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

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.

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

We didn't ask IT leaders, we asked the **people on the front lines of** Healthcare, Education, Finance and Government.

Through the study we can highlight the **sentiments** of front-line educators and recommend insights and actions.

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 new employees remotely**
5. The **great resignation** in 2021 changed how employers treat their employees

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

Denis O'Shea
Founder
Mobile Mentor

Key Findings

Key Findings in Endpoint Security

1. **We have a security awareness problem**
   Security policies are largely invisible, security training is infrequent and the approach to shadow IT is immature. People underestimate the gravity of a security breach.

2. **We have a password hygiene problem**
   We save our work passwords in our personal journals and on our personal phones. We choose easy passwords, and don't use password management tools, or MFA.

3. **We have a shadow IT problem**
   We use personal devices with little security. We perceive security policies to be restrictive, find ways to work around them and we prefer to use unapproved cloud apps.

Endpoint Security
Part One

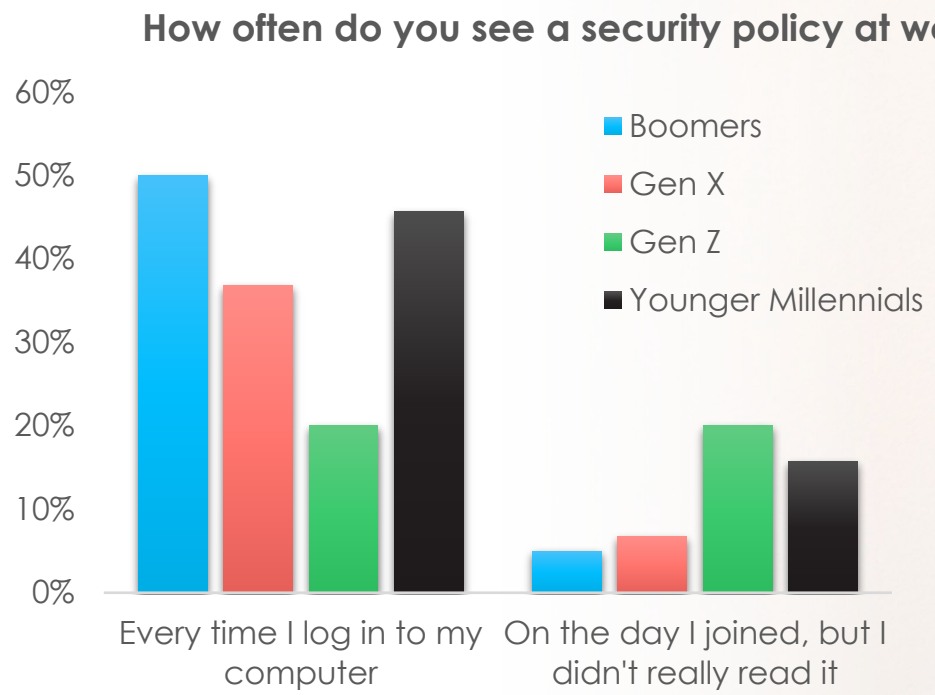
Security is not a big deal for us

Gen Z Doesn't See (Or Notice) Security Policies

Across all industries, only **20% of Gen Z** see a security policy when they log-in at work.

18% admit they saw a security policy the day they joined the company but didn't read it.

45% of Gen Z see (or notice) **privacy policies** 'often' (vs. 39% of older workers).



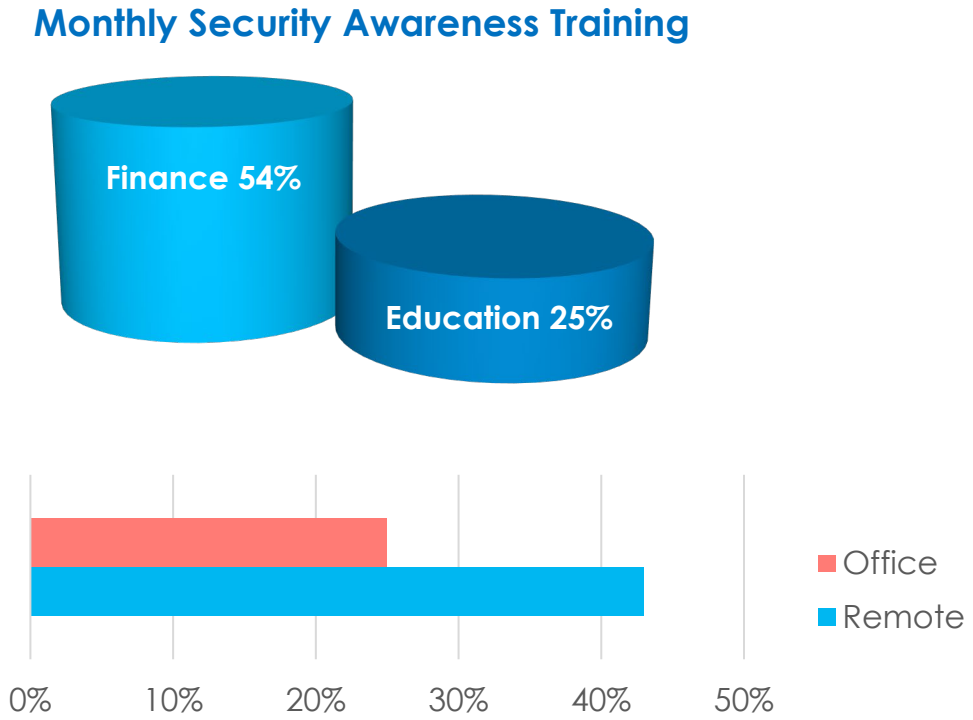
Insight: *Since Gen Z are **hyper aware of privacy policies**, employers should involve younger workers when drafting policies and writing company-wide communications on security.*

Is Security Awareness Training Effective?

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.

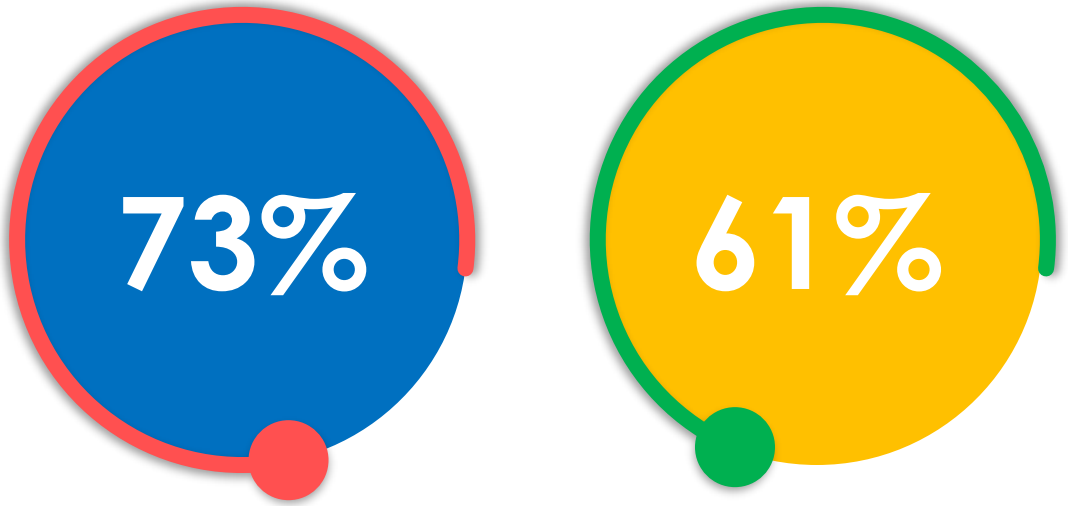


***Insight: The** quality of security awareness training was very poor in the past and this may have undermined its importance for people who were forced to watch the same videos annually.*

Visibility of Security Policies

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

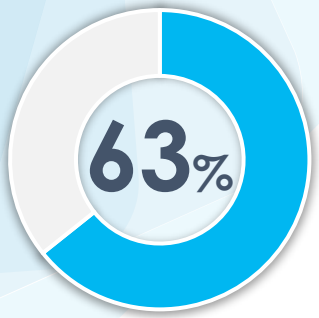
- In the US, **61%** of Financial employees see security policy every time they log on.
- In AU, **73%** of Government employees see security policy every time they log on.
- Education and Healthcare employees are least likely to see security policies.



Insight: *Employees don't actually read security policies. They just click to agree. People need to be actively engaged via practical tips or questions on security.*

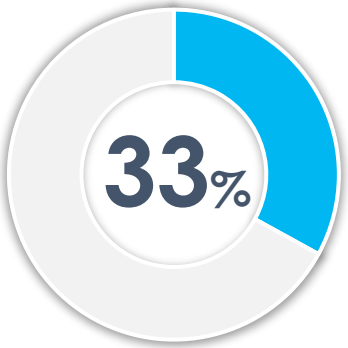
Fear of Data Breaches

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



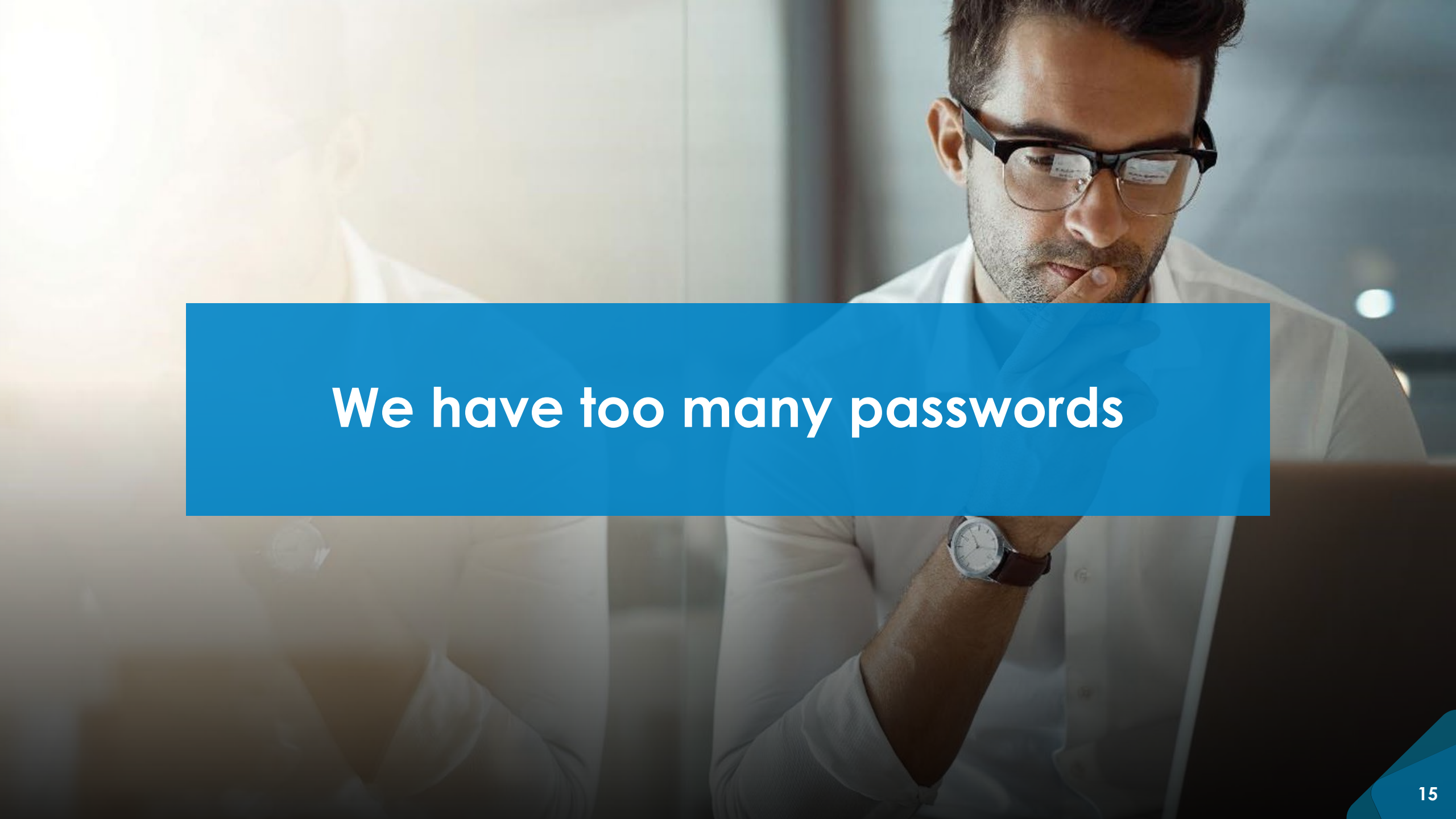
believe they will get fired for a data breach

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 only Finance workers truly understand the gravity and cost of a security breach.*



We have too many passwords

Knowledge Workers Are Fatigued With Passwords

69%

choose work passwords that are easy to remember

25%

Have NEVER reset their work password

Insight: *The vast majority of cyber attacks start with compromised credentials. Employers need to commit to going fully* ***password-less*** *or provide their employees with a password management tool.*

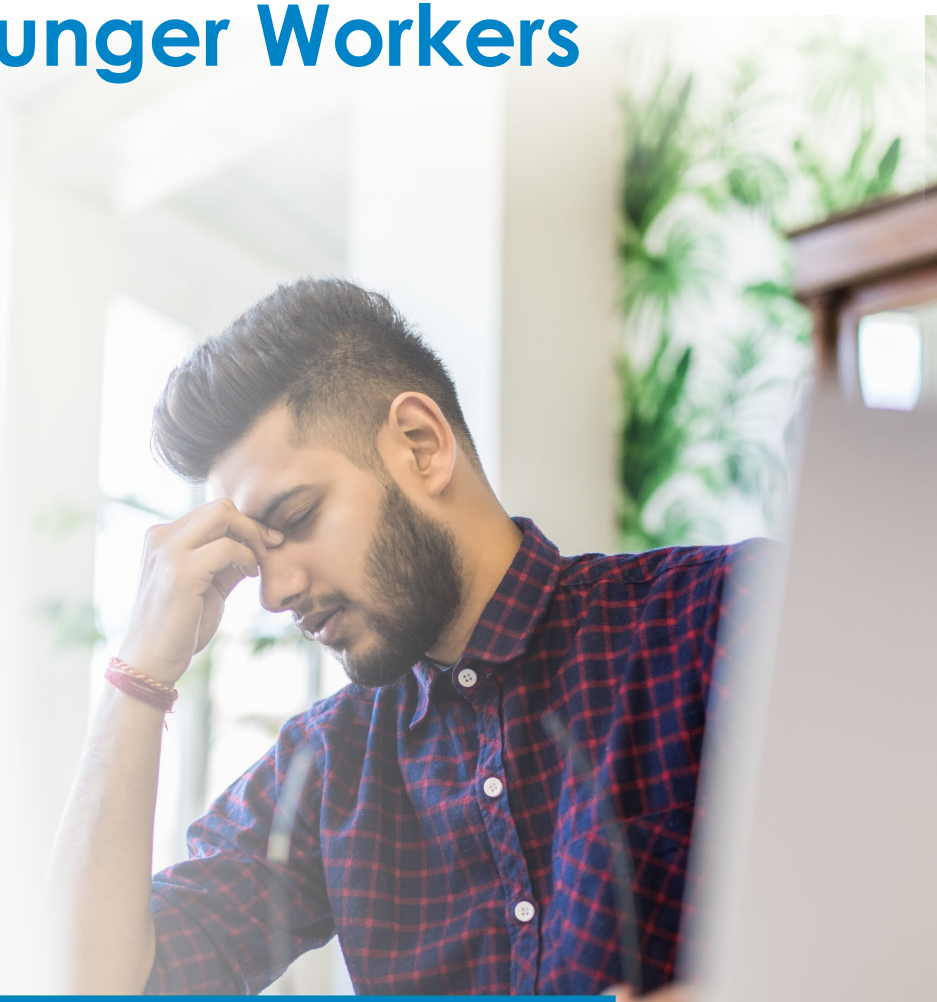
The Password Problem is Worse for Younger Workers

18%

of Gen Z have more than **40 unique passwords** for work accounts & applications

18%

of Gen Z workers type their **work passwords** more than 20 times / day



Insight: *The more passwords we have, the more likely we are to pick easy passwords and predictable patterns. Employers need to accelerate the journey to password-less authentication.*

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

27% store work passwords in Excel or Word on a PC

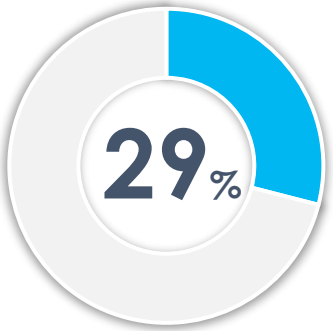
Insight: *Employers need to commit to going fully* ***password-less,*** *or else provide their employees with a secure password management tool.*

We All Have Too Many Passwords

Across all industries, **69%** of people choose passwords that are easy to remember.

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

Remote workers have a lot more work passwords than office workers



29% 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 Static in Education

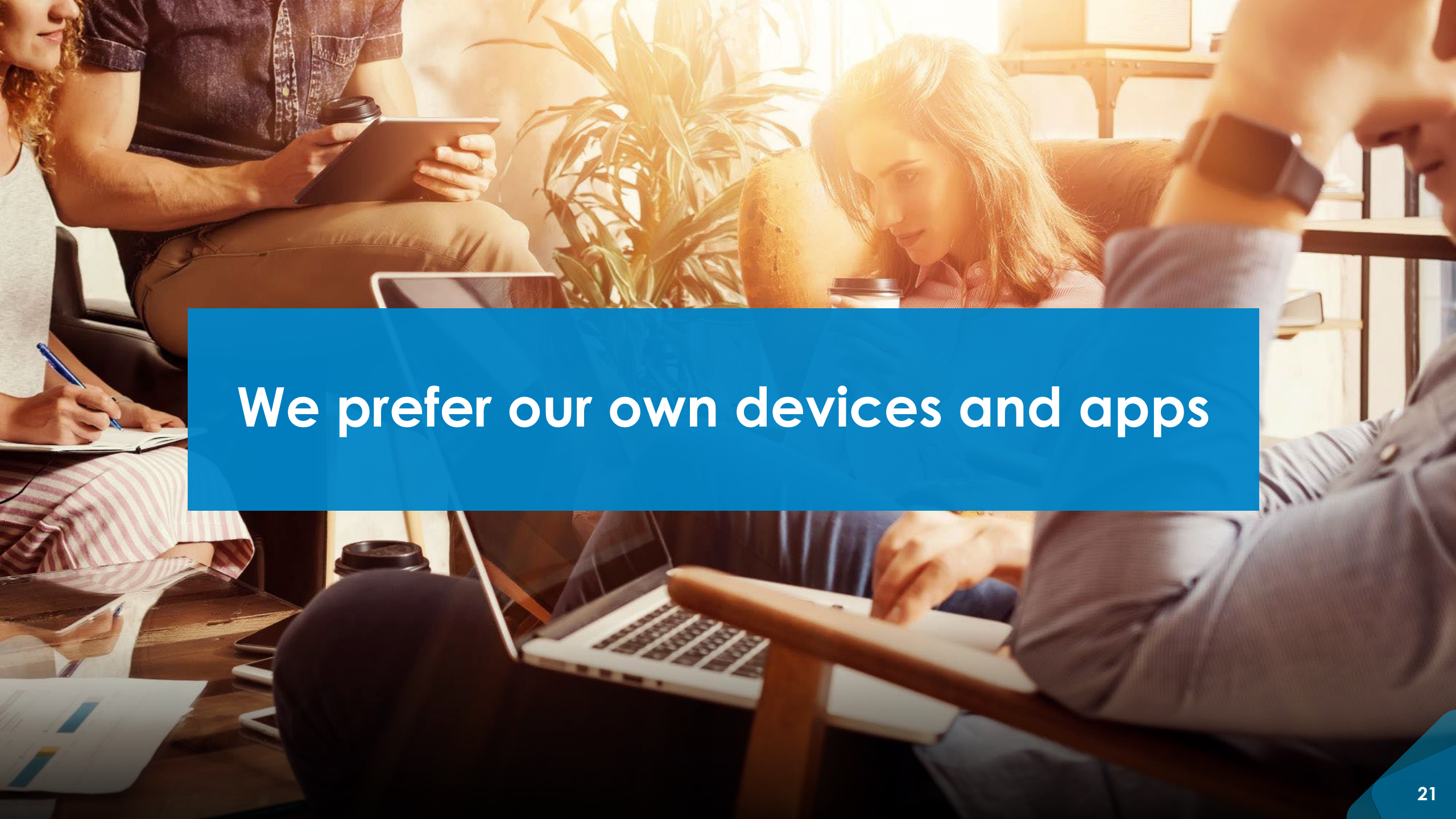
Male employees reset their passwords more often than female employees

18%

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

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

Insight: *39% of Baby Boomers have never used the reset password feature at work. Perhaps they call the service desk to change passwords, or maybe the just use the same password forever.*



We prefer our own devices and apps

Shadow IT Is Driven 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

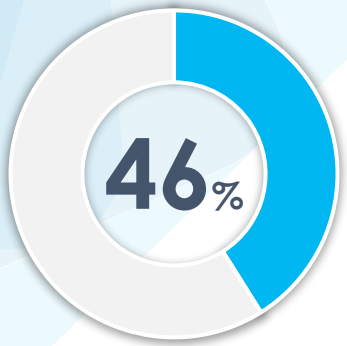
42% find ways to work around security policies

57% are more efficient with Dropbox and Gmail

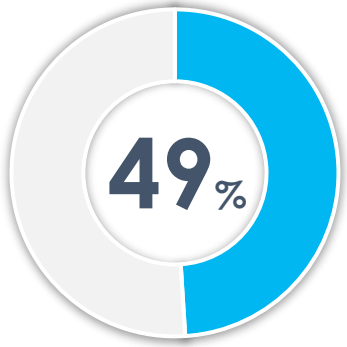
Insight: *Shadow IT will get worse as remote work becomes the norm. Employers need to identity the right tools to empower remote workers and reduce their need for unsanctioned apps.*

Young Workers Are Accelerating Shadow IT

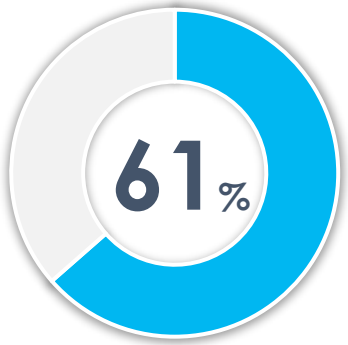
Young Workers = Gen Z + Young Millennials combined. Older Workers = Gen X + Boomers combined.



Young workers find security policies to be restrictive



Young workers find ways to work around security policies



Young workers are more efficient with apps like Gmail and Dropbox

Insight: *Employers have not found the right balance between security and employee experience. IT leaders can reduce Shadow IT by involving younger workers in product selection decisions.*

Shadow IT Is Driven 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

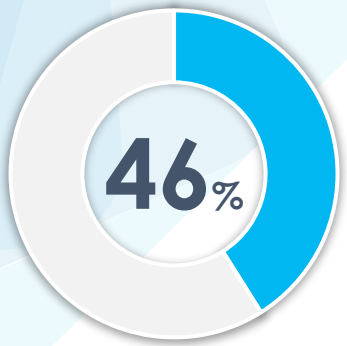
42% find ways to work around security policies

57% are more efficient with Dropbox and Gmail

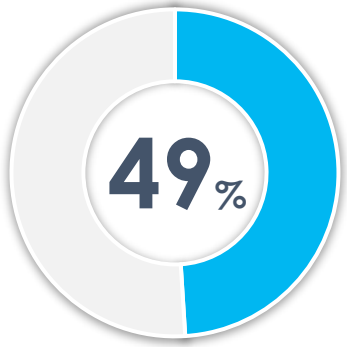
Insight: *Shadow IT will get worse as remote work becomes the norm. Employers need to identity the right tools to empower remote workers and reduce their need for unsanctioned apps.*

Young Workers Are Accelerating Shadow IT

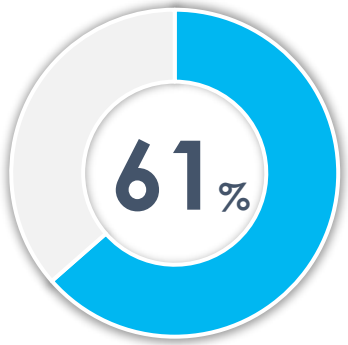
Young Workers = Gen Z + Young Millennials combined. Older Workers = Gen X + Boomers combined.



Young workers find security policies to be restrictive



Young workers find ways to work around security policies



Young workers are more efficient with apps like Gmail and Dropbox

Insight: *Employers have not found the right balance between security and employee experience. IT leaders can reduce Shadow IT by involving younger workers in product selection decisions.*

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 their work devices for personal use

71%

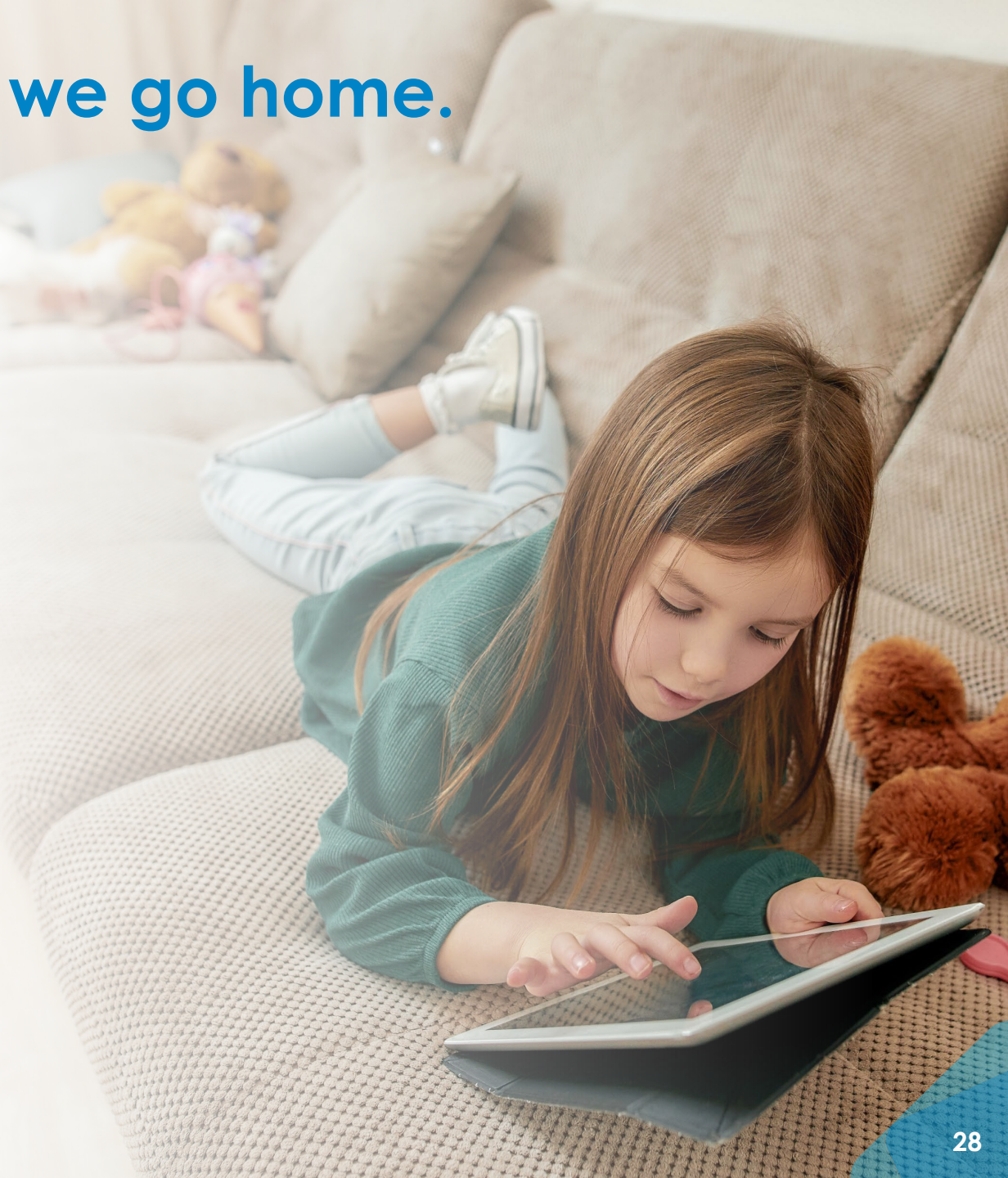
of younger employees use personal devices for their work

Insight: *Best practice is to use MDM (mobile device management) for company owned devices, but use MAM (mobile application management) for employees' personal devices (BYOD).*

Security at work is great - until we go home.

46%

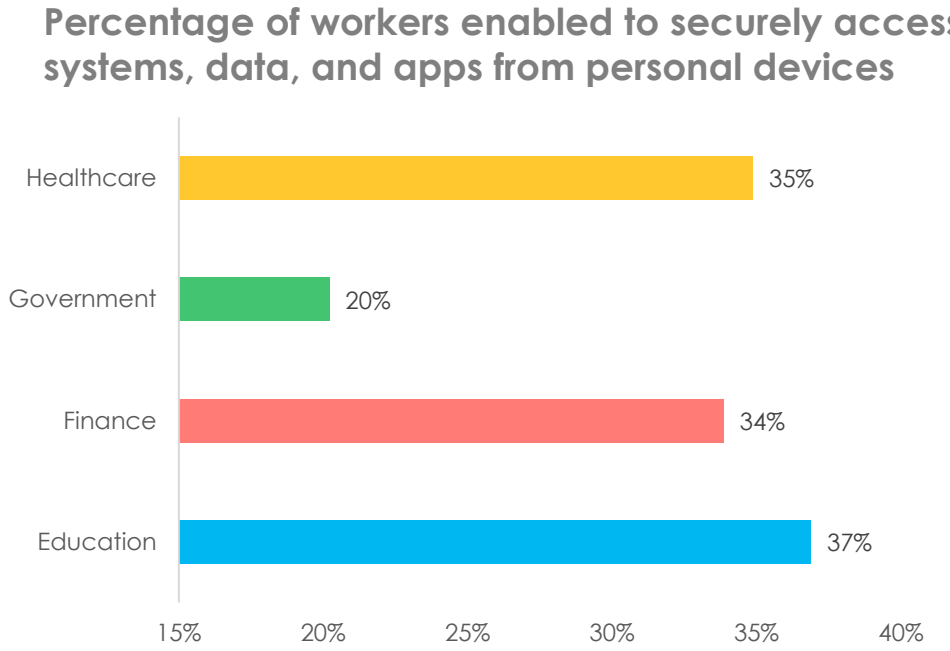
of young workers allow other **family members** to use their work devices for personal usage.



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 **37%** 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 can do the same



Insight: *Unsecured BYOD puts companies at risk when company data is exposed on an unmanaged app, on an unmanaged device. That data is effectively in the wild with no security controls.*

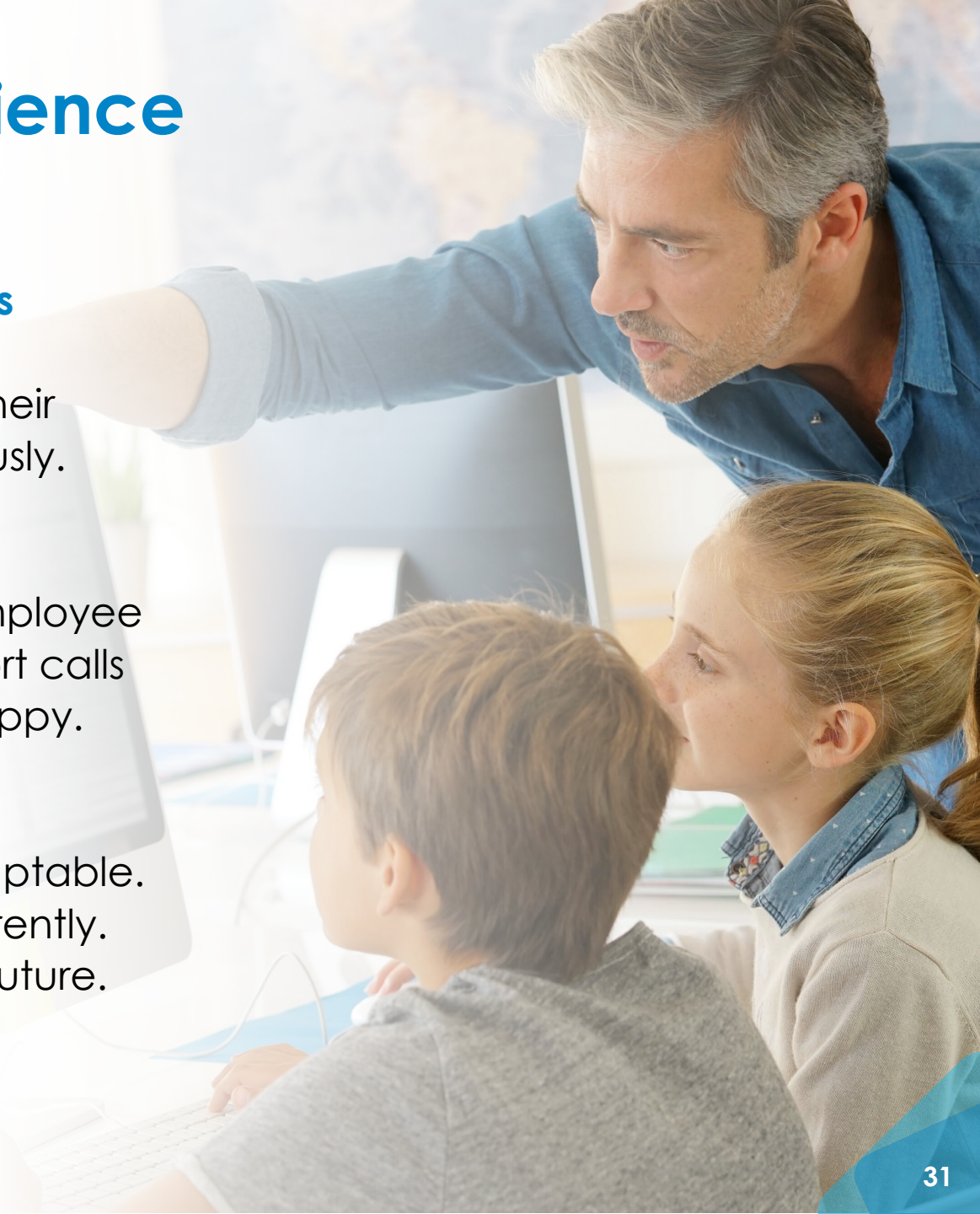
Employee Experience
Part Two

Key Findings in Employee Experience

1. **Employers and employees have different priorities**
   Employees care about their personal privacy, job satisfaction and personal well-being. They think their employer needs to take data privacy more seriously.

2. **Employee onboarding is clunky and painful**
   It takes 3 days to set up a laptop for a remote employee and requires 3 to 4 technical support calls. Support calls often take days to resolve. Employees are not happy.

3. **We can predict the future through Gen Z**
   Knowledge workers are very resourceful and adaptable. **Gen Z** thinks differently. **Remote workers** act differently. We can learn from both groups and predict the future.

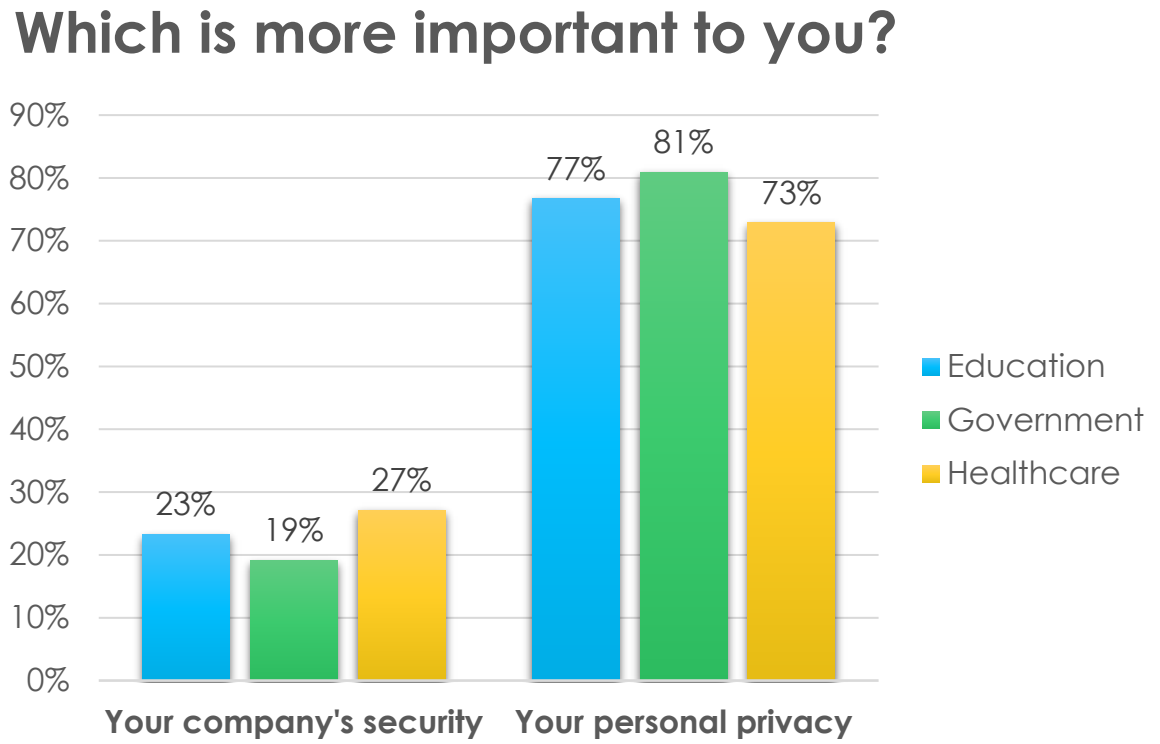


We have different priorities

Attitudes Toward Personal Privacy and Company Security

People in all industries care more about personal privacy than company security, but…

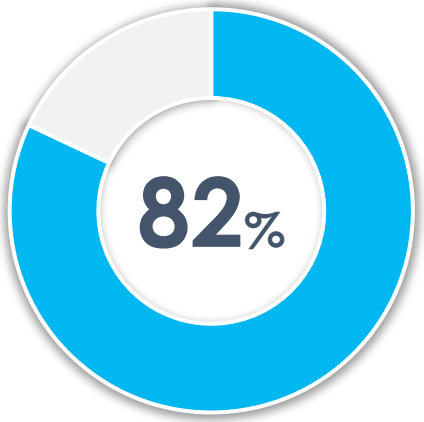
Healthcare workers care more about company security, and less about their personal privacy, than people in Education and Government.



Insight: *IT leaders can leverage this insight by positioning security and privacy as two sides of the same coin. People tend tune out for security measures, but they tune in for privacy measures.*

Employees and employers care about different things

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



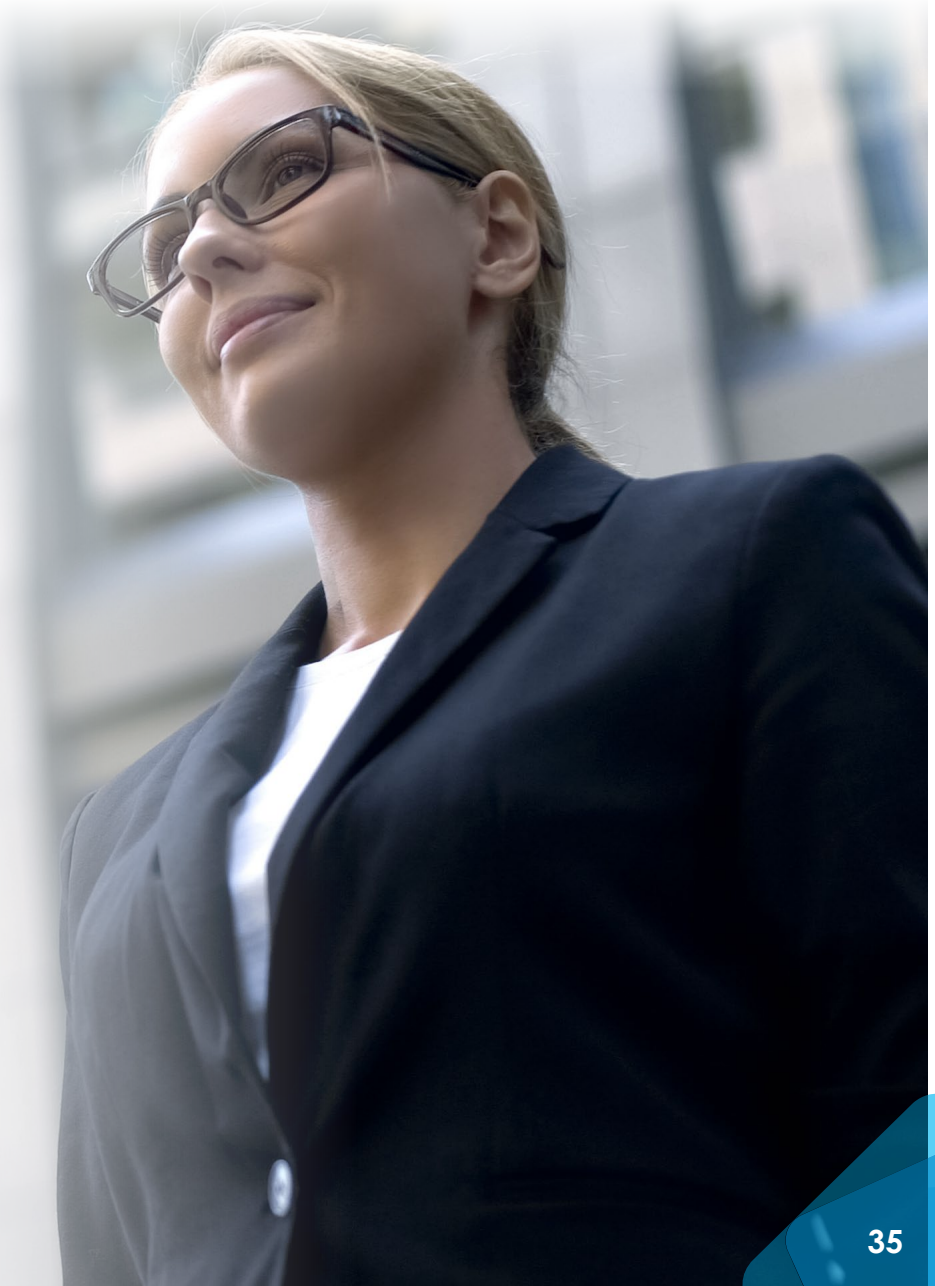
82% of Gen Z believe that their personal privacy is more important than company security

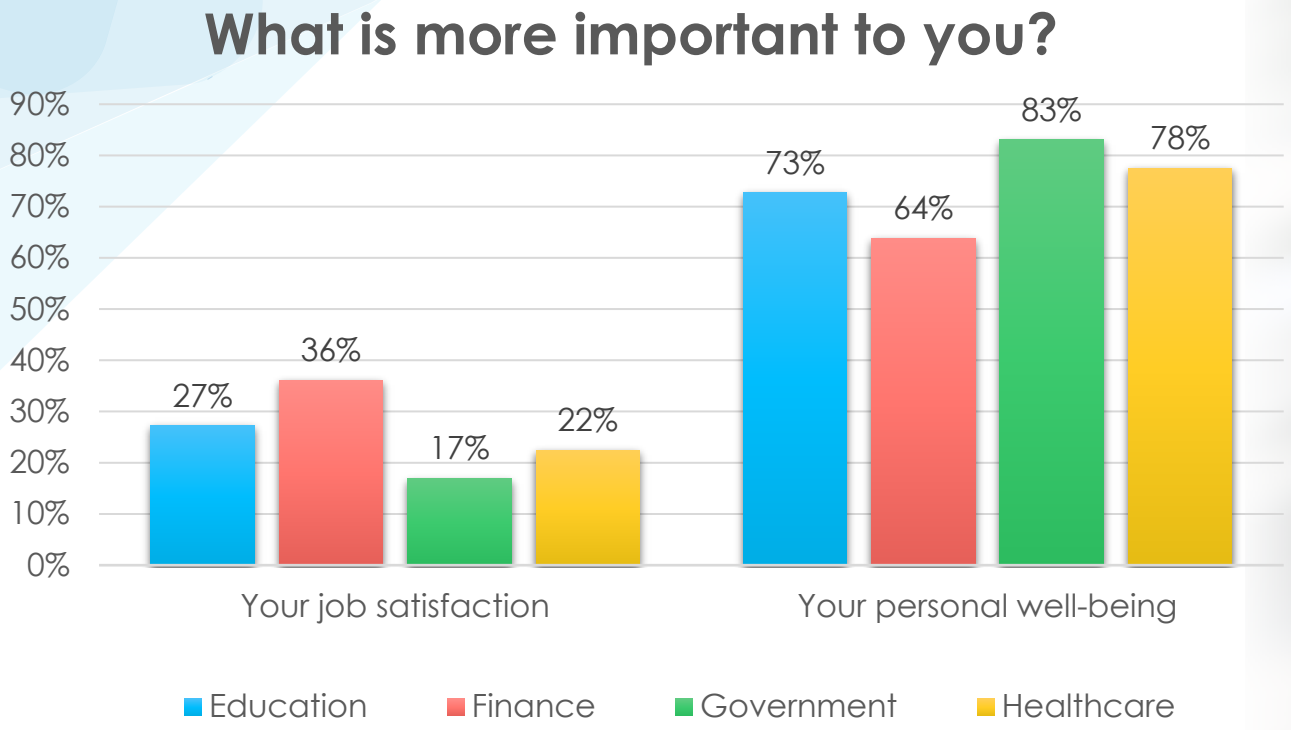
Insight: *It is clear that privacy matters* ***much*** *more to employees than security. Employers can leverage this by positioning* ***security and privacy as two sides of the same coin.***

Personal Well-being Beats Job Satisfaction

58% are working **longer hours** now than 2 years ago, and 64% say they their job satisfaction is higher!

Personal well-being is more important to Government workers relative to others

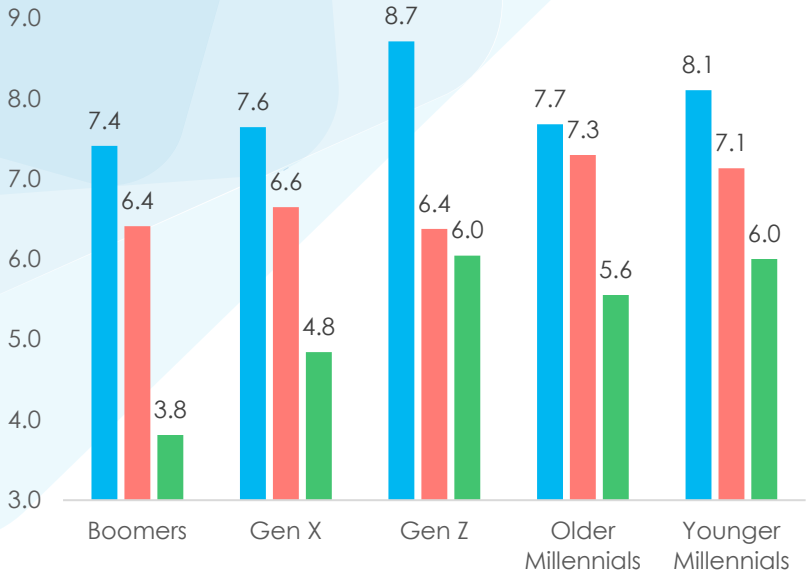


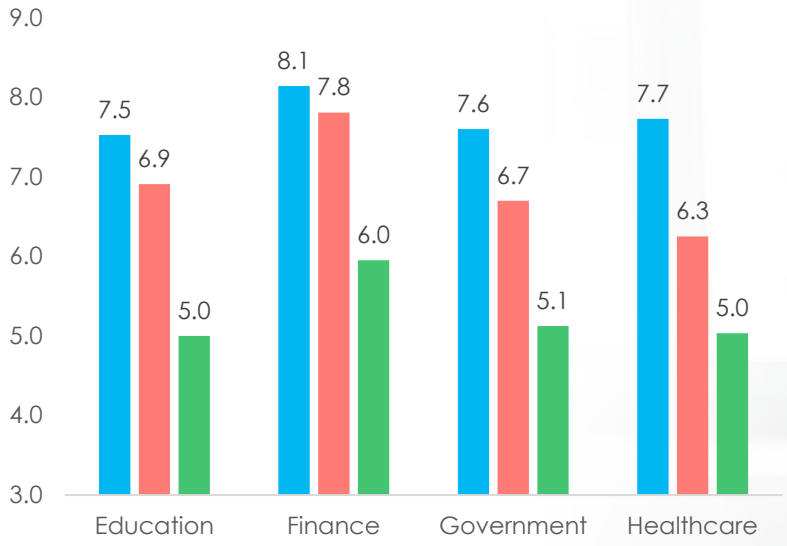


Employees Feel Most Productive in the Office

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

Where Workers Feel the Most Productive
(Average Productivity Rating)





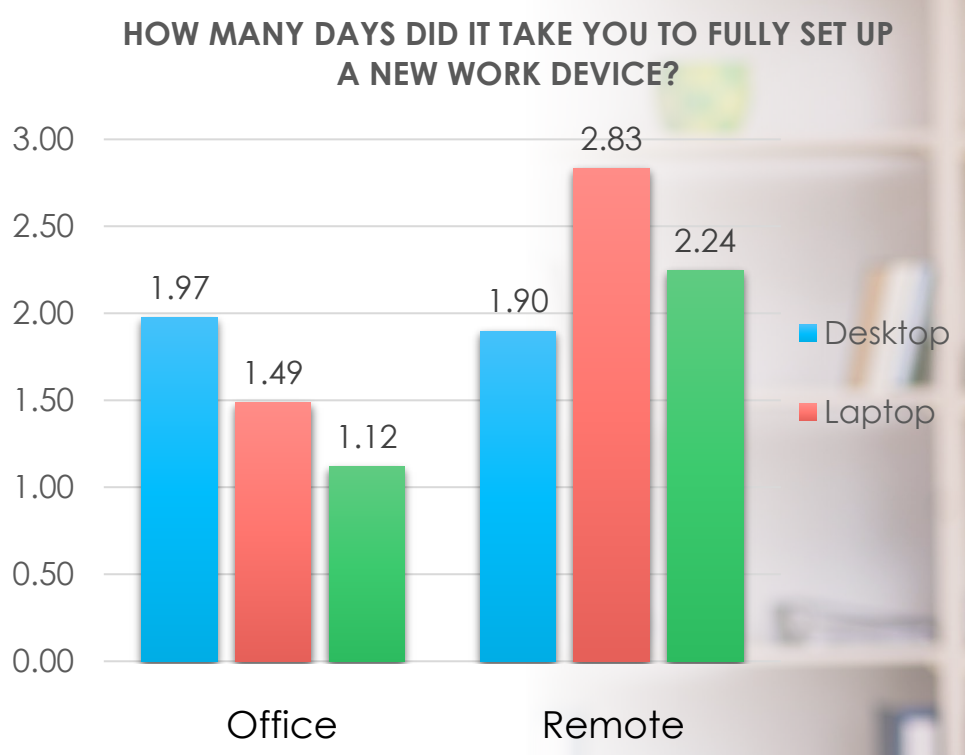
Insight: *The office environment provides context, broad relationships and a sense of belonging. This is especially true for young workers who joined the workforce remotely during the pandemic.*

We are frustrated with IT support

Employee Onboarding Is Clunky

Almost 3 days to set-up a laptop for a new remote employee

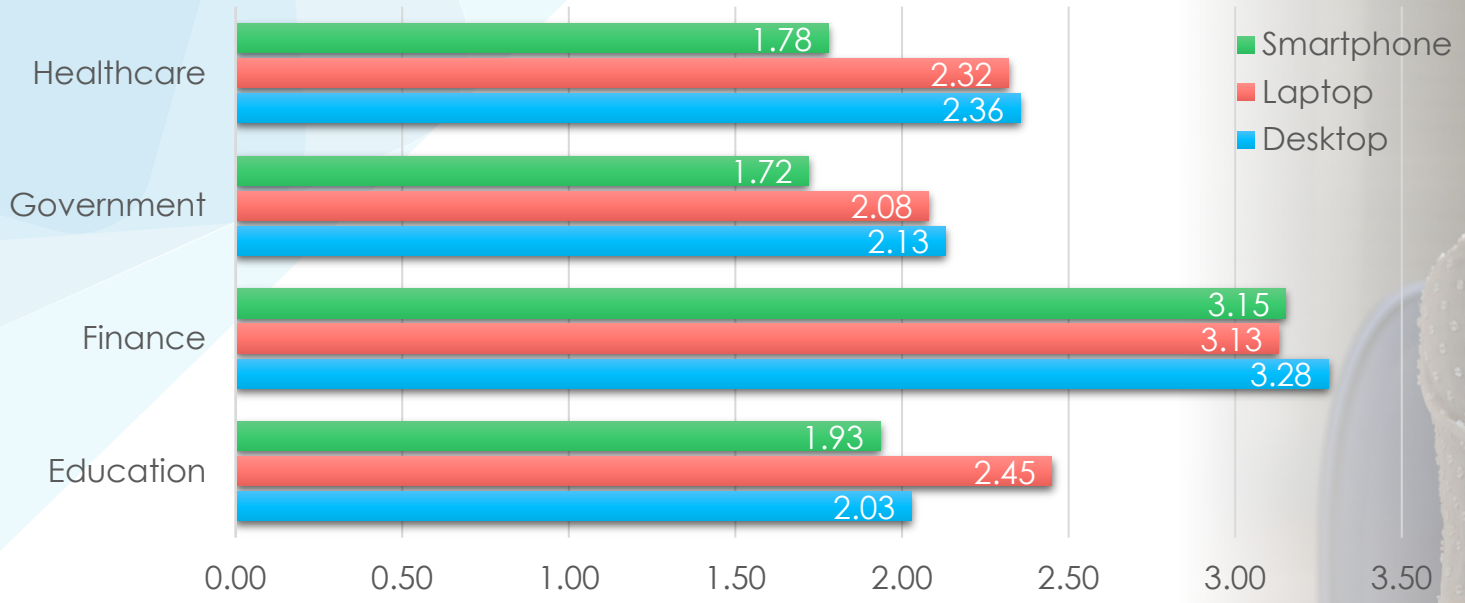
3 support calls / tickets to set-up devices for a new employee

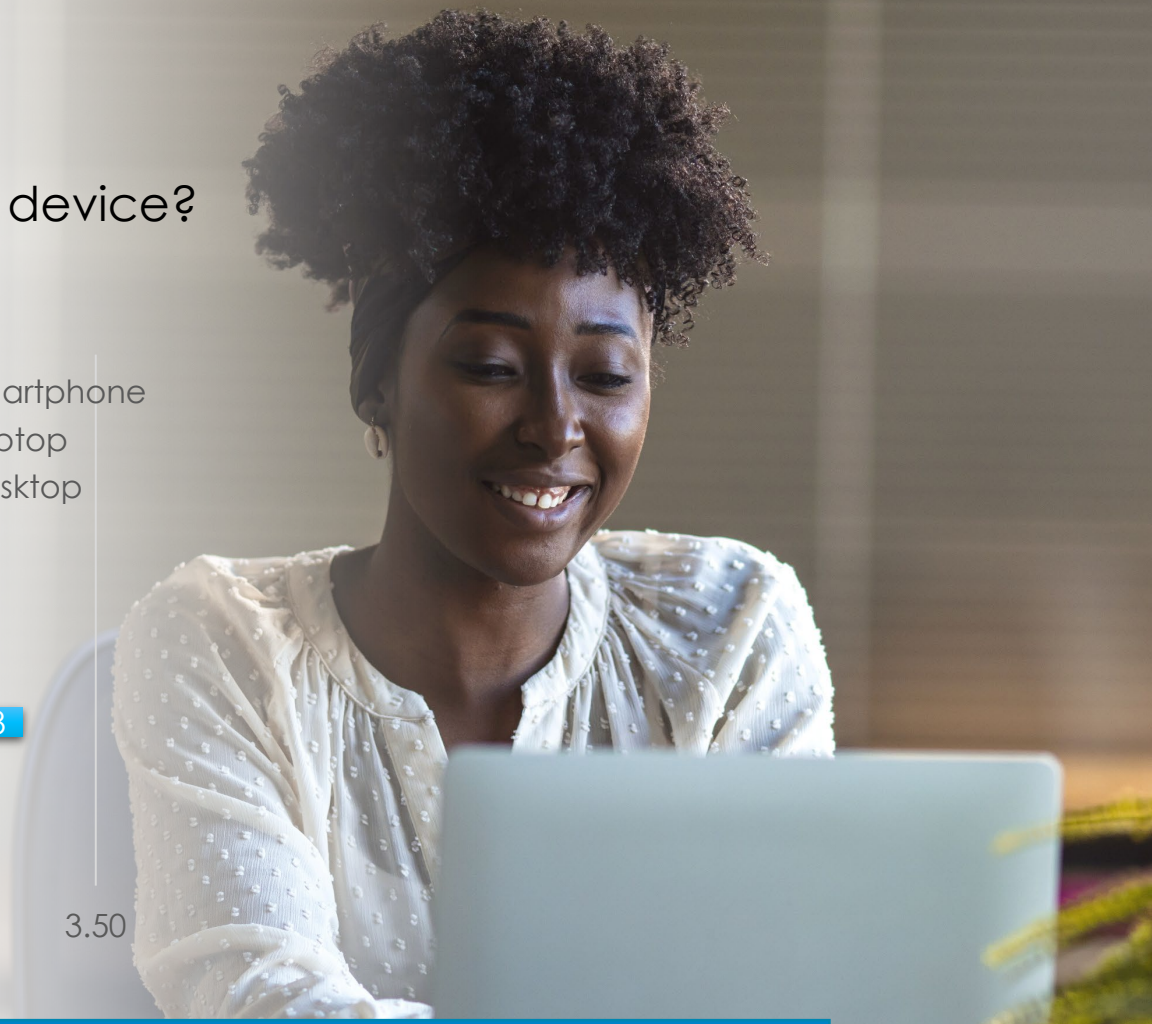


Insight: *Employers need to be more intentional about designing an onboarding process for remote workers. Zero-touch provisioning and password-less authentication simplify the set-up experience.*

Onboarding Varies By Industry

How many days did it take you to fully set up a new work device?





Insight: *Employers need to be intentional about designing an onboarding process for remote workers. Zero-touch provisioning and password-less authentication simplify the onboarding experience.*

Most People Are Not Impressed with Their IT Support

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

Support Wait Times Vary Across Industries

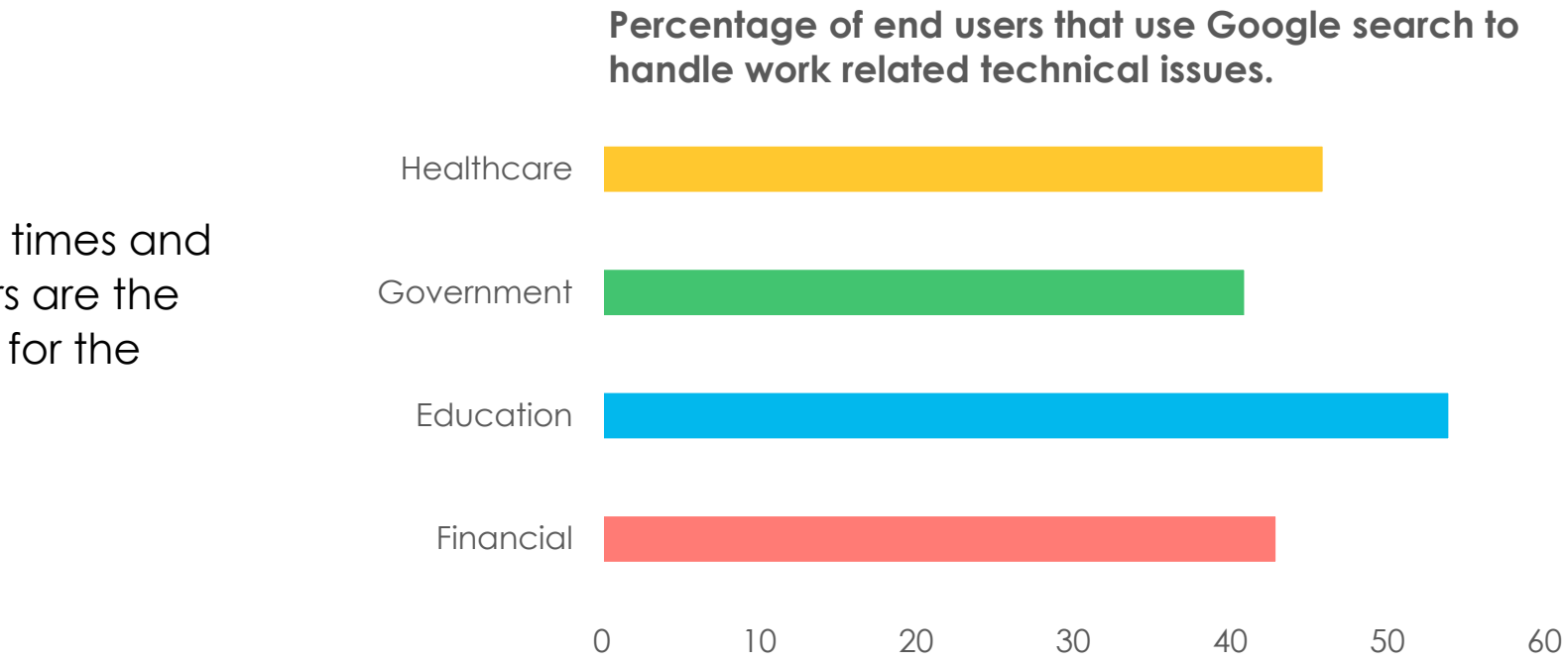
72% of Finance workers get their issues resolved **in less than a few hours**

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.

Tech Support

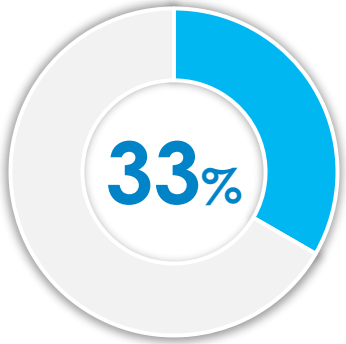
Perhaps because of the long wait times and low satisfaction, Education workers are the biggest users of Google to search for the answer to technical issues.



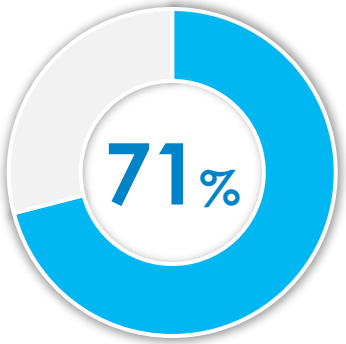
***Insight**: The Financial industry often outsources their IT support to managed service providers with defined SLAs for response and resolution times. Education, on the other hand, generally relies on internal IT staff who are spread thin, resulting in longer wait times …and more Google searches.*

Employee Experience with Tech Support

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

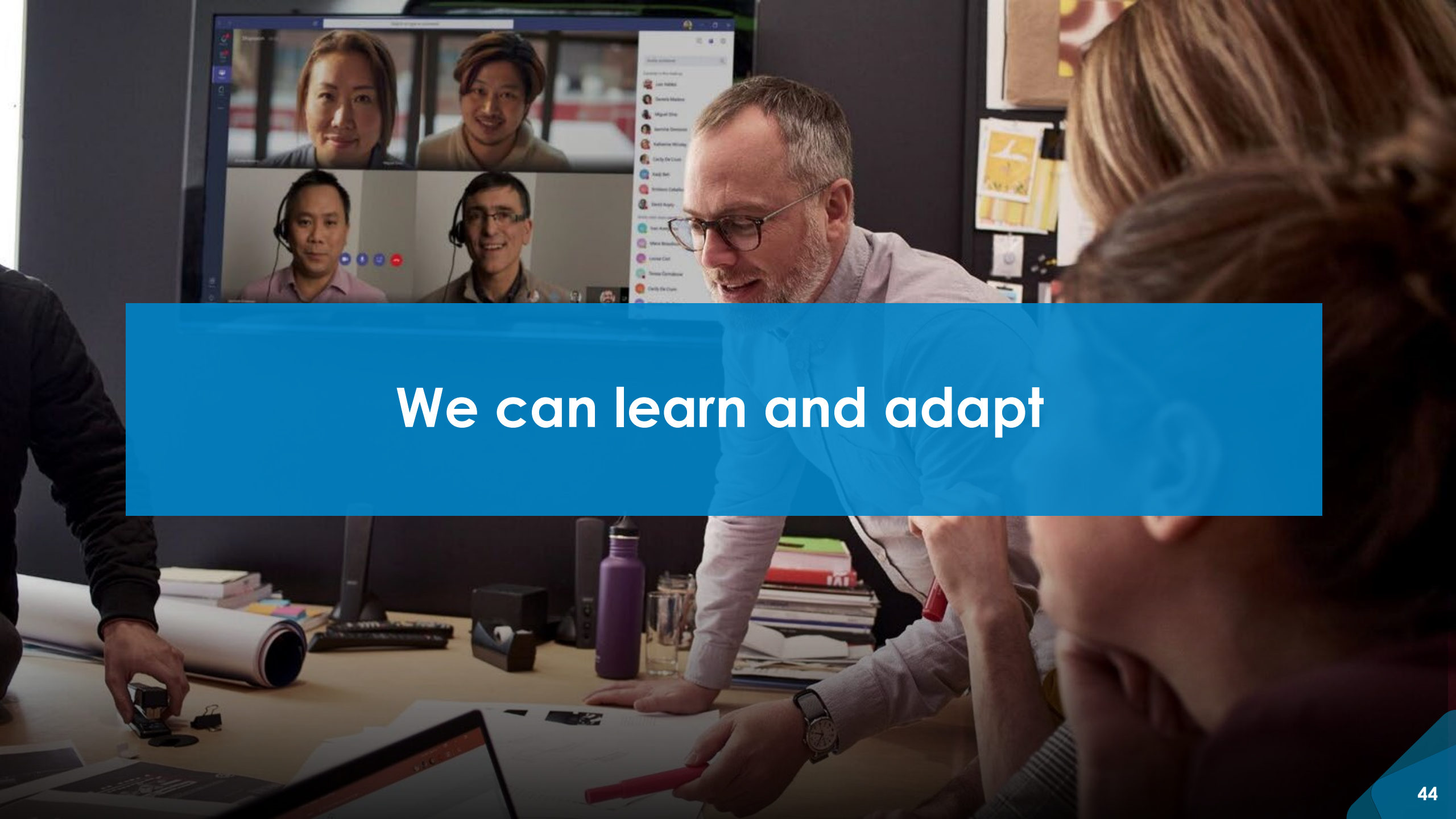


33% of remote workers are very satisfied happy with their IT support compared to office workers.



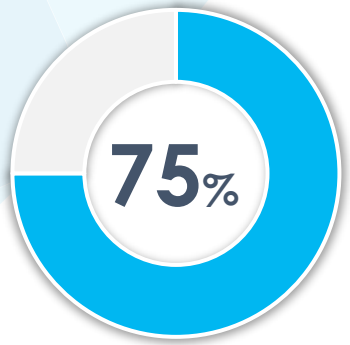
71% of remote workers are more satisfied with technical support now than 2 years ago

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



We can learn and adapt

Leaders Are Listening to their Employees



75% of employees believe their leadership is "**very open**" or "**somewhat open**" to listening to new ideas about the use of technology to improve the way they work

mobile mentor

What Can We Learn from Remote Workers?

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 secure 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. Employers should involve remote workers in product decisions.*

Gen Z Presents the Greatest Flight Risk

Gen Z entered the workforce during the pandemic, often onboarded remotely.

71%

believe **other companies** are doing a better job with modern tools and technology.

Insight: *Many Gen Z employees have not experienced a traditional office-based work culture. They only know remote work and assess their employer through the lens of a remote worker.*

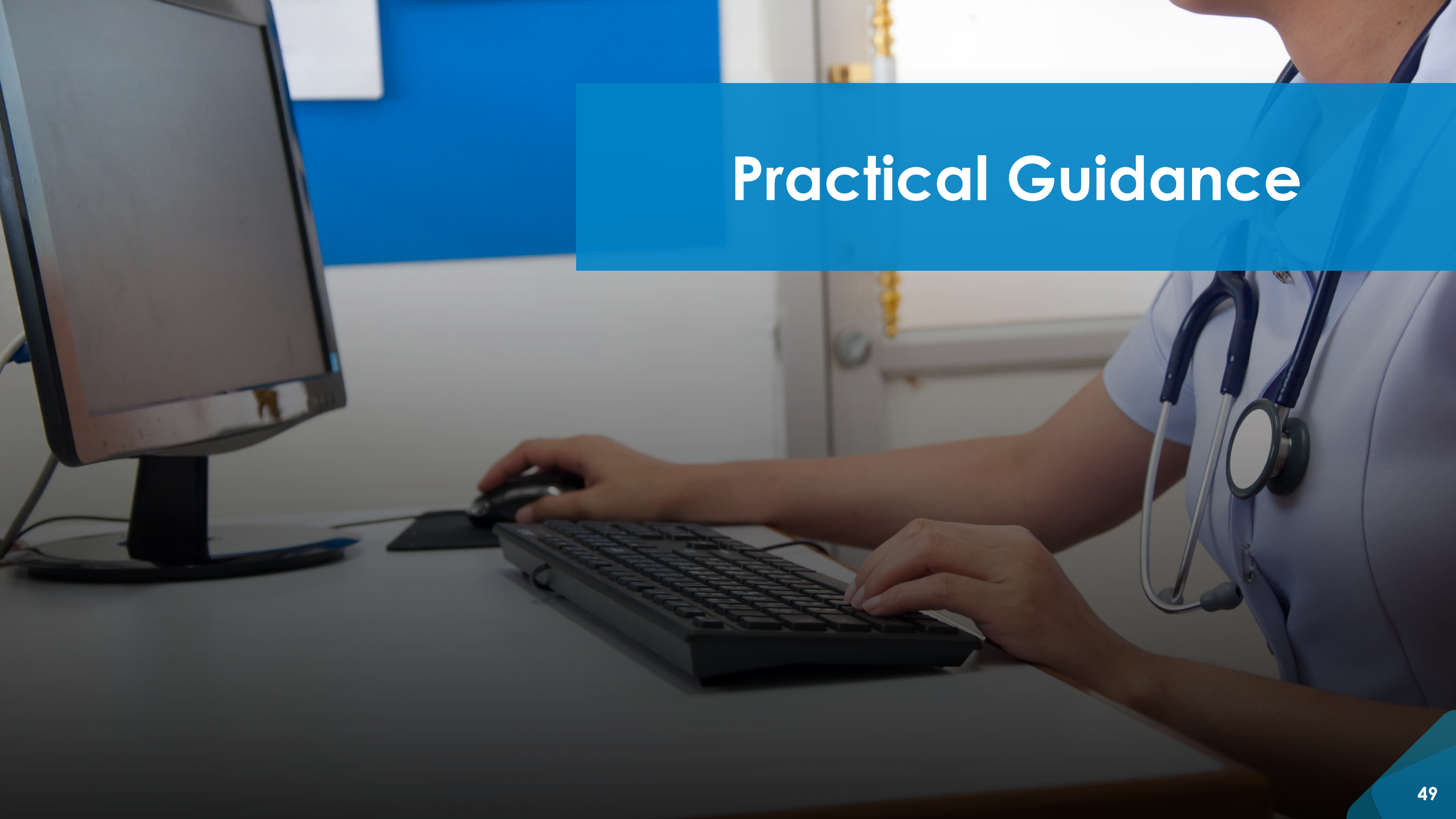
Conclusions

All 4 industries experienced disruptions during the pandemic. This study highlights several big trends, issues and opportunities.

First, we all came under attack from cyber-crime and many schools, hospitals and companies found their security was poor. We all need to treat security as a top priority in the coming years and improve our defenses, security awareness and governance.

Second, technology is still underfunded in many companies. This shows through the slow onboarding of new employees, the delays in getting IT support, the use of unsecured personal devices and the ease of working around security policies.

Finally, remote working is becoming the norm, and the preference for many employees. Budgets and priorities will need to be adjusted and businesses need to empower their employees with solutions that **balance security with the user experience.**



Practical Guidance

Practical Guidance for Employers

1. Embrace Zero Trust

Zero Trust means you assume every login is a breach - unless explicitly verified.

Zero Trust leads to fewer breaches and less Shadow IT. Move away from using network drives and eliminate VPNs. Use Conditional Access, Azure Active Directory, OneDrive, and Microsoft Intune to build a perimeter based on devices and identity.

2. Go Password-less

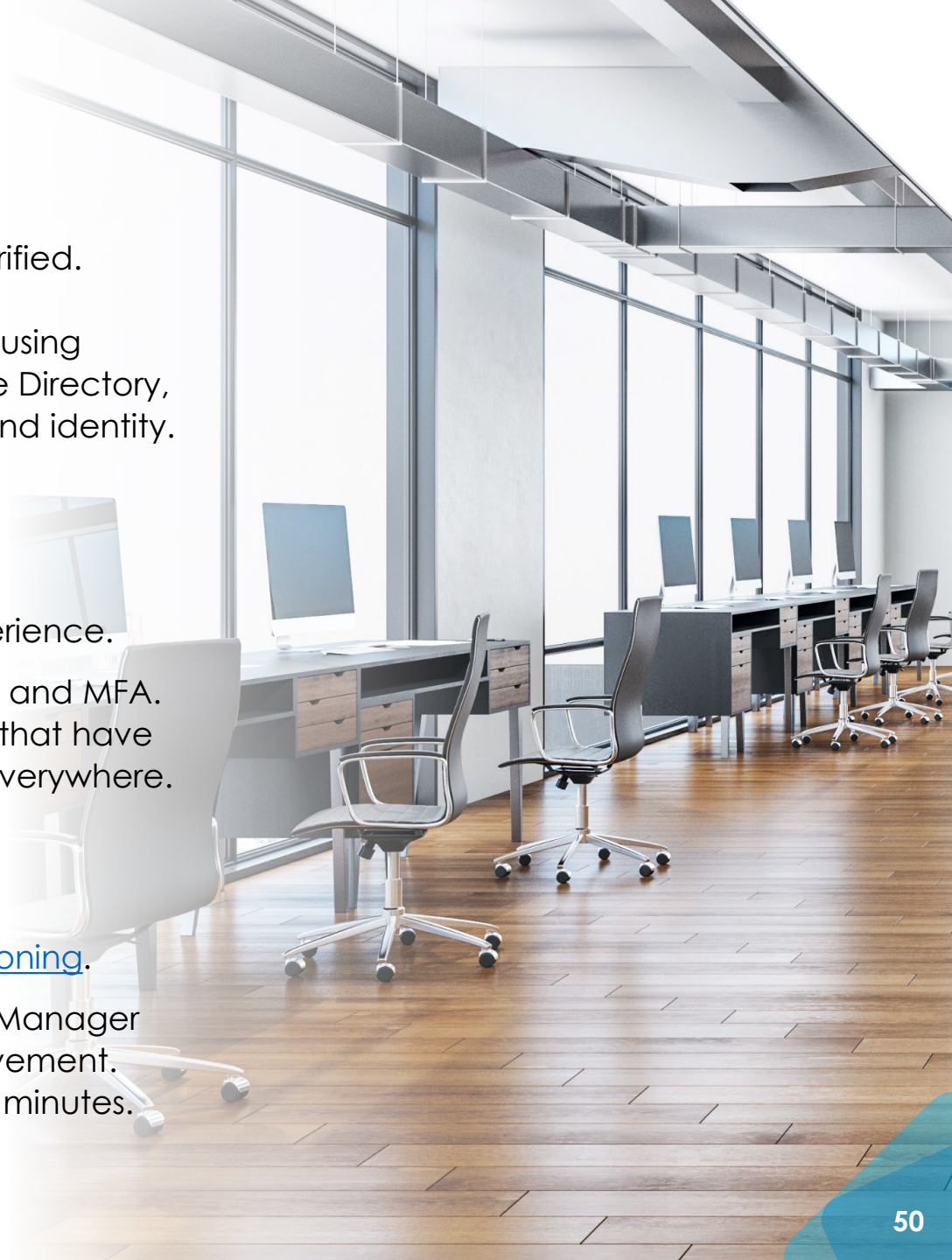
Password-less authentication is more secure, cheaper and a better experience.

Modern authentication means replacing passwords with biometrics, SSO and MFA. Choose laptops with TPM 2.0 to use Windows Hello, choose applications that have Single Sign-On via Azure AD and use MFA (multi-factor authentication) everywhere.

3. Reduce employee onboarding from 3 days to 3 hours

New employee devices can be set-up in minutes with Zero-Touch Provisioning.

Microsoft Intune, combined with Windows Autopilot and Apple Business Manager enables employers to ship devices directly to employees with no IT involvement. The employee can sign in and the devices self-configure, over the air, in minutes.



Research Methodology

NATIONAL STUDY METHODOLOGY

CUSTOM 25-QUESTION SURVEY COMPLETED BY

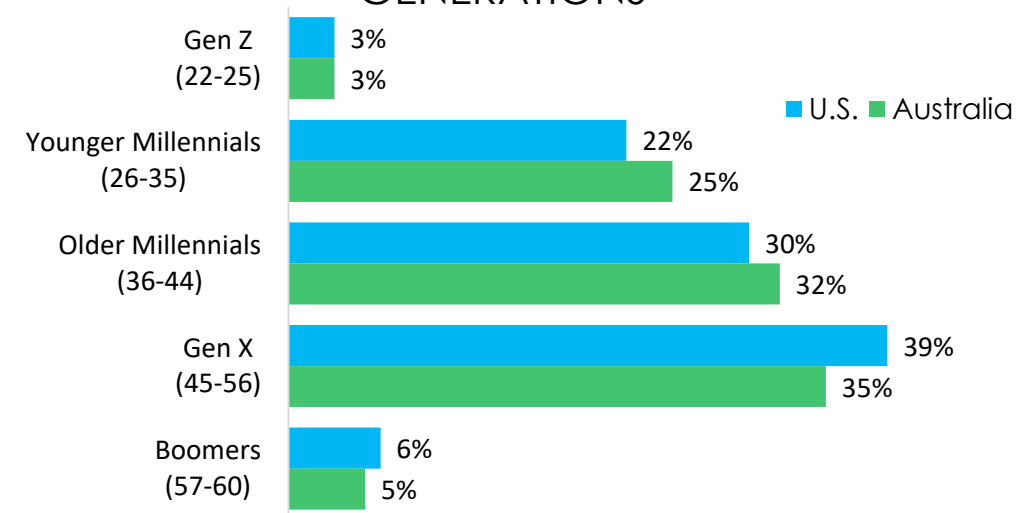
1,000
U.S. PARTICIPANTS
(AGES 22-60)

500
AUSTRALIAN PARTICIPANTS
(AGES 22-60)

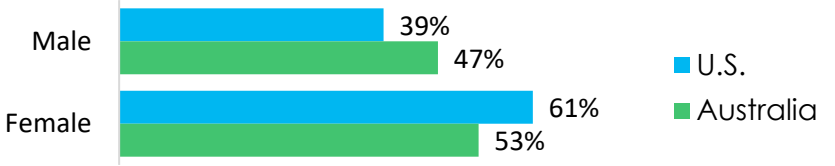
NATIONAL SAMPLE INCLUDES:

- 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

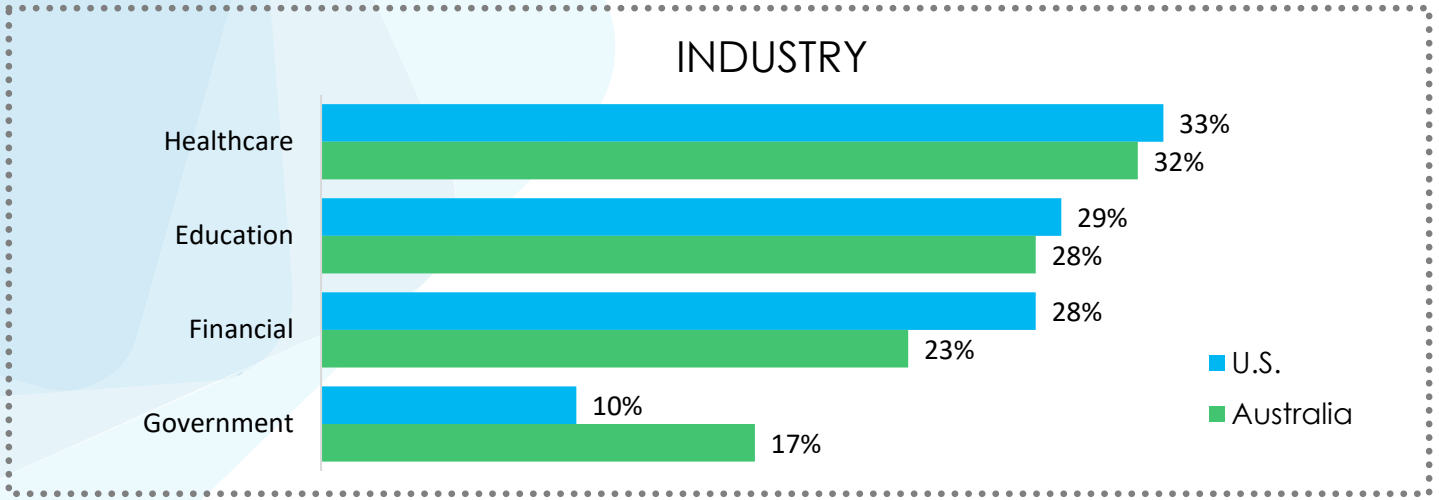


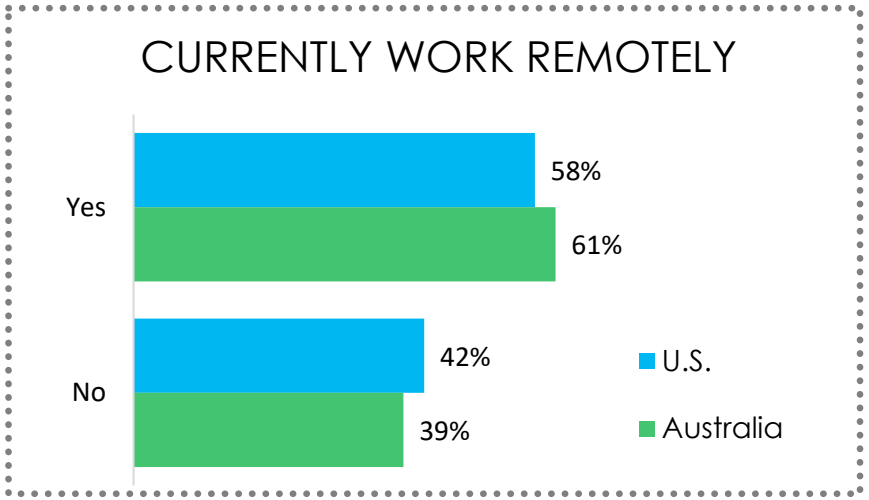
1% - U.S. Non-binary or prefer not to answer

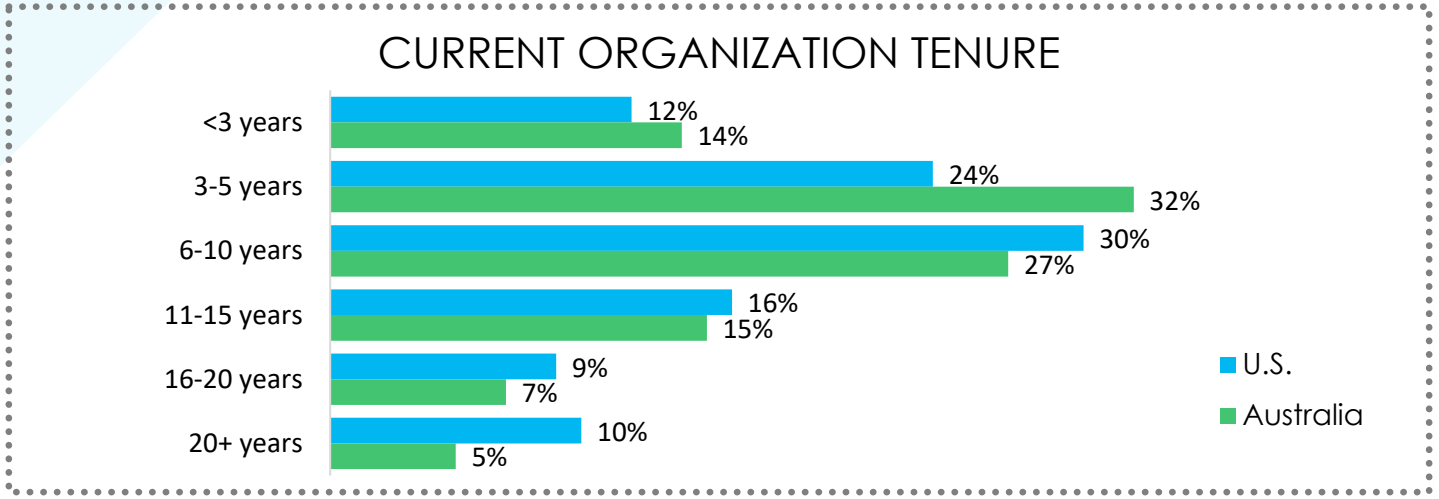
*U.S. Figures are statistically significant at the 95% confidence level. Margin of error is +/-3.1 percentage points.
*Australia Figures are statistically significant at the 95% confidence level. Margin of error is +/-4.38 percentage points.
*In an instance that a chart total for a single select question 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.

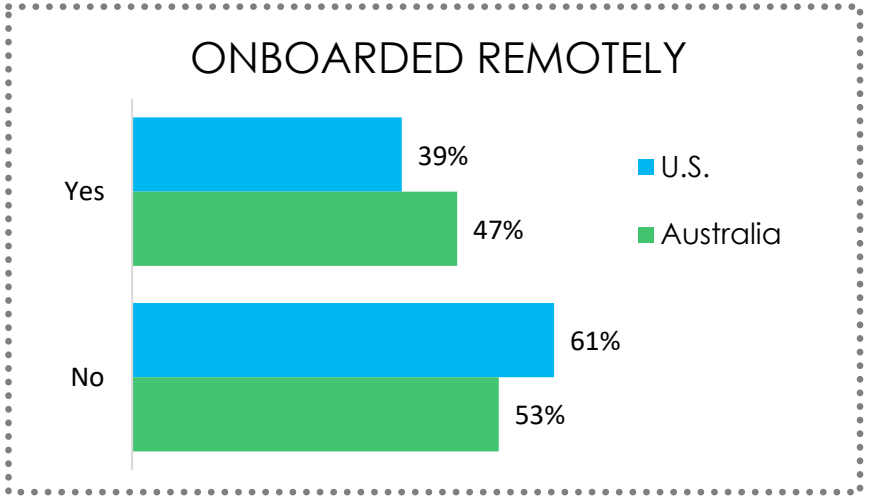
mobile mentor

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.