2020

REMOTE WORK FROM HOME CYBERSECURITY REPORT

Cybersecurity INSIDERS

Research Sponsor

Pulse Secure®

OVERVIEW

Secure Access solutions keep businesses running by enabling safe remote computing and connecting people and devices to the data center and cloud applications — even during the most unpredictable circumstances.

As the impact of the Coronavirus (COVID-19) intensified and became a pandemic, the World Health Organization suggested that citizens work from home, and avoid using public transportation and office environments as a precaution to mitigate the spread and risk of infection.

At the start of 2020, government and local officials across the globe began advising and requiring citizens to shelter in place and cease on-premises work for all but essential businesses. Companies initiated immediate actions to expand and facilitate remote work from home (WFH) capabilities.

Beyond potentially impacting user productivity, this emergency workplace shift and rapid need for remote work capacity threatened IT infrastructure, business continuity and information security.

This 2020 Remote Work From Home Report, sponsored by Pulse Secure and produced by Cybersecurity Insiders, offers an in-depth perspective on how enterprises transitioned workers and resources, and reveals WFH cybersecurity challenges, concerns, strategies, and anticipated outcomes. The survey, conducted in May of 2020, polled over 400 IT security decision-makers, practitioners, and companies of varying sizes across multiple industries. The survey found that 84% of companies anticipate broader and permanent remote work and nearly one-third plan to increase their budget for secure access in the near-term.

Key findings include:

- More than a 3x increase in WFH user capacity expansion with over 75% of organizations providing nearly 100% coverage
- 33% of businesses were insufficiently prepared for emergency remote secure access
- 54% will accelerate more workflows and apps to the cloud
- 38% of organizations experienced productivity gains and other benefits
- 84% anticipate broader and permanent WFH programs
- Over half expect to increase a secure access budget over the next twelve months (beyond April 2020)
- 66% expect increased WFH security threats and 63% foresee that WFH could expose compliance risks
- Malware, phishing, unauthorized user and device access, and unpatched systems were perceived as the highest WFH attack vectors
- Anti-virus/malware, firewall, SSL VPN, multi-factor authentication and backup were the top employed solutions to ensure WFH security/business resiliency

Many thanks to Pulse Secure for supporting this important research project.

We hope you find this report informative and helpful as you continue your efforts to protect your IT investments, ensure business continuity, and safeguard your employees.

Thank you,

Holger Schulze

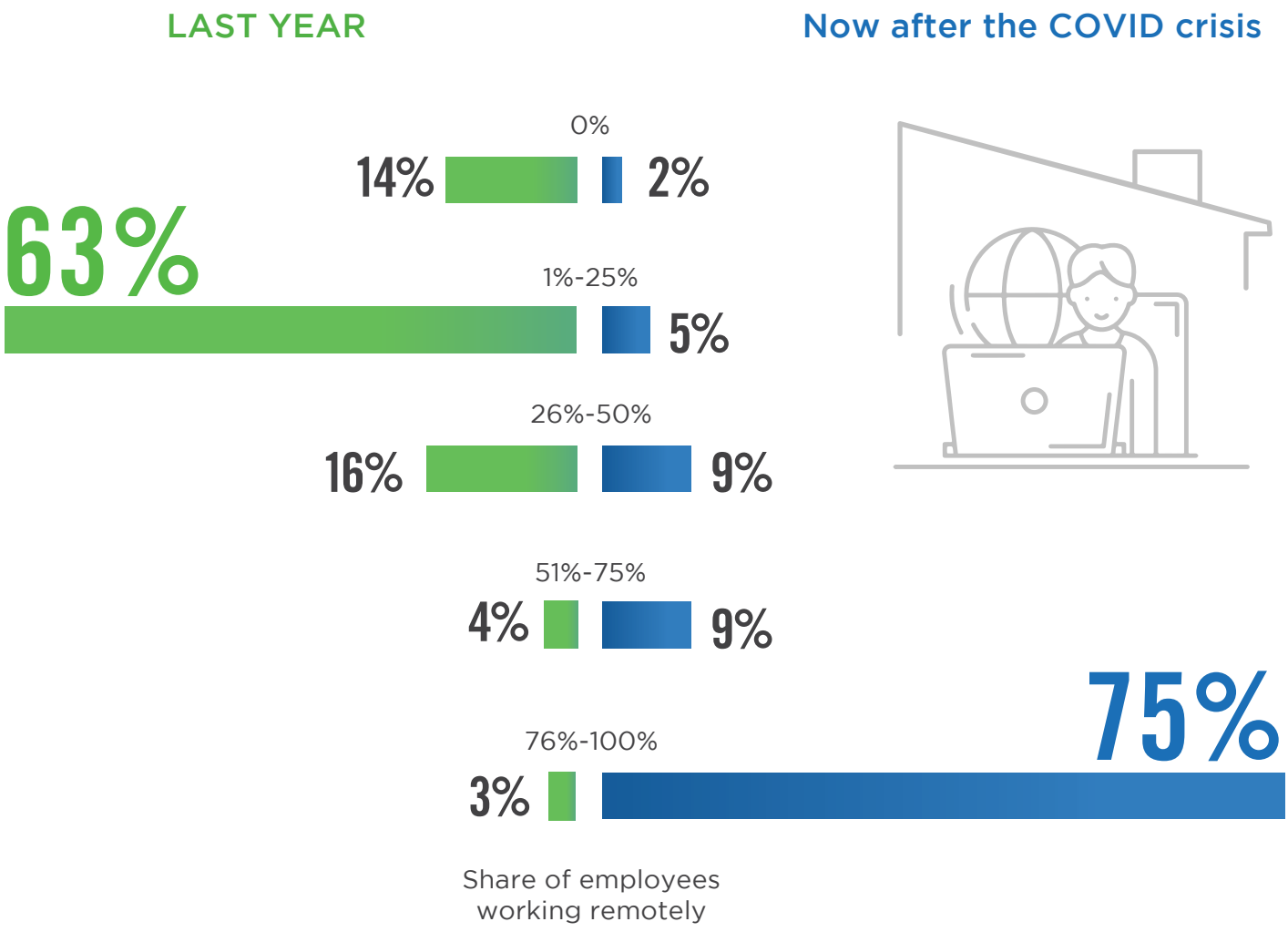
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

EXPLOSIVE 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 up to a 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?

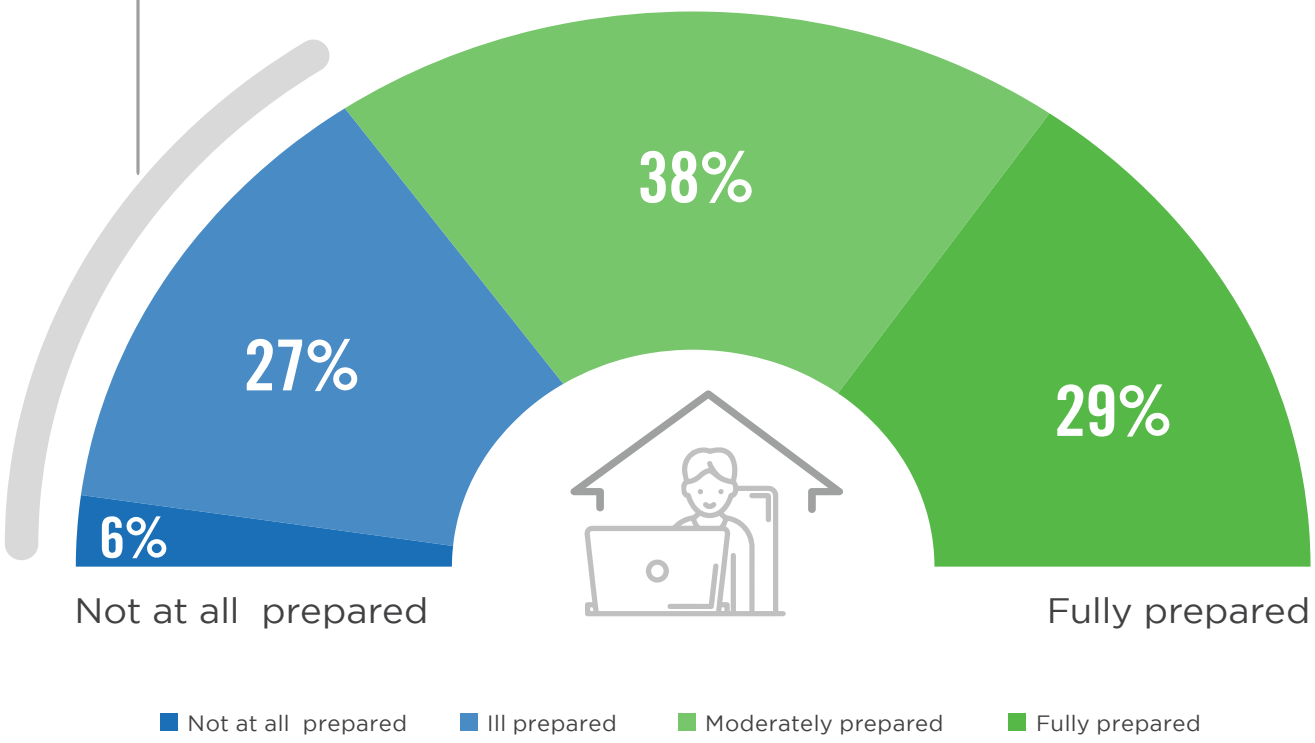


READINESS FOR REMOTE WORK

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 to a remote workforce?

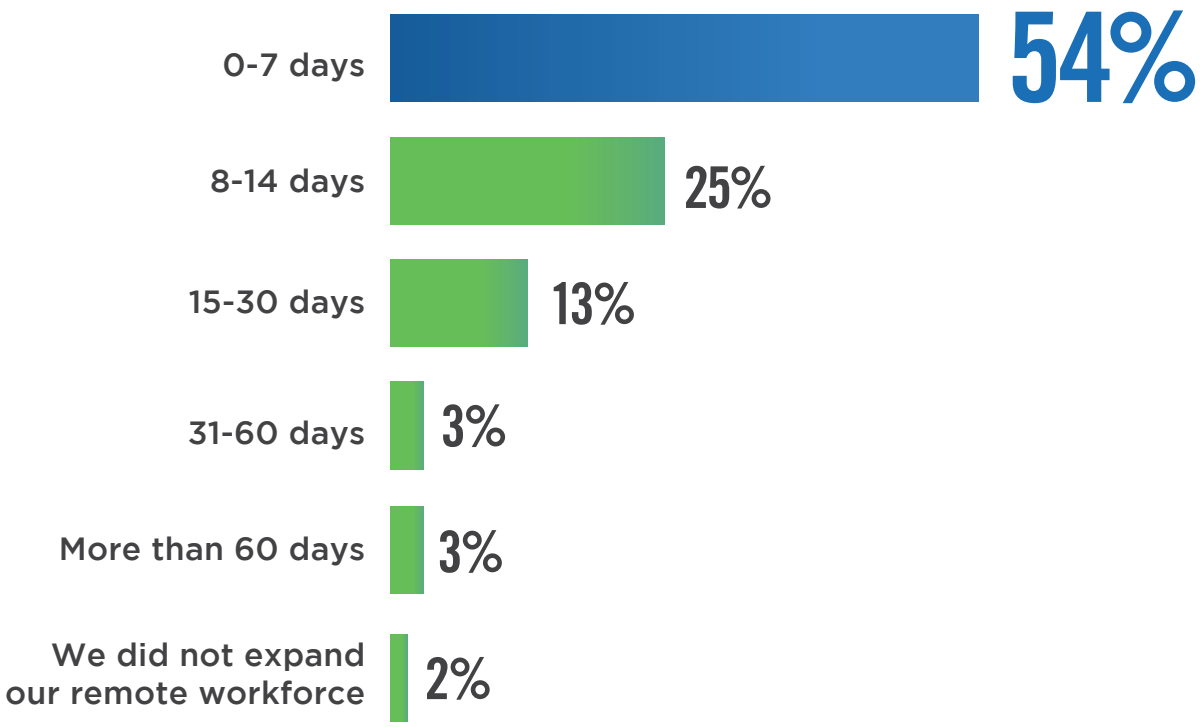
33% Of organizations report they were not sufficiently prepared.



DAYS TO EXPAND REMOTE CAPACITY

A majority of organizations (54%) say they successfully expanded capacity to fully support the expanded workforce in seven days or less.

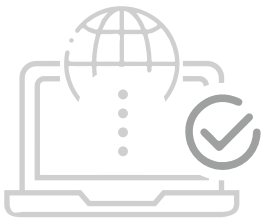
How many days did it take your organization to expand capacity to fully support the recently expanded remote workforce?



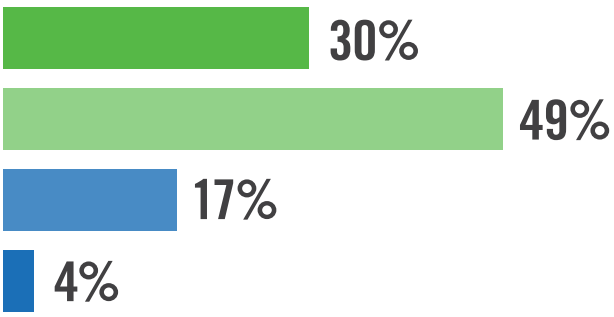
REMOTE WORK SECURITY PERCEPTIONS

While 79% of organizations believe they had adequate WFH security preparations, two-thirds of organizations in this survey (69%) are concerned with the security risks by users working from home.

How concerned are you about the security risks introduced by users working from home and how prepared was your organization for the shift to remote work from a security perspective?

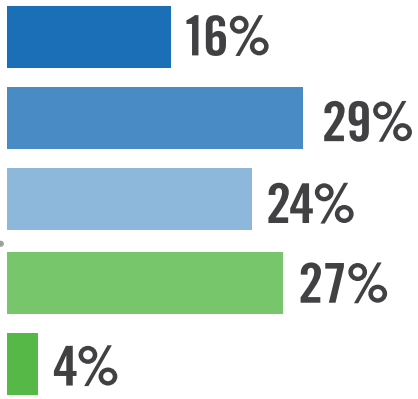


79% Of organizations had adequate WFH security preparations.



Fully prepared
Moderately prepared
Not at all prepared
Ill prepared

69% Are concerned with WFH security risks.



Extremely concerned
Very concerned
Moderately concerned
Slightly concerned
Not at all concerned

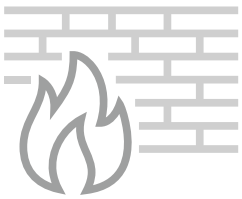
SECURITY CONTROLS IN PLACE

The top security controls in place to protect remote work/work from home are anti-virus/ anti-malware solutions (77%), firewalls (77%), virtual private networks (66%), and multi-factor authentication (66%).

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

77%

Anti-virus/ anti-malware



77%

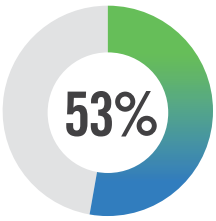
Firewalls

66%

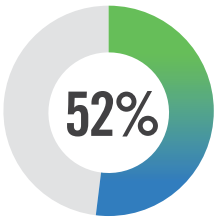
Virtual Private Network (VPN/SSL-VPN)

66%

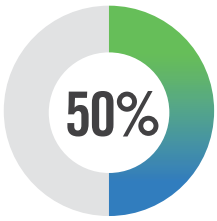
Multi-Factor Authentication (MFA)



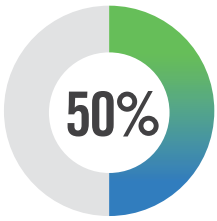
Backup and recovery



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 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%

KEY SECURITY CHALLENGES

User awareness ranks highest (59%) on the list of key security challenges facing organizations that are increasing their remote workforces. This is followed by accessing through home or unsecure public 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%

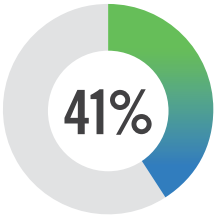
User awareness and training

56%

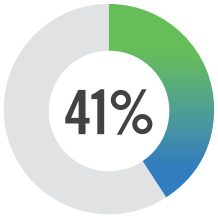
Home/public WiFi network security

43%

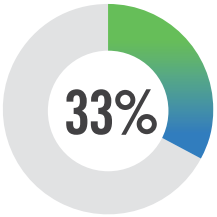
Use of personal devices/BYOD



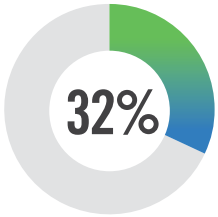
Sensitive data leaving perimeter



Increased security risks



Lack of visibility



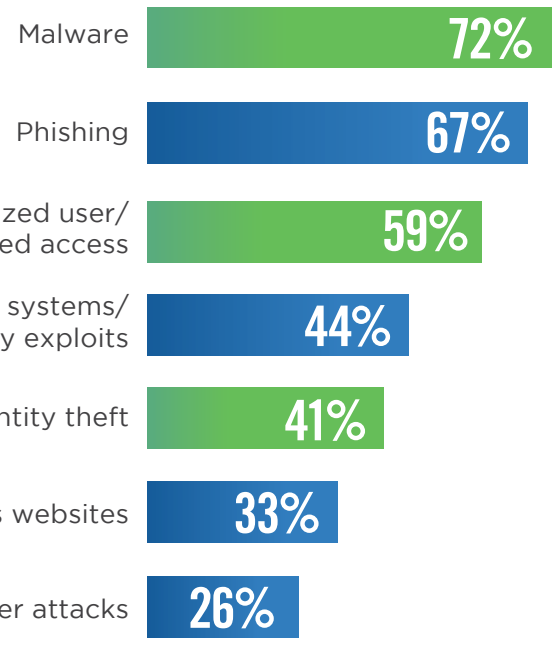
Additional cost of security solutions

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

AMPLIFIED ATTACK VECTORS

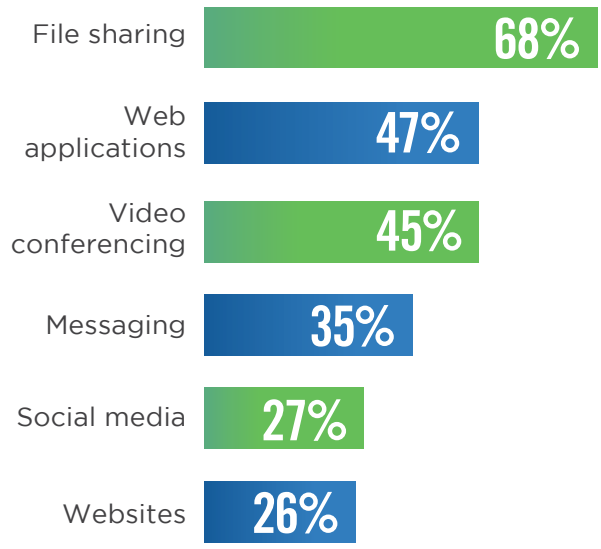
Malware, phishing, unauthorized user/device access, and unpatched systems were identified as top attack vectors due to employees working from home. Among applications contributing to productivity and collaboration, organizations have the most security concerns with file sharing (68%), web applications (47%), video conferencing (45%), and messaging (35%).

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



Other 5%

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



Other 2%

LEVEL OF REMOTE WORK SECURITY

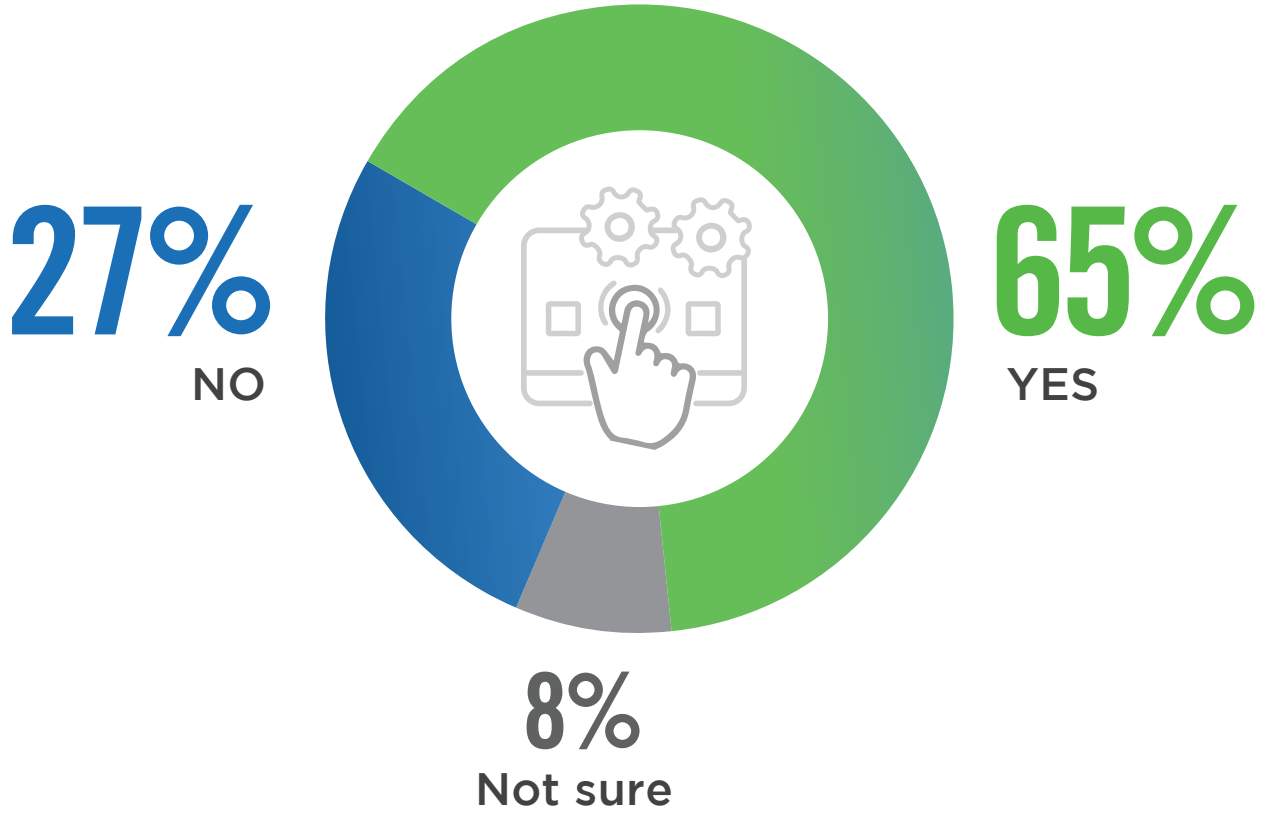
A majority of 78% confirm they enforce the same level of security controls for all roles that access remotely.

Do you enforce the same level of security controls and data management for all roles in the company as they access remotely?

ACCESS FROM PERSONAL DEVICES

Nearly three-quarters of organizations allowed access from personal, unmanaged devices to support work from home, while at least 27% see this scenario as a significant security risk.

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



MIGRATION TO CLOUD

A majority of 54% confirm that the COVID pandemic accelerated migration of workflows to cloud-based apps.

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

REMOTE SECURITY RISK

Organizations are most concerned with protection of sensitive data, especially when accessed by unmanaged endpoints (46%), followed by added exposure to malware (34%).

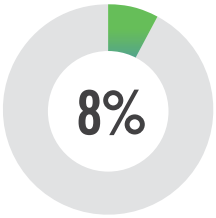
What is the primary risk you're concerned with as your users connect remotely?

46%

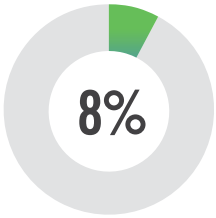
Protection of my data, especially when accessed by unmanaged endpoints

34%

Exposure to malware, phishing or other exploit



Ensure compliance of my regulated users



Audit and oversight of employees conducting work from unmanaged resources

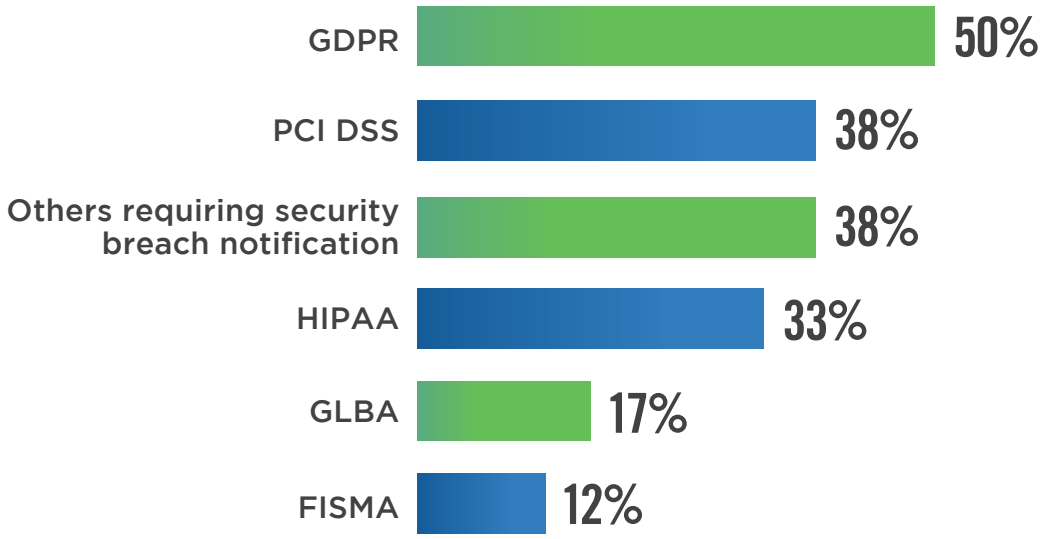
Other 4%

COMPLIANCE IMPACT

Two-thirds of organizations see remote work environments having an impact on their compliance posture.

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

If so, which ones?



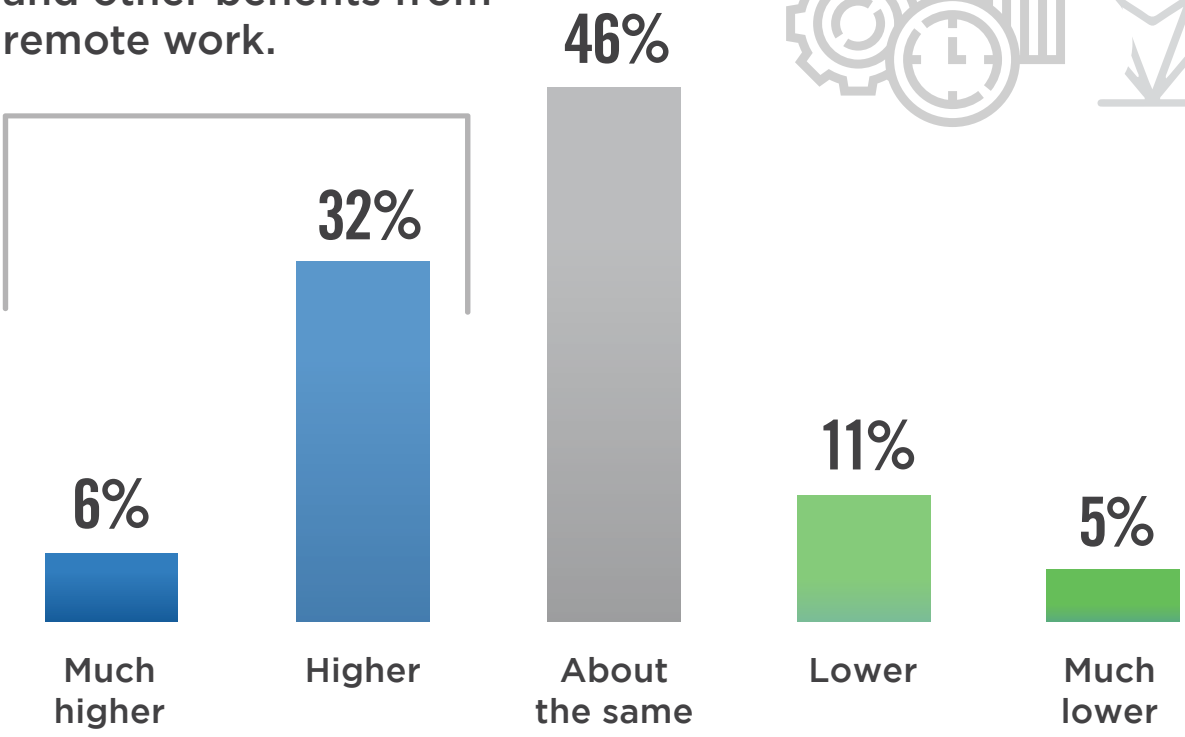
PRODUCTIVITY EFFECTS

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.

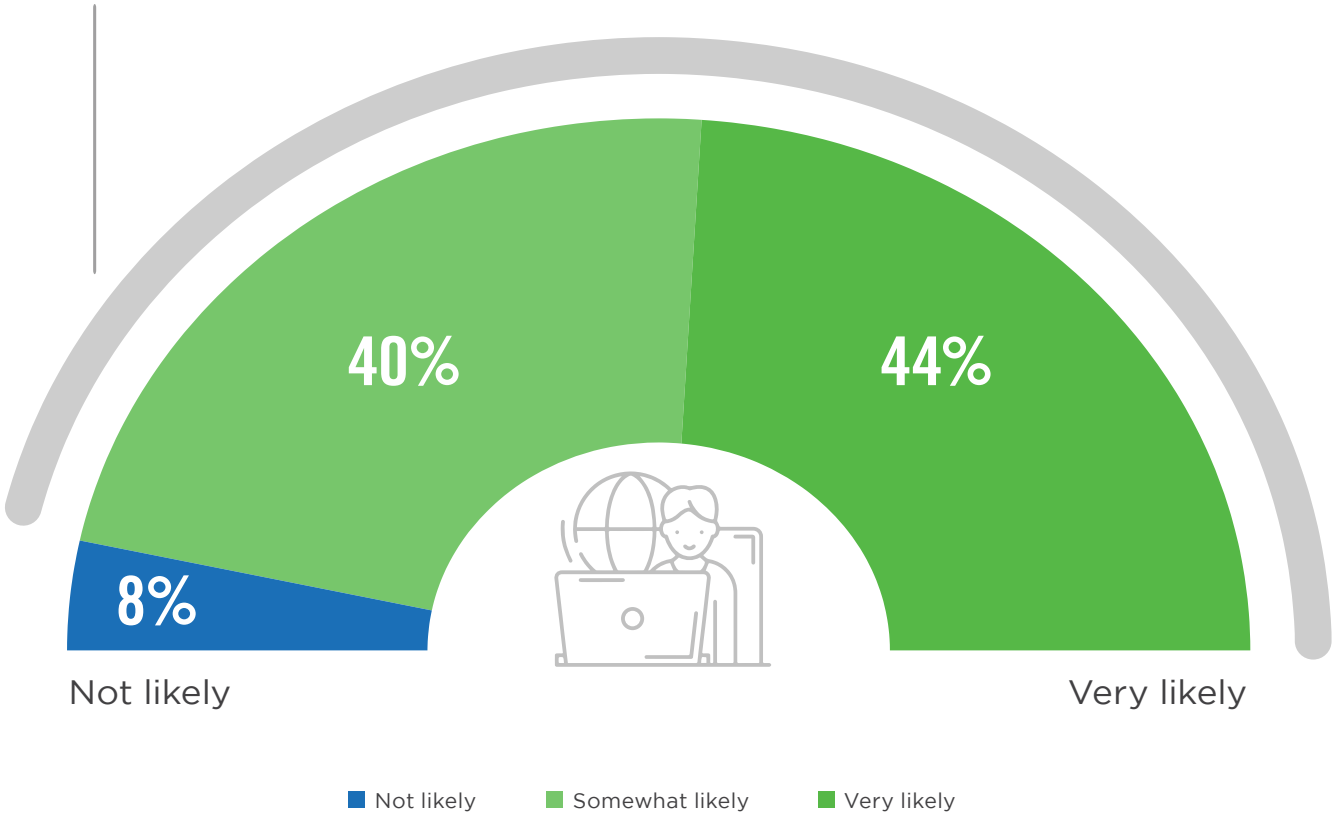


FUTURE REMOTE WORK

A majority of 84% of organizations consider it likely (44% very likely) that they will continue increased work from home capabilities in the future, taking advantage of increased productivity and other business benefits.

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

84% Of organizations consider likely that they will continue increased work from home capabilities in the future.

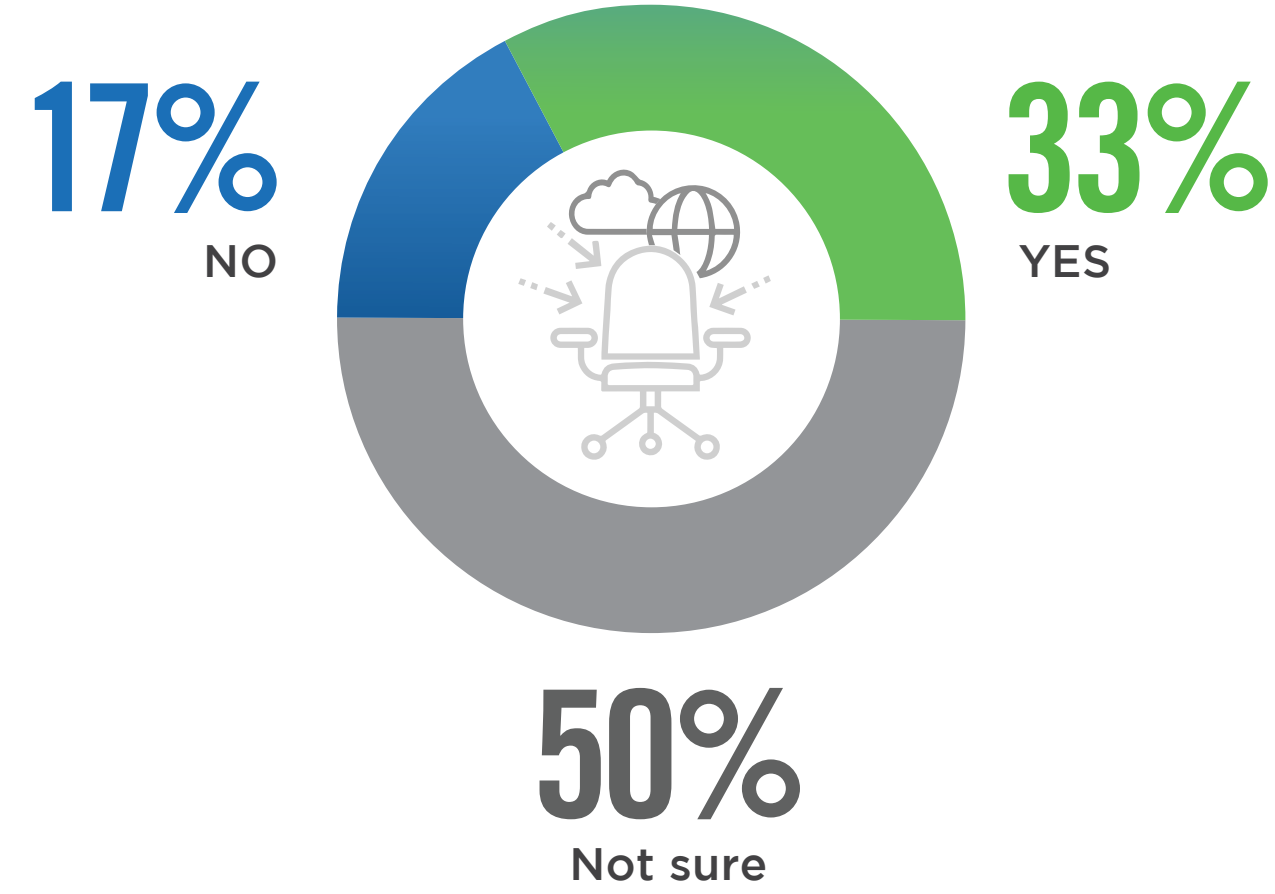


Not sure 8%

MAKING REMOTE WORK PERMANENT

A third of organizations are considering to make some positions permanently remote after the COVID crisis ends.

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

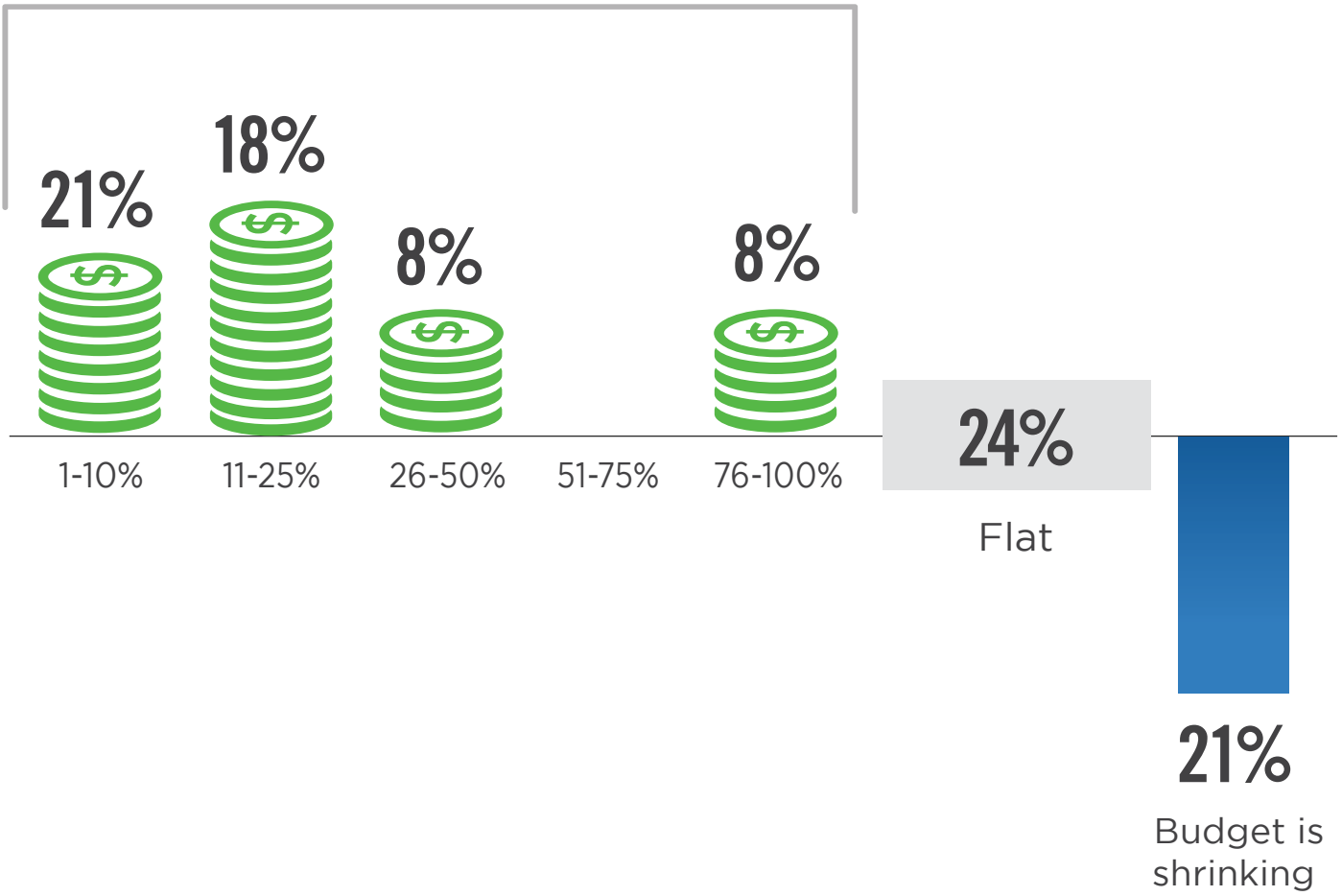


BUDGET TRENDS

A majority (55%) of organizations expect budgets for remote workforce security to increase over the next 12 months (beyond April 2020). For a quarter of respondents, these security budgets will stay flat and only 21% see budgets shrinking.

How is your budget for remote work security controls increasing in the next 12 months?

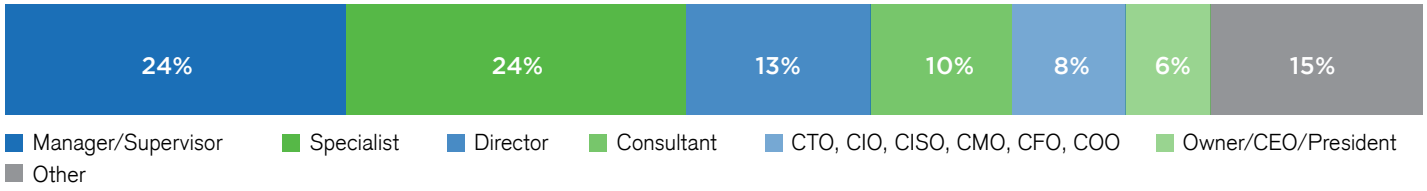
55% Expect budgets for remote workforce security to increase over the next 12 months.



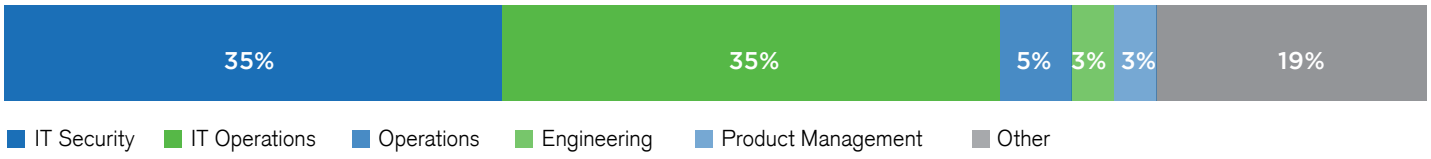
METHODOLOGY & DEMOGRAPHICS

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.

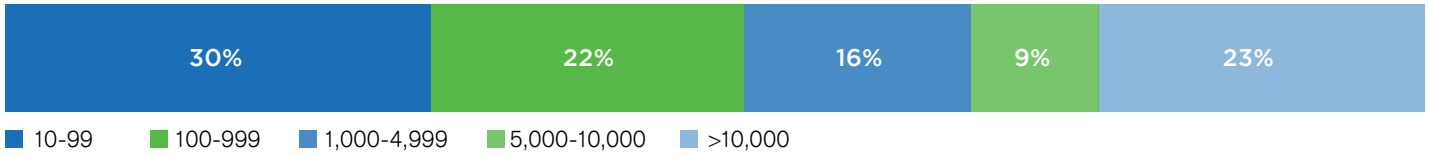
CAREER LEVEL



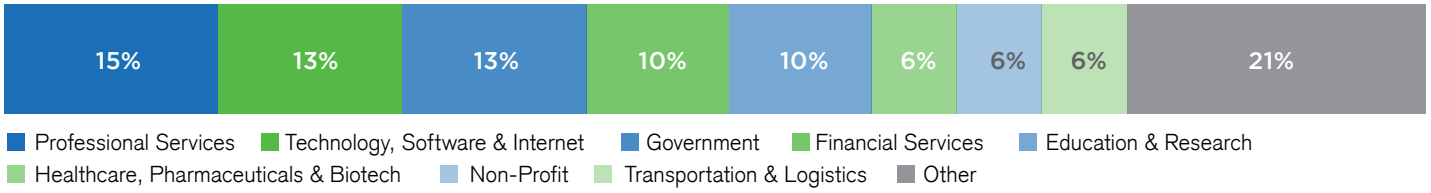
DEPARTMENT



COMPANY SIZE



INDUSTRY



Research Sponsor

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 23,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net