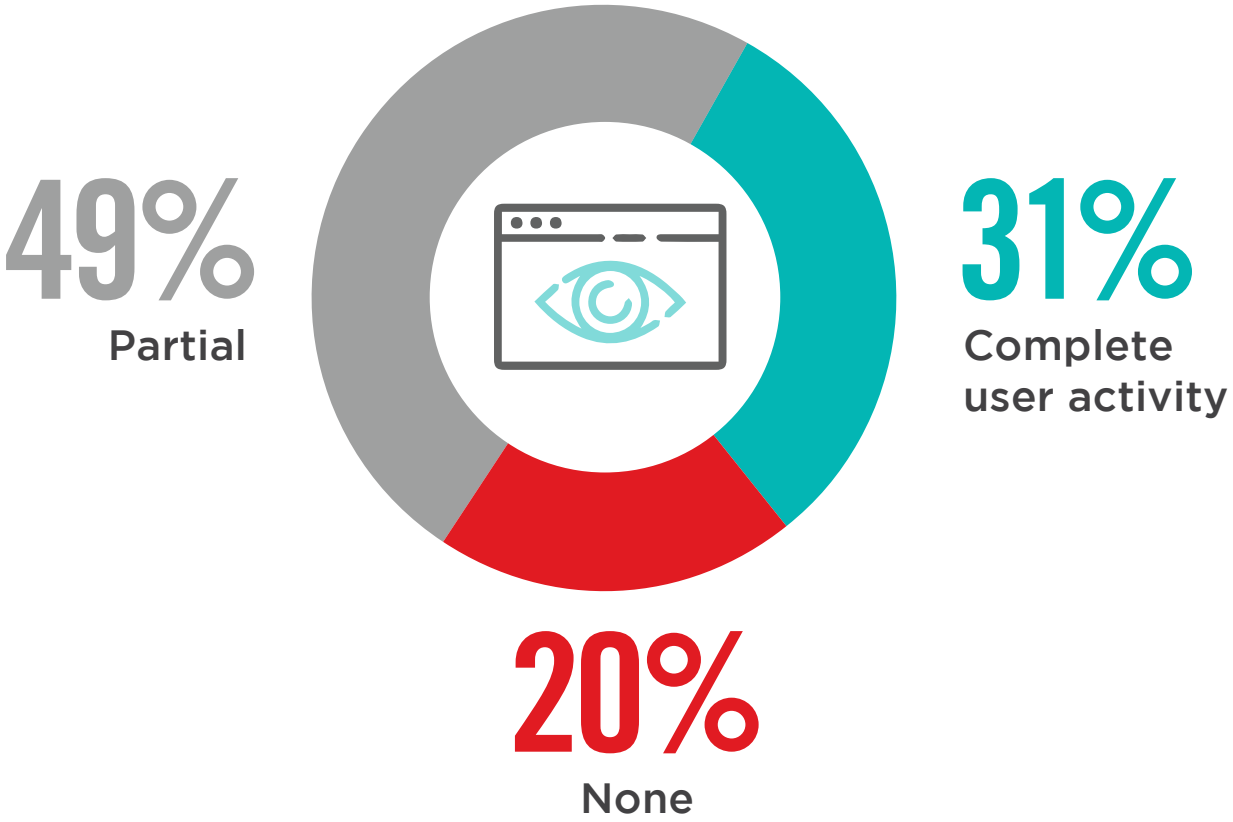
Anti-phishing

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% | None 10% | Credential exposure monitoring/dark web monitoring 9% | Software-Defined Perimeter (SDP) 7% | Load balancing/ Application Delivery Controller (ADC) 4% | Other 3%

VISIBILITY INTO USER ACTIVITY

We asked what visibility organizations have over user activity if VPN is disabled by a remote worker. Sixty-nine percent of organizations have either partial or nonexistent visibility when employees disable VPN.

What visibility do you have over user activity if VPN is disabled by a remote worker?



VPN IS PROVING CHALLENGING

Despite their continued emphasis on using VPN to secure off-premises network access, 55% of organizations agree that relying upon the tool proved challenging throughout the shift to remote work. Using VPN frustrates users, is challenging to scale, and doesn't provide zero-trust security.

Do you agree with the following statement: "Throughout the shift to remote work, leaning upon VPN has proven challenging."

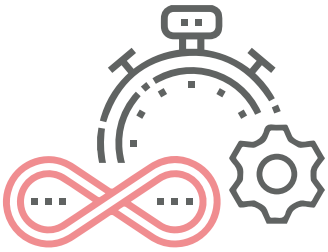
55%

Agree that throughout the shift to remote work, leaning upon VPN has proven challenging.

BARRIERS TO SECURING REMOTE WORK

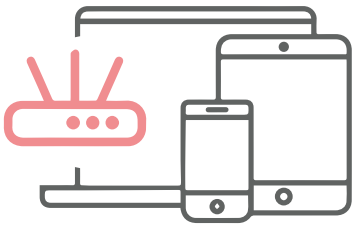
While the primary barrier to securing remote work last year was getting equipment for employees, bandwidth restrictions (41%) were the top barrier this year. This highlights the challenges associated with appliance-based tools, like VPN, which lack sufficient scalability for today's dynamic business world. Similarly, using agents to secure personal devices (29%) is an example of relying upon a poorly suited tool for an important use case.

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



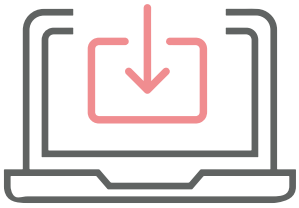
41%

Bandwidth restrictions impacting productivity



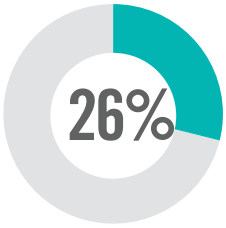
39%

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

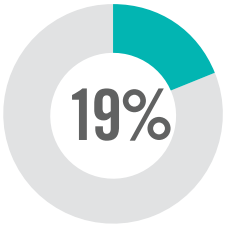


29%

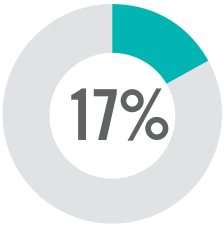
Logistics of installing agents on employees' personal devices



We have not experienced security scaling issues



Not enough security staff



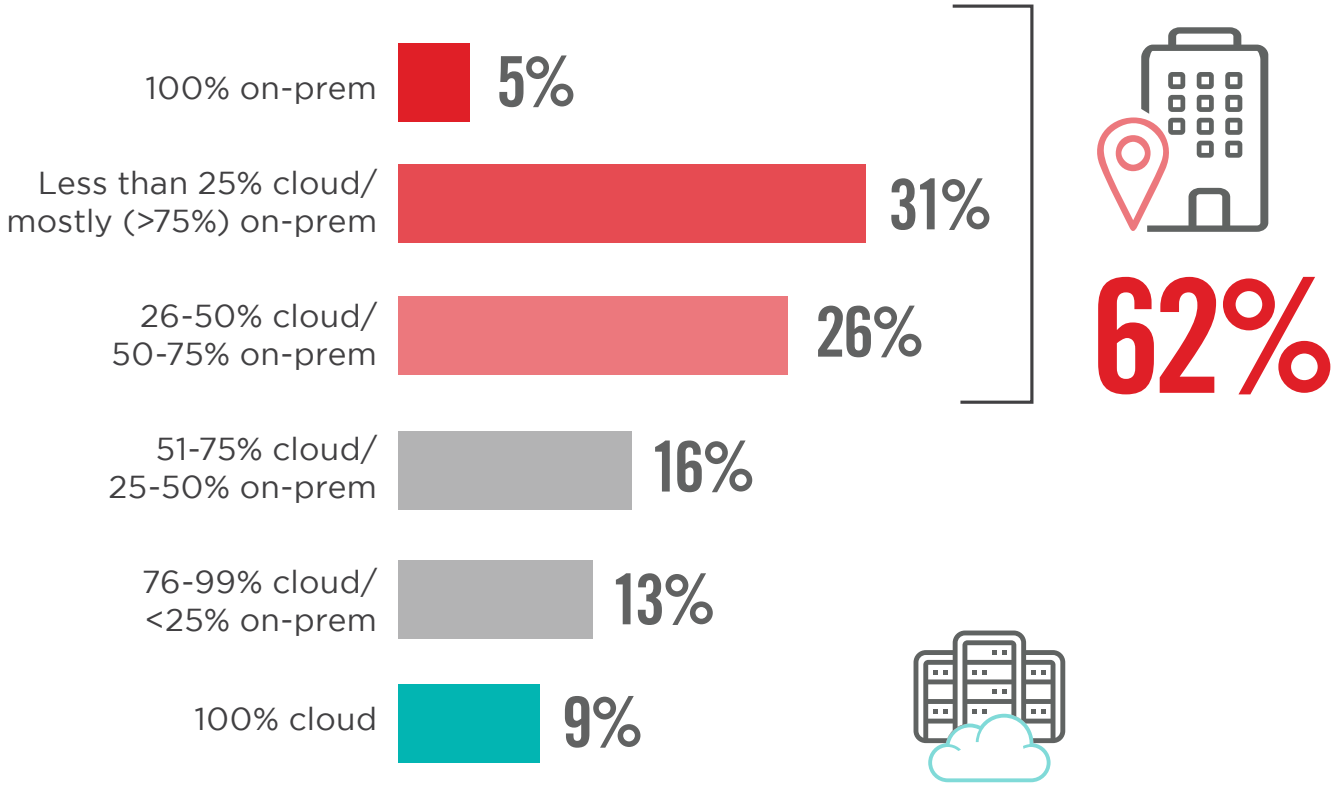
Monetary requirements for buying more or better security appliances

Not enough licenses 16% | Not enough security budget 12% | The logistical challenge of installing more or better security appliances 11% | Other 1%

CLOUD VS ON-PREM APPS

Organizations are still relying on legacy security systems and tools. When asked what percentage of their application stack is in the cloud vs. on-premises, a majority of organizations (62%) report they have less than half of their applications in the cloud. Enabling the modern workforce requires more flexible IT ecosystems and calls for increased reliance on the cloud (as well as cloud security tools).

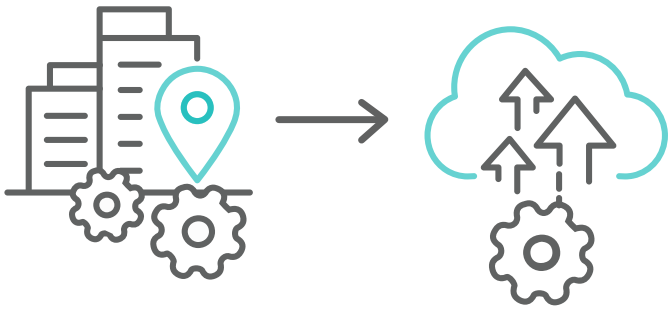
What percentage of your app stack is cloud vs. on-premises?



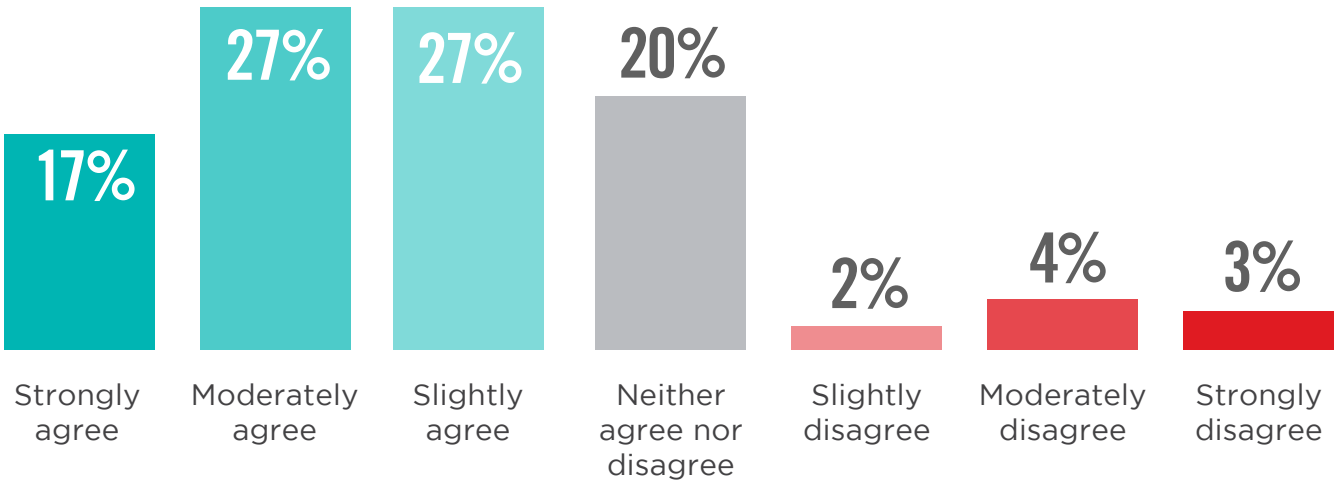
REMOTE WORKING ACCELERATES TRANSITION TO CLOUD

The remote state of operations for organizations calls for an increasingly cloud-centric IT ecosystem. A majority, at 71%, are in agreement that their organization will shift away from on-premises appliances and tools in favor of the cloud for enabling remote work. Timing for this shift is critical and should happen sooner versus later, especially in light of the pressures imposed by the COVID-19 pandemic.

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



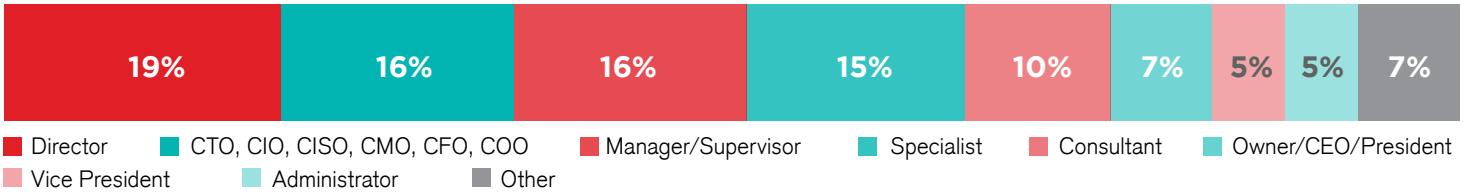
71% Agree with organizations shifting away from on-premises appliances and tools in favor of the cloud for enabling remote work.



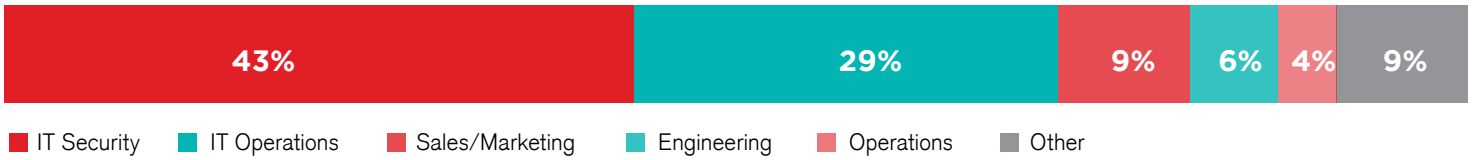
METHODOLOGY & DEMOGRAPHICS

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.

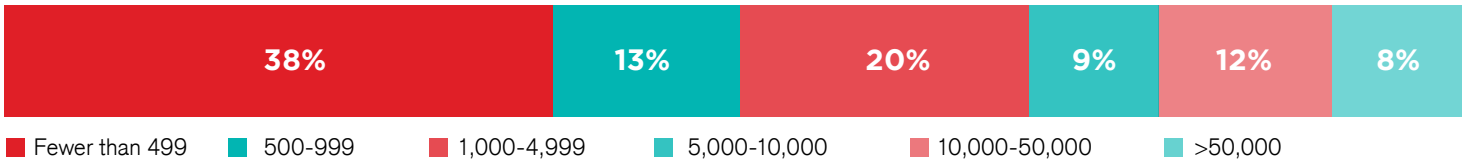
CAREER LEVEL



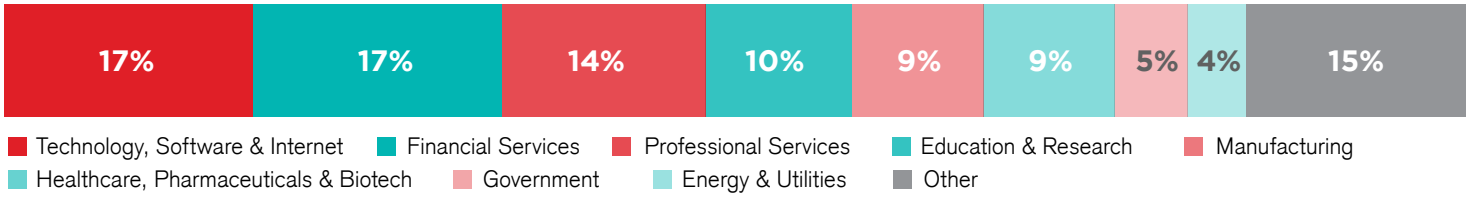
DEPARTMENT



COMPANY SIZE



INDUSTRY



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