mobile mentor

THE ENDPOINT ECOSYSTEM

2022 NATIONAL STUDY

How employees are using devices in high-risk and highly regulated industries in a post-pandemic world.

CONTENTS

Study Motivation

Navigating trade-offs between endpoint security and employee experience has always been challenging but it has become critical in this post-pandemic world.

Employers are investing in cyber security initiatives, but as the workforce become increasingly distributed and autonomous, employers ***simply aren't keeping up.***

Companies are getting hacked, employees are resigning, and the battle for talent is intensifying.

This inaugural study of **The Endpoint Ecosystem** explores how employees perceive privacy, security, productivity and personal well-being in the modern workplace.

The goal of the study is to **educate and inform** employers how to prevent security breaches, and then how to attract and retain motivated employees.

National Research Study Goals

This study was commissioned, funded, interpreted and published by **Mobile Mentor**. We wanted to know if employees are better or worse off - so we asked them.

We didn't ask their employers or IT leaders, we asked the **people on the front lines:**

- Healthcare
- Finance
- Education
- Government

In late 2021, the **Center for Generational Kinetics** (CGK) conducted this study of 1,500 employees across four regulated industries in the United States and Australia.

Each interview consisted of 25 questions to understand what is really happening, then **prove or disprove** our assumptions about work in a post-pandemic world.

What is the Endpoint Ecosystem?

The combination of devices, operating systems, applications, sign-in experience and supporting processes for employees.

Why the Endpoint Ecosystem matters now?

1. The pandemic forced people to work remotely and to rely more on their devices
2. There was a **500%** increase in cyber-crime which increased the focus on security
3. The global chip shortage forced companies to rely on employees' personal devices (BYOD)
4. In late 2020, companies started hiring and onboarding employees remotely
5. The great resignation in 2021 changed how employers treat their employees

"When the endpoint ecosystem works well, you have a secure, productive and happy workforce".

Denis O'Shea
Founder
Mobile Mentor

Key Findings in Endpoint Security

1. **Many employees are unaware of security risks**
   27% of employees see security policies less than once per year and **39%** receive security awareness training less than once per year.

2. **Passwords are a massive vulnerability**
   Everyone has too many passwords, especially the younger generation. Only **31%** of people use a password management tool. **69%** of people admit to choosing passwords that are easy to remember.

3. **The BYOD risk is huge (bring your own device)**
   The use of personal devices is rampant and many employers have not addressed the security risk. **64%** of people use personal devices for work, but only **31%** have a secure BYOD program.

4. **Shadow IT is out of control (use of unapproved apps)**
   There is a real struggle between security and employee experience. **41%** of people say security policies restrict the way they work. **53%** believe they are more efficient using Dropbox and Gmail.

5. **Remote workers are more secure**
   Compared to office workers, remote employees appear to be more tech savvy, more aware of security and privacy policies, and more careful with their passwords.

Key Findings in Employee Experience

1. **Employees and employers are not aligned**
   72% of employees values their personal privacy over company security. Gen Z don't see (or notice) security policies, but they are hyper aware of privacy policies.

2. **Blurred Lines**
   Employees are using personal devices for work and work devices for personal use. They also allow other family members to use their work devices. This problem is worse for younger generations.

3. **People feel more productive in the office**
   Contrary to our expectations, employees of every generation, and in all four industries, feel more productive working in the office than working at home.

4. **Employee Onboarding is Clunky**
   Employees take an average of three days to get their device(s) setup. Young and remote employees take the longest. Gen Z workers need **3.8** helpdesk calls to get fully setup.

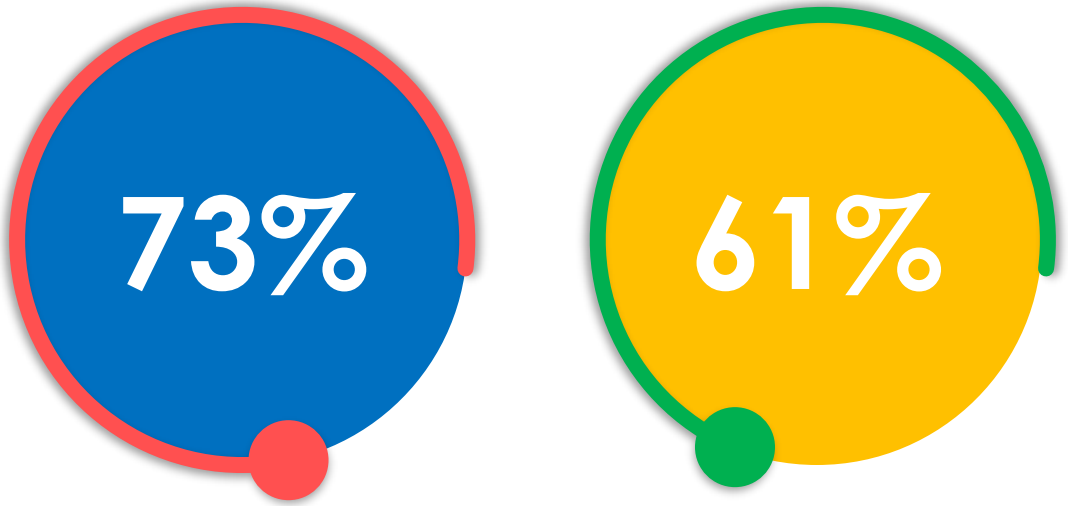
5. **Gen Z presents a flight risk**
   Many Gen Z workers were onboarded remotely during the pandemic, and they view their employers through a unique lens. **66%** perceive other companies are doing a better job with technology.

Endpoint Security
Part One

Visibility of Security Policies

Less than half of all respondents see a security policy every time they log on to their computer.

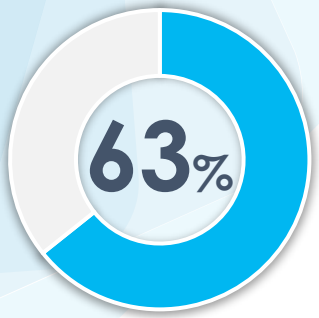
- In the US, **61%** of Financial employees see security policy every time they log on.
- In AU, **73%** of Government employees see security policy every time they log on.
- Education and Healthcare employees are least likely to see security policies.



***Insight**: Employees **don't actually read** security policies, they **just click to agree**. More effective reminders would be very short practical tips or a thought-proving question on security.*

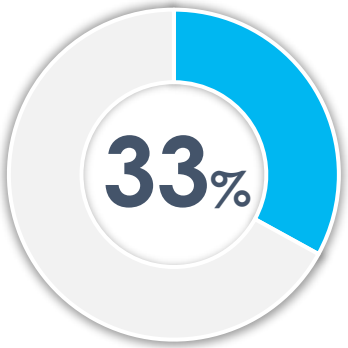
Healthy Fear of Data Breaches

One-third of employees feel their employer did not adequately train them to protect company data.



believe they will get
fired for a data breach

believe their execs
should be fired for a breach

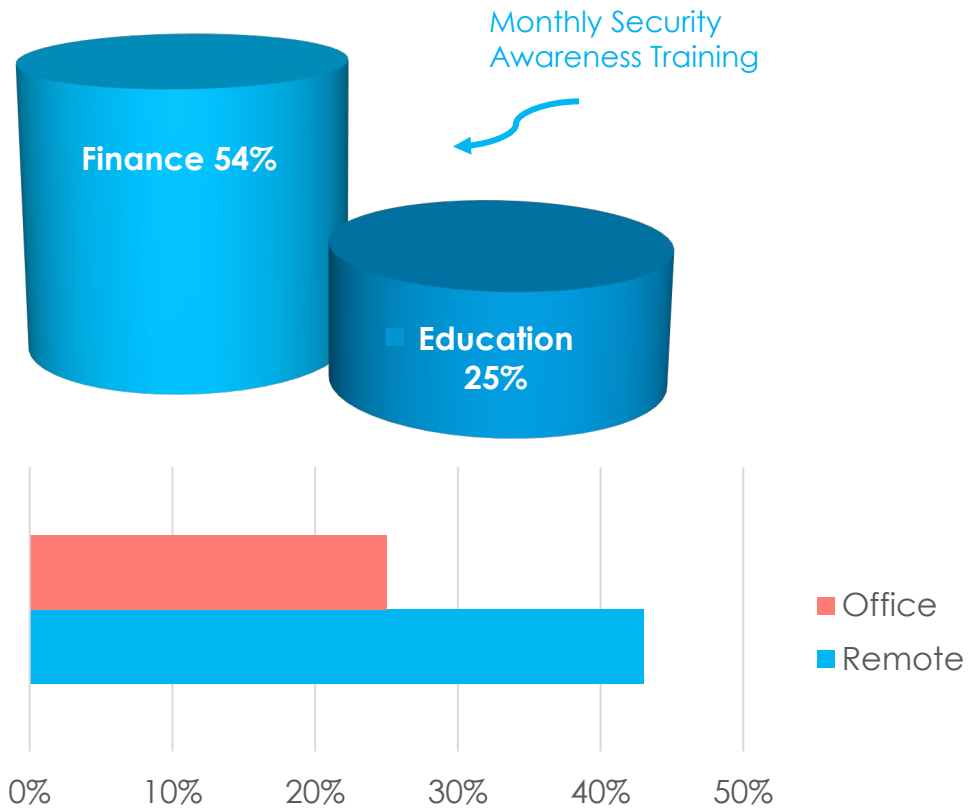


know someone
who caused a breach

Insight: *These figures are much higher in Finance than other regulated industries, indicating that Finance workers understand the gravity and cost of a security breach.*

Security Awareness Training is Irregular and Inconsistent

- **54%** of Financial employees receive monthly security awareness training vs. only **25%** of Education workers
- **43%** of remote workers receive security awareness training monthly vs only **25%** of office workers
- Male employees are **more likely** to receive monthly security awareness training than female employees.



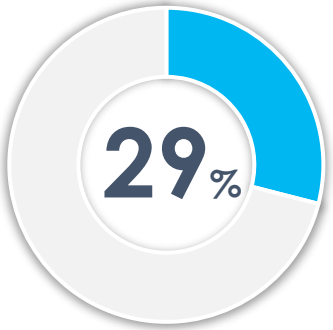
Insight: *It is unlikely that office workers, or male workers, are treated differently. We believe remote workers are engaging more with training content, whereas others are ignoring it.*

We have a password problem

We All Have Too Many Passwords

Government workers have the least, and Finance workers have the most passwords

Remote workers have a lot more work passwords than office workers



of Gen Z have more than **20** work passwords - which is much higher than other generations

Insight: *The more passwords we have, the more we are inclined to pick easy passwords and use predictable patterns. As a society, we need to* ***adopt password-less authentication.***

Passwords Are A Pain

18%

of people in the Finance industry
use the password reset feature daily

Male employees reset their passwords more often than female employees

Younger employees use the forget password or reset password feature at work much more than older workers

Insight: *Over 1/3 of Boomers have never used the forget password or reset password feature at work, suggesting they contact support directly.*

Passwords Are Poorly Managed

Across all industries, only **31%** of people manage their passwords with a password management tool.

29% write work passwords in a personal journal

24% store work passwords using notes on their phone

Insight: *Employers either need to commit to going fully password-less or provide their employees with a secure password management tool.*

Passwords Lead to Phishing Attacks

Across all industries, **32%** of Boomers type their password more than **10** times per day.

In the US, **18%** of Gen Z workers type **16+** passwords in a typical day.

27% of Gov workers have to type their passwords more than **11** times per day.

Insight: *80% of cyber attacks start with a compromised password. The best way to reduce the risk of getting phished is to adopt biometrics.*

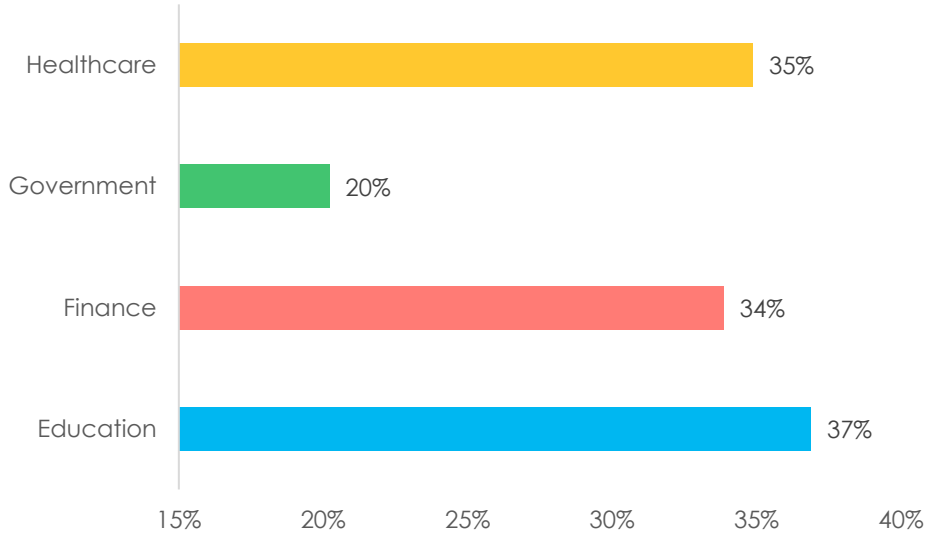
The BYOD risk is being ignored

Employers Are Ignoring The Risk of Personal Device Use

64% of people use a personal device for work but only **43%** have BYOD securely enabled.

- **69%** of workers use personal laptops and **87%** use personal smartphones for work in a typical week
- Only **33%** of workers are enabled to securely access systems, data, and apps from personal devices
- **39%** of remote workers can securely use personal devices but only **25%** of non-remote workers

Percentage of workers enabled to securely access systems, data, and apps from personal devices

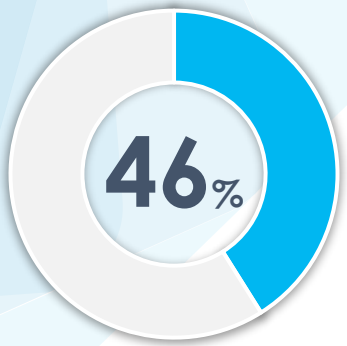


Insight: *Unsecure BYOD puts companies at significant risk when company data is exposed on an unmanaged app on an unmanaged device with no security controls.*

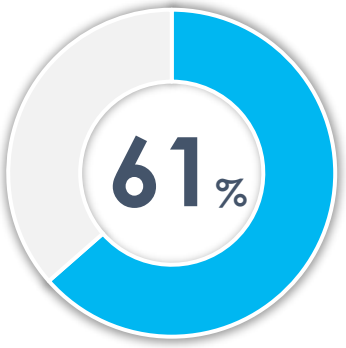
Shadow IT is out of control

Young Workers Lead The Way With Shadow IT

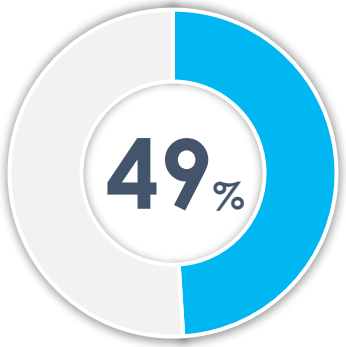
Young Workers = Gen Z + Young Millennials combined. Older Workers = Gen X + Boomers combined.



Young workers find security policies to be restrictive



Young workers are more efficient with apps like Gmail and Dropbox

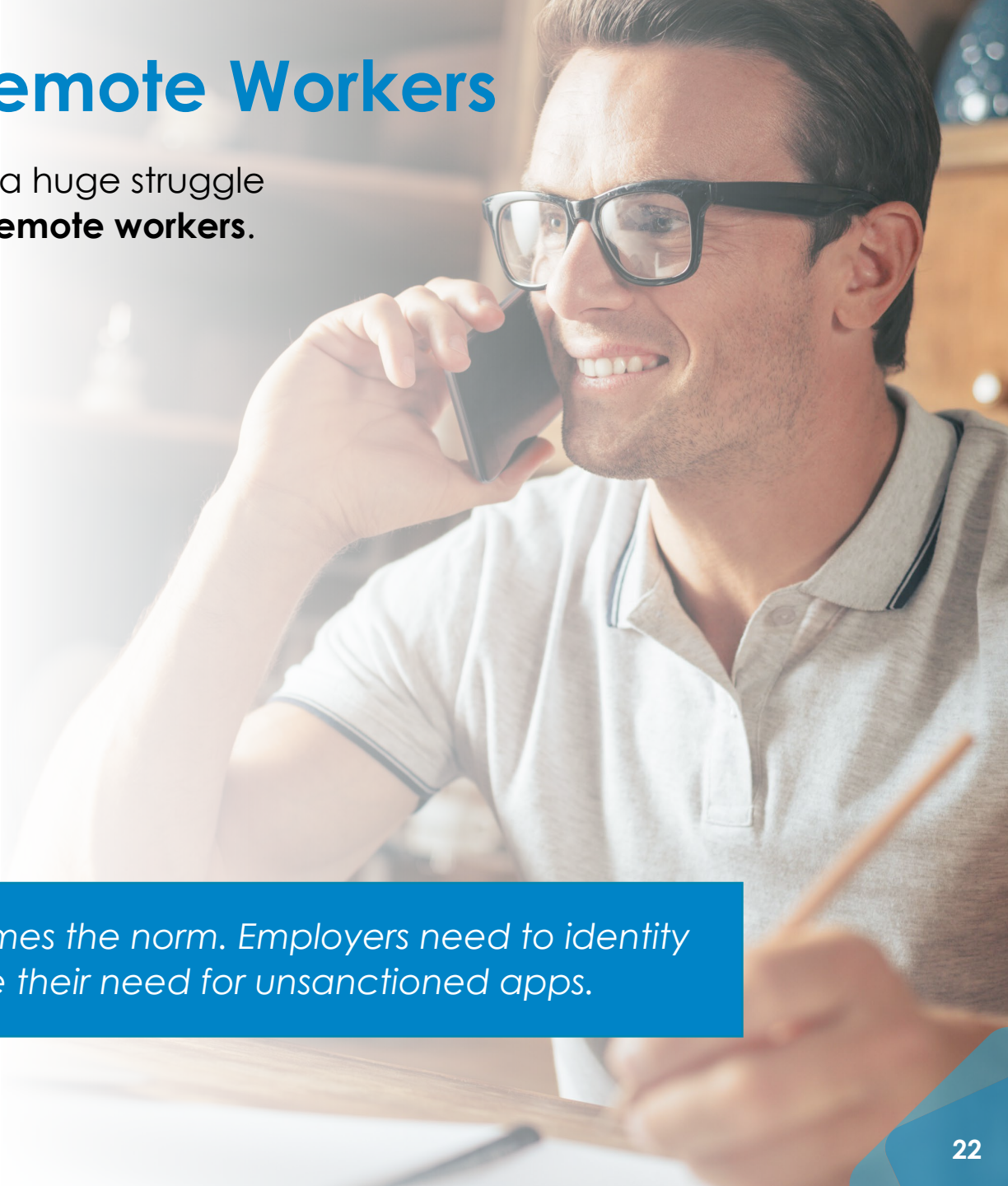


Young workers find ways to work around security policies

Insight: *Employers have not found the right balance between endpoint security and employee experience for their youngest workers. IT leaders can slow the growth of Shadow IT, by involving Gen Z and young millennials in product selection decisions.*

Shadow IT Is Accelerated By Remote Workers

Despite substantial efforts through the pandemic, there is still a huge struggle between security and employee experience, **especially for remote workers**.



- **46%** find security policies restrictive
- **42%** find ways to work around security policies
- **57%** are more efficient with Dropbox and Gmail.

Insight: *Shadow IT will get worse as remote work becomes the norm. Employers need to identity the right tools to empower remote workers and reduce their need for unsanctioned apps.*

Remote Workers Are More Secure

Remote Workers Are More Aware Of Security And Privacy

Remote workers care more about security, and less about privacy, than office workers.

Remote workers have much better password hygiene than office workers, with about **50%** higher adoption of security storage methods.

46% of remote workers see a privacy policy often vs. only **34%** of office workers.

Insight: *Remote employees are more aware of security and privacy policies, and more careful with their passwords. What can employers learn from their remote employees?*

Gen Z Sees What They Want To See

Gen Z does not appear to see (or notice) security policies when they log onto their computer compared to other generations, but they notice **privacy policies** more than any other generation.

24% of Gen Z saw a security policy the day they joined the company but didn't really read it.

Only **33%** of Gen Z see a security policy when they log in to their computer (vs 54% for Boomers)

45% of Gen Z and young millennials see (or notice) privacy policies often at work compared to 39% of older employees (Gen X and Boomers)

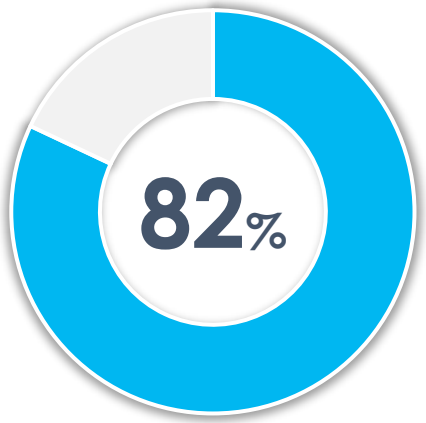
Insight: *Since Gen Z are hyper aware of privacy policies, employers need to shape communications to younger workers with emphasis on privacy.*

Employee Experience
Part Two

Employees and employers are not aligned

Employees and employers care about different things

- Healthcare employees feel the strongest of any industry about protecting their personal information
- Boomers feel the strongest of any generation about protecting their personal information
- Gen Z has an extreme bias for privacy over security



82% of Gen Z believe that their personal privacy is more important than company security

Insight: *It is clear that privacy matters **MUCH** more to employees than security. Employers can leverage this by positioning security and privacy as two sides of the same coin.*

Blurred Lines

The Line Between Work and Personal Life is Blurred

Younger workers (Gen Z & young millennials) don't see a clear line between their work and personal lives.

57% of younger employees use work devices for personal use

71% of younger employees use personal devices for work

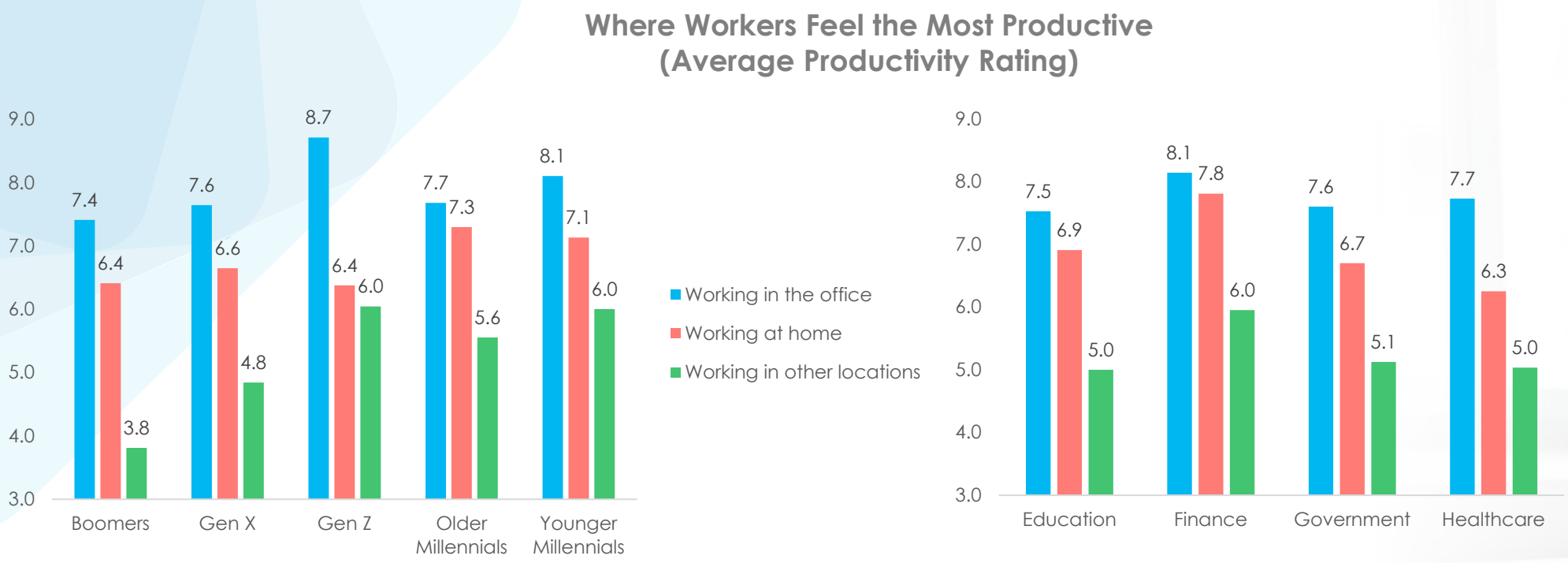
46% of younger employees allow family members to use their work devices

Insight: *These younger employees see the world differently and this present challenges for IT leaders. Best practice is to secure and manage COPE devices (company owned, personally enabled) and only apply application management policies to BYOD (bring your own device).*

Where do people feel most productive?

Employees Feel Most Productive in the Office

Workers in all industries, and all generations, feel more productive working in an office than at home.



Insight: *Companies should not close their office as many workers feel more productive there. This is especially true for companies with a young workforce.*

How Has Job Satisfaction Changed?

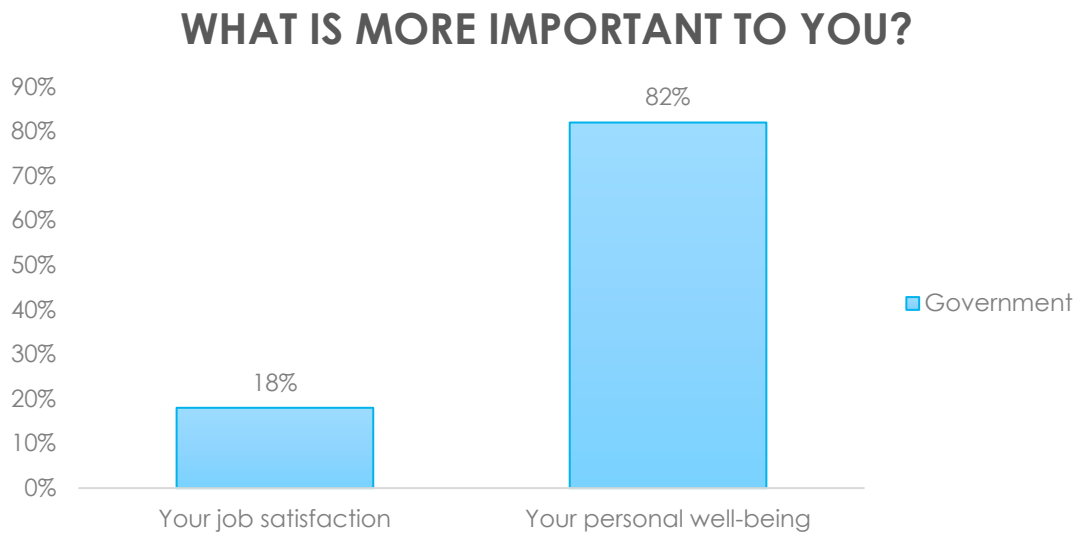
Job Satisfaction

58% are working **longer hours** now than 2 years ago. How has that impacted job satisfaction?

71% of remote workers have **better job satisfaction** now than 2 years ago vs **53%** for office workers

Financial workers care the most about job satisfaction and government workers the least.

80% of older employees care most about personal well-being than their job satisfaction

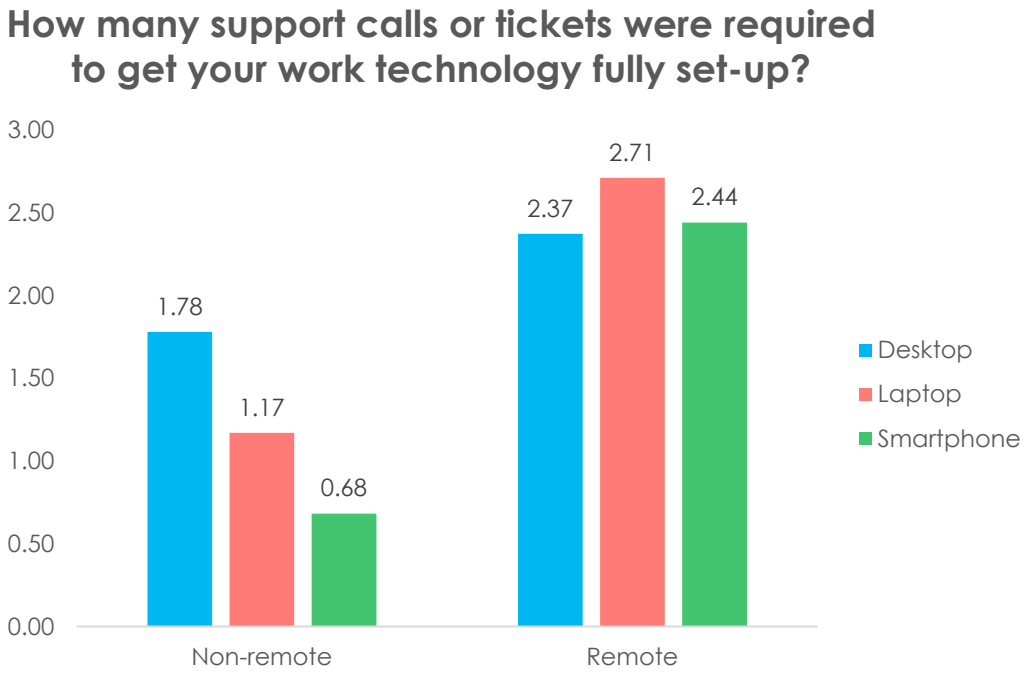


***Insight:** The pandemic impacted industries in different ways, and it appears the degree of personal risk faced by frontline healthcare, education and government workers dented their job satisfaction.*

Employee Onboarding is Inefficient

The Employee Onboarding Experience is Clunky

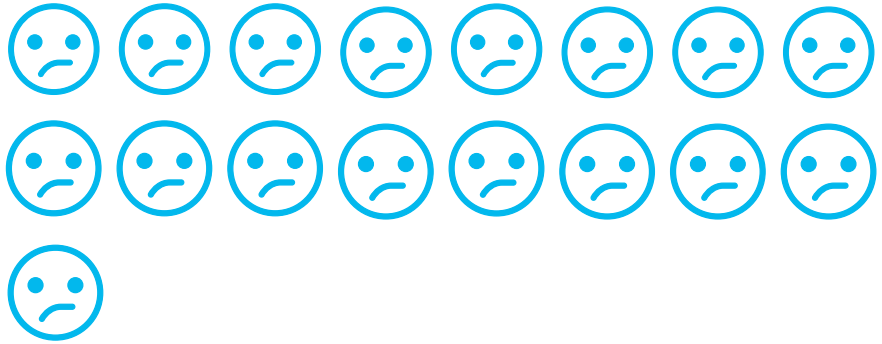
- Remote workers require almost double the time for office workers to set-up their devices
- Remote workers also require more technical support than office workers.
- Finance workers have the worst set-up experience and require the most support.



Insight: *The lack of walk-up IT support in an office is impacting remote workers. Employers need to be more intentional about designing an onboarding process for remote workers. Zero-touch provisioning and password-less authentication greatly simplify the set-up experience.*

Employee Support

24% of Finance workers are very satisfied with the IT support at work compared to just **17%** for Education workers.



Employee Support

72% of Finance workers get their issues resolved **in less than a few hours**

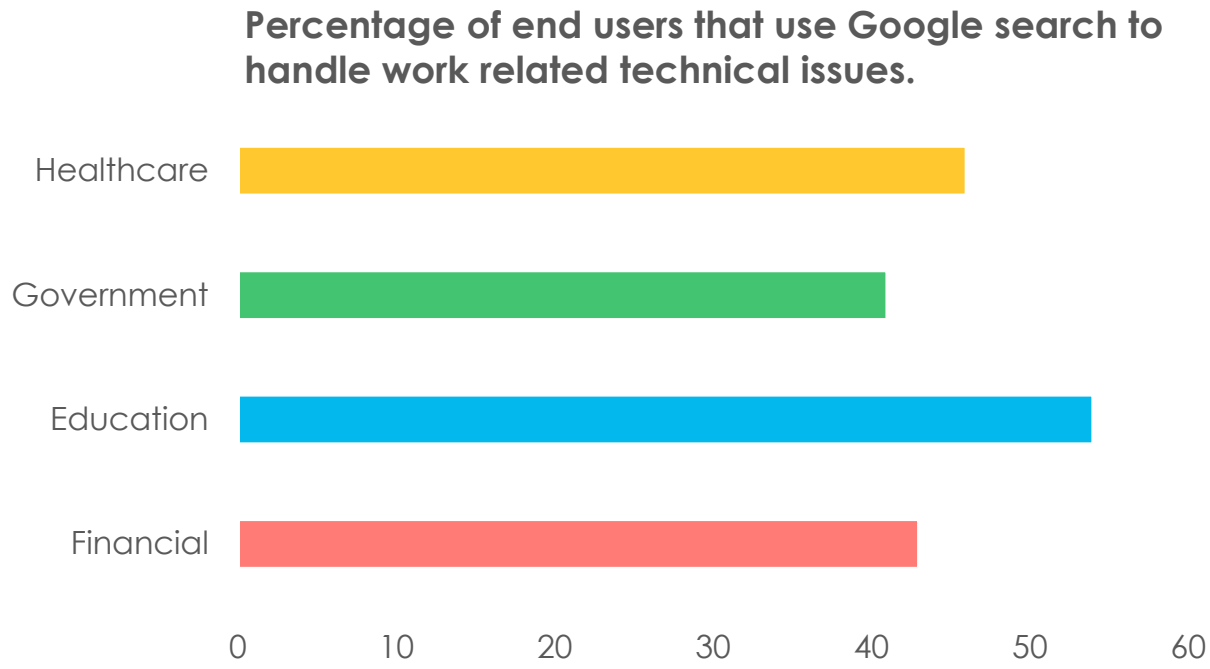
43% of Education workers wait for **a day or longer** to get their issues resolved

> In the US, **36%** of people get a helpful response from IT **within minutes**, in contrast to just **27%** in Australia.

Technical Support

Tech Support

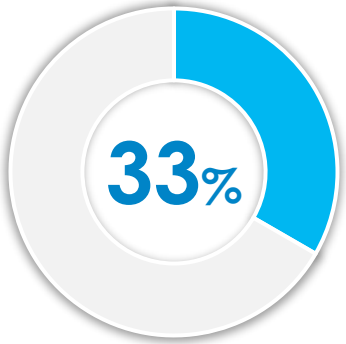
Perhaps because of the long wait times and low satisfaction, Education workers are the biggest users of Google to search for the answer to technical issues.



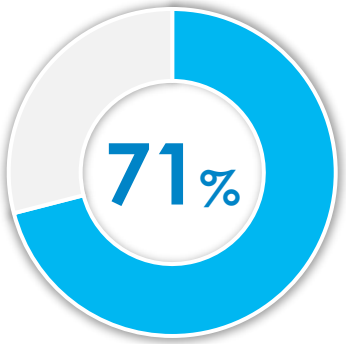
***Insight**: The Financial industry often outsources their IT support to managed service providers with defined SLAs for response and resolution times. Education, on the other hand, generally relies on internal IT staff who are spread thin, resulting in longer wait times.*

Employee Experience with Tech Support

50% of remote workers spend more time dealing with tech support issues now than 2 years ago



33% of remote workers are very satisfied happy with their IT support compared to office workers.



71% of remote workers are more satisfied with technical support now than 2 years ago

Insight: *In 2020, employers enabled their staff to work remotely and in 2021 employers started hiring and onboarding new people remotely. The challenge in 2022 is to build a sustainable and scalable remote support model.*

Research Methodology

NATIONAL STUDY METHODOLOGY

CUSTOM 25-QUESTION SURVEY COMPLETED BY

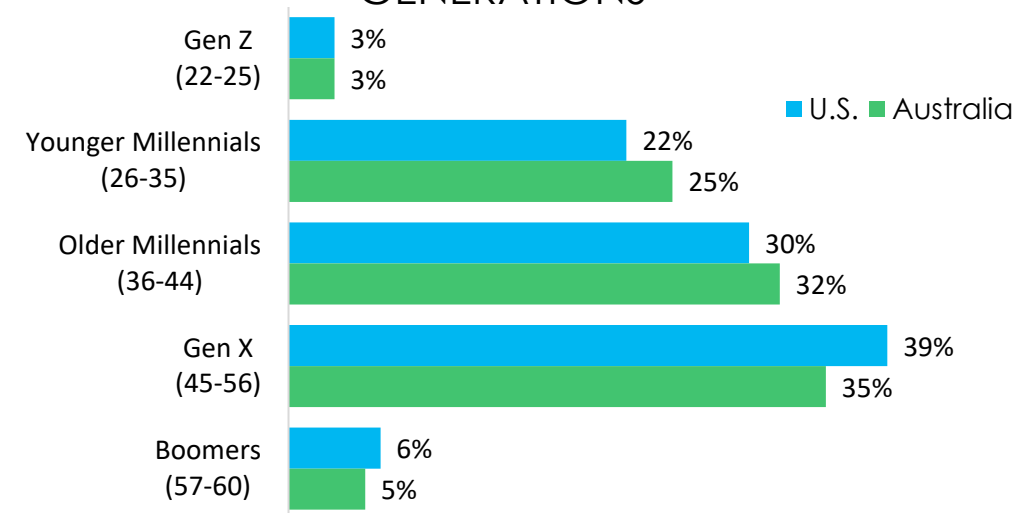
1,000
U.S. PARTICIPANTS
(AGES 22-60)

500
AUSTRALIAN PARTICIPANTS
(AGES 22-60)

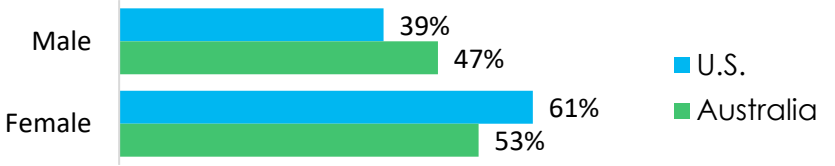
NATIONAL SAMPLE INCLUDES:

- Employed full-time, part-time, or self-employed
- Use a computer as part of their job
- Work in Healthcare, Education, Government, or Financial Services industries

GENERATIONS



GENDER

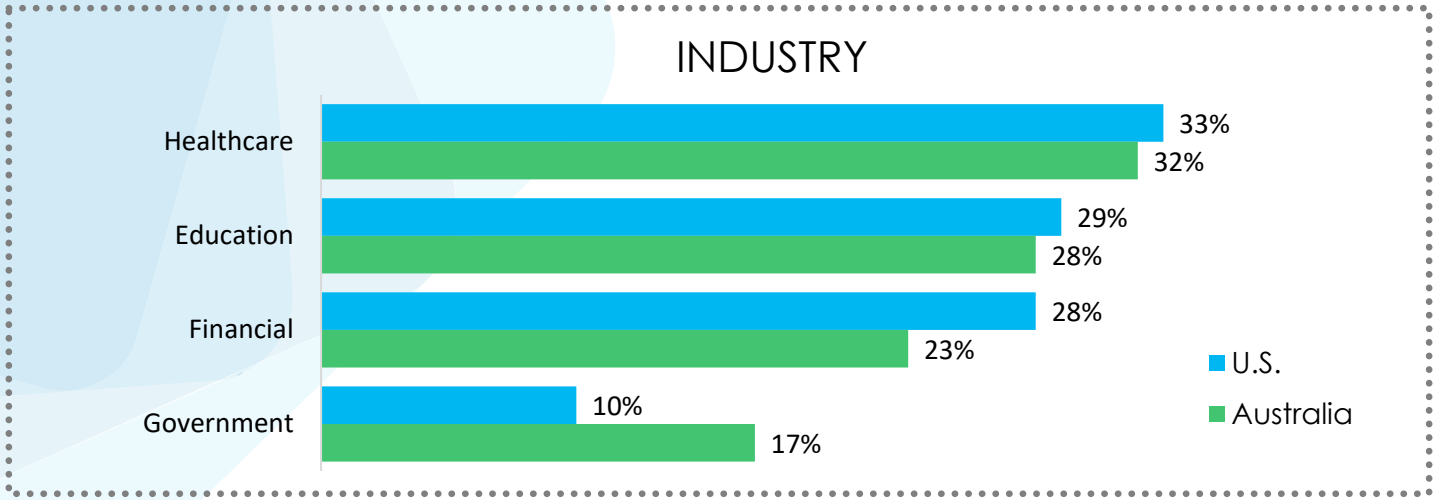


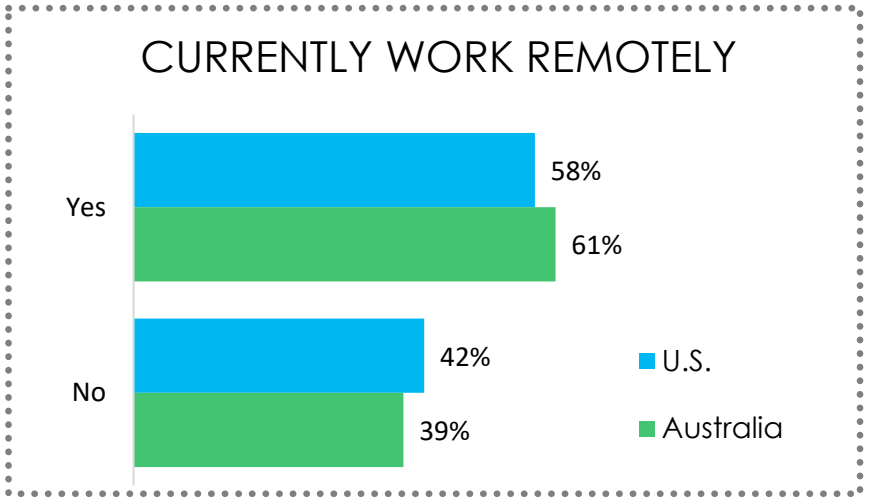
1% - U.S. Non-binary or prefer not to answer

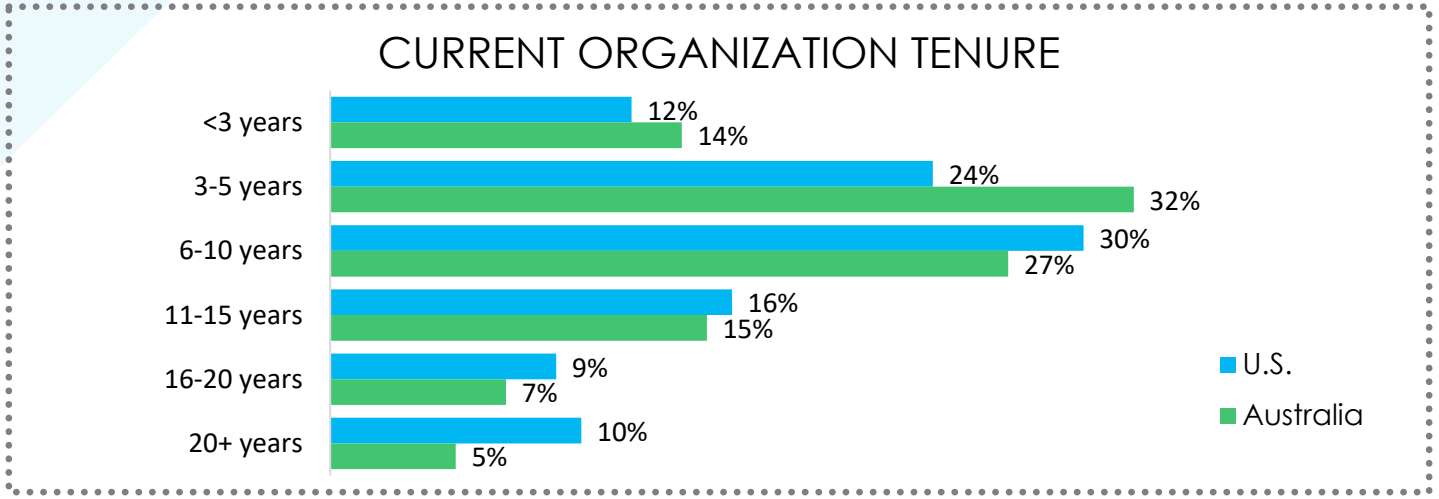
*U.S. Figures are statistically significant at the 95% confidence level. Margin of error is +/-3.1 percentage points.
*Australia Figures are statistically significant at the 95% confidence level. Margin of error is +/-4.38 percentage points.
*In an instance that a chart total for a single select question does not add to 100%, please note that this is due to the minimal effect of rounding.
*Survey was conducted online from November 11, 2021, to November 30, 2021.

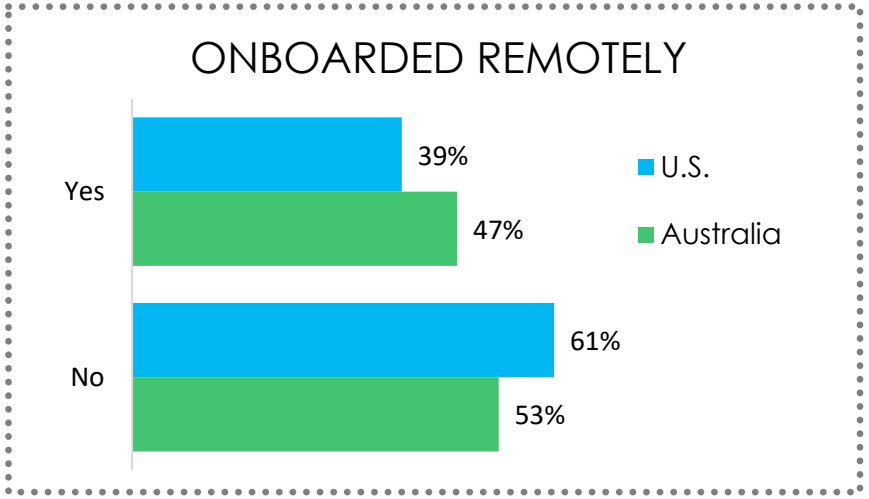
mobile mentor

NATIONAL SAMPLE OVERVIEW









mobile mentor

How to Share this Study

The content of this study is freely available to the general public. You are welcome to share any singular data point (or small groups of data points) in presentations, podcasts, radio shows, reports, articles, blog posts, etc.

Please always mention the source "a national research study conducted by Mobile Mentor…"

Please do not forward, send, or share this study in full. Anyone can access it freely at endpointecosystem.com.

If you have questions or comments about this research report, including permission to cite or reproduce the report, please contact the authors at research@mobile-mentor.com.