FORRESTER®

A Custom Technology Adoption Profile Commissioned By Dell | October 2017

Evolving Security To Accommodate The Modern Worker

GET STARTED ▶

A Custom Technology Adoption Profile Commissioned By Dell | October 2017

Evolving Security To Accommodate The Modern Worker

Security Should Protect And Enable

In order to keep pace with the growth of business mobility without falling prey to its potential risks, IT must be able to efficiently address complex issues ranging from service provisioning, device procurement, and security oversight. Why? Information workers need access to often sensitive information across a wide range of business applications and devices from wherever they are. In other words, security and privacy policies that doesn't impede end-user productivity will empower workers and boost their performance.

PROJECT BACKGROUND

In July 2017, Dell commissioned Forrester to conduct a study of the 21st century workforce and how their new habits, attitudes, and workstyles are reshaping the world of work. With more personas in a single organization to cater to, businesses are failing to deliver against workforce demands. To get their tasks done, workers are circumventing security policies to get what they want, in their moment of need. Organizations have to understand the different behaviors across the workforce and balance security needs carefully and equally or risk exposing themselves to existing and unprecedented new threats.

Country

- Australia: **25%**
- India: **25%**
- US: **25%**
- UK: **25%**

Type of organization

- Local: **11%**
- Regional: **35%**
- Multinational: **54%**

Annual revenue (USD)

- $400m to $499m: **21%**
- $500m to $999m: **31%**
- $1B to $5B: **28%**
- >5B: **20%**

Types of personas

- Office workers: Desk-centric: **32%** and Corridor warrior: **23%**
- Non-office workers: On-the-go pro: **24%** Remote worker: **22%**
- **Specialized role:** Intellectual property workers: Creative worker: **30%** and Engineer worker: **24%**

1 2 3

Today's Varied Workforce Uses Lots Of Devices

The digitization of the workplace is empowering information workers to get what they want, whenever they want, in their moment of need. The days of a dedicated worker who commutes to and from a single location every day of the week are just about over. The pervasiveness of mobile technologies, flexible work policies, and employee preferences now mean that today's digital workforce works from home, in public places, and in multiple locations. Information workers are also using a wide variety of devices. The challenge is for IT to help its workers use these devices safely to meet IT's own security protocols and make the business more efficient and successful, without interfering with employee autonomy or productivity.

For the purpose of this study, we defined the following types of workers:

- **Office workers:** Desk-centric and Corridor warriors.
- **Non-office workers:** Remote workers and On-the-go pros.
- **Intellectual property workers:** Creative workers and Engineer workers.

Laptops are still the most popular device amongst all types of workers with an average of 57% using them to get their jobs done, wherever they work from.

"Where do you use the following devices for work in a typical week?"

	Remote workers	On-the-go pro	Desk-centric	Corridor warrior	Creative worker	Engineer worker
Any type of desktop computer	58%	45%	67%	63%	58%	53%
Any type of laptop computer	69%	50%	63%	38%	61%	63%
Any type of 2-in-1/'convertible' with touch screens and screens that swivel	26%	34%	17%	23%	33%	38%
Any type of shared workspace	20%	28%	16%	22%	31%	19%
Any type of ad hoc displays for collaboration	19%	20%	17%	12%	24%	20%
Any type of portable data storage and accessories	21%	34%	26%	21%	36%	32%
Any type of tablet computer between 7 and 12 inches in size	17%	35%	20%	18%	27%	28%
Cell phone	13%	22%	6%	6%	15%	14%
Smartphone	56%	64%	57%	41%	70%	59%
Purpose-specific mobile connected device	10%	16%	5%	18%	9%	10%

Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

A Custom Technology Adoption Profile Commissioned By Dell | October 2017

Evolving Security To Accommodate The Modern Worker

1 2 3

Employees Perceive Their Firms' Security Processes To Be Reactive

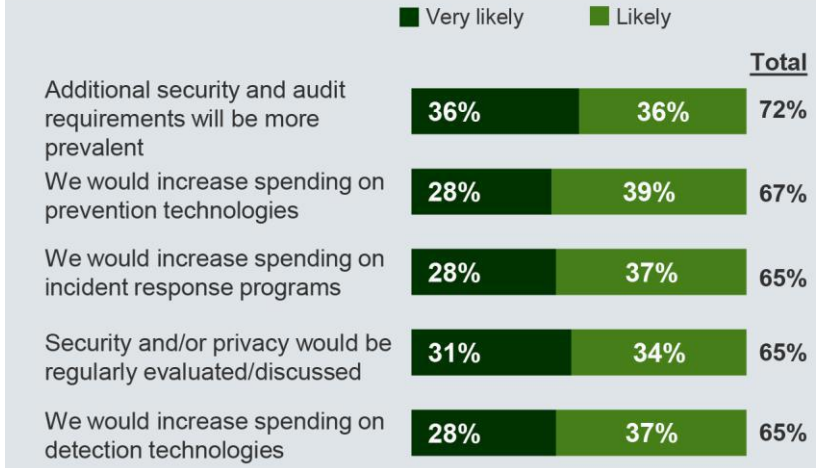
Data is the lifeblood of today's digital businesses; protecting it from theft, misuse, and abuse is a top priority for organizations across the globe, especially since firms don't have to look far or even follow the news to know that threats to data are running rampant.

Information workers revealed that if a security breach did occur, it would lead to more spending, more security projects, and more requirements. For instance, respondents said more security and audit requirements (72%), increased spend on prevention (67%), and increased spend on detection technologies (65%) would occur due to a security breach.

Moreover, a security breach would not only gain organizationwide attention but would directly impact the business in that the brand will be portrayed negatively (62%) and attract bad publicity (59%).

82% of information workers rated their company's response to a security breach as very responsive or responsive.

"What do you think is most likely in the event or consequence of a security breach?" (Showing top five "Very likely" and "Likely" only)



Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

Evolving Security To Accommodate The Modern Worker

Coaching, Not Controlling, Leads To Better Security Practices

Organizations struggle to understand who and what their workforce is comprised of and how to manage today's diverse combination of worker types. All types of workers strongly agree or agree that security teams should explain how they help protect them, which will make them to more likely conduct good security practices.

However, some interesting variations emerge across the personas. Non-office workers (54% on average) and intellectual property workers (57% on average) said security costs them business opportunities, and that it should be easier for workers to communicate with prospects. Additionally, security teams must be able to support and even accelerate the use of different devices for workers; however, non-office workers and intellectual property workers said they find it difficult to work with their security teams: that they come across paranoid and hold them back.

"How much do you agree with the following statements about the teams managing security protocols on the devices you use for work? (Showing "Strongly agree" and "Agree" only)

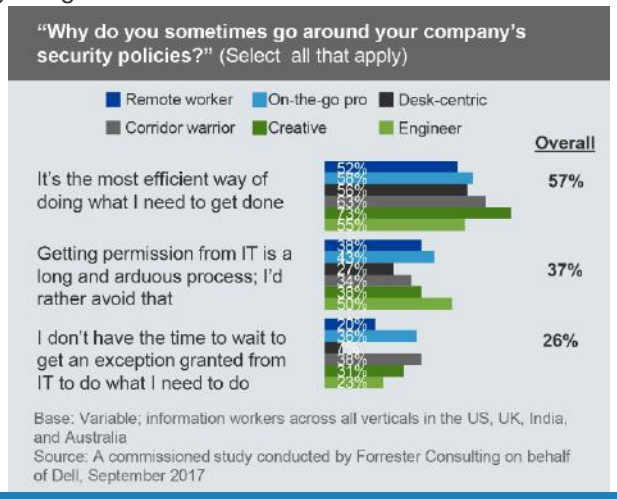
Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

1 2 3

Workers Are Thwarted By Their Own Organization's Policies

Workers are trying to get work done, but security controls prevent them from completing their tasks effectively, because security controls are poorly designed and because they're not dynamic enough to meet the different personas and their needs. This explains why half (50%) of information workers said security restrictions and policies make them less productive, and 41% said they sometimes go around the company's security policies.

In other words, workers choose the path of least resistance to get things done because it's the most efficient way (57%). Workers need and demand access to sensitive corporate information from their devices, and getting permission from IT is a long and arduous process (37%). Interestingly, non-office and intellectual property workers are more likely to break security protocol to get what they need. For instance, 75% of on-the-go pros and IP workers, as well as engineer (49%) and creative workers (52%), are more likely to break security policies; thus, firms should focus on them since they bring more concern.



1 2 3

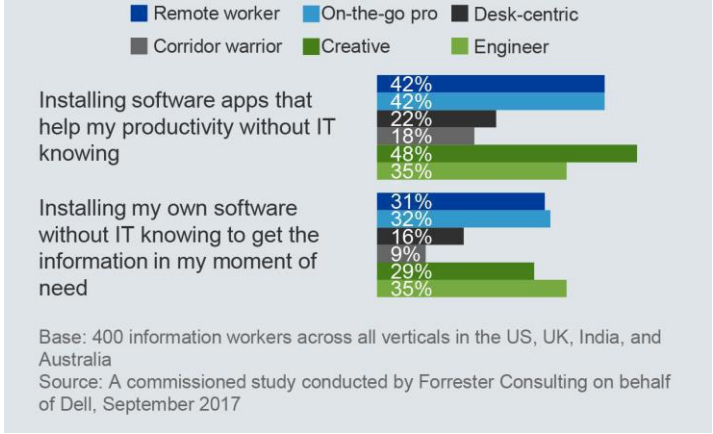
Workers Want To Be Productive, Not Malicious

Workers want access to software and apps to help them get their jobs done. If security teams place too many policies and controls in their way, like getting access to an app or downloading software, they'll actively look for alternatives from other sources and circumvent security processes — without IT knowing — increasing security risk. But, these actions are not being carried out by workers to be malicious in intent; they need access to apps and software in their moment of need to be productive.

Not surprisingly, office workers (desk-centric and corridor warriors) are less likely to install software or apps without IT knowing than their non-office (remote worker and on-the-go pros) and IP (creative and engineers) counterparts. They are instead more likely to do what they want if it means they're able to be productive and gain access to information when they want, wherever they want.

There are clear gaps in security: *62% of remote workers are worried about being blamed for a security breach or event. Engineer workers are worried about causing customer data leakage (73%) yet they feel they need to install apps to help with their productivity without IT knowing.*

"How would you go about getting the software you need in order to be productive?" (Select one)



Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

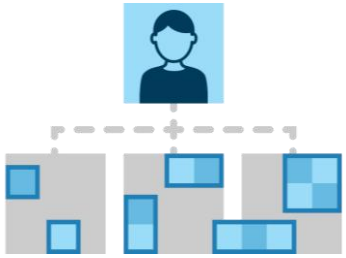
Evolving Security To Accommodate The Modern Worker

Workers Need To Share Data: IT Should Enable Them In A Secure Way

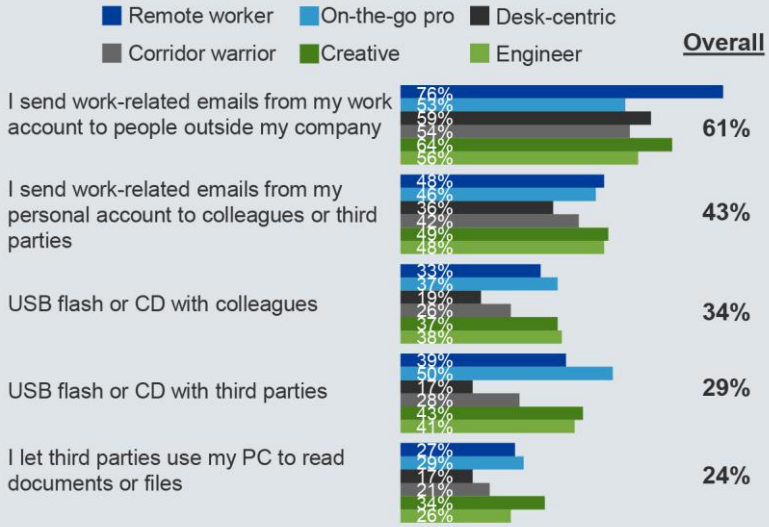
In the 21st century, data economy is mission-critical to understand that data has a life of its own. Organizations are collecting mountains of data, which means the burden of protecting data is growing due to the amounts of data that are being generated by the end-users and stored and duplicated in various places like cloud, USB flash drives etc.

Despite knowing the impact and what it would mean if a security breach does occur, workers want to share, need to share, and will share data amongst colleagues or third-party organizations. However, workers are sharing information in insecure environments, opening up the business to risk. Security professionals must find solutions to help support today's different personas in a much more secure fashion that's easy to access and seamless to use.

71% of workers said they share files with third parties daily or weekly.



"How do you share documents or files with third parties?" (Select all that apply)



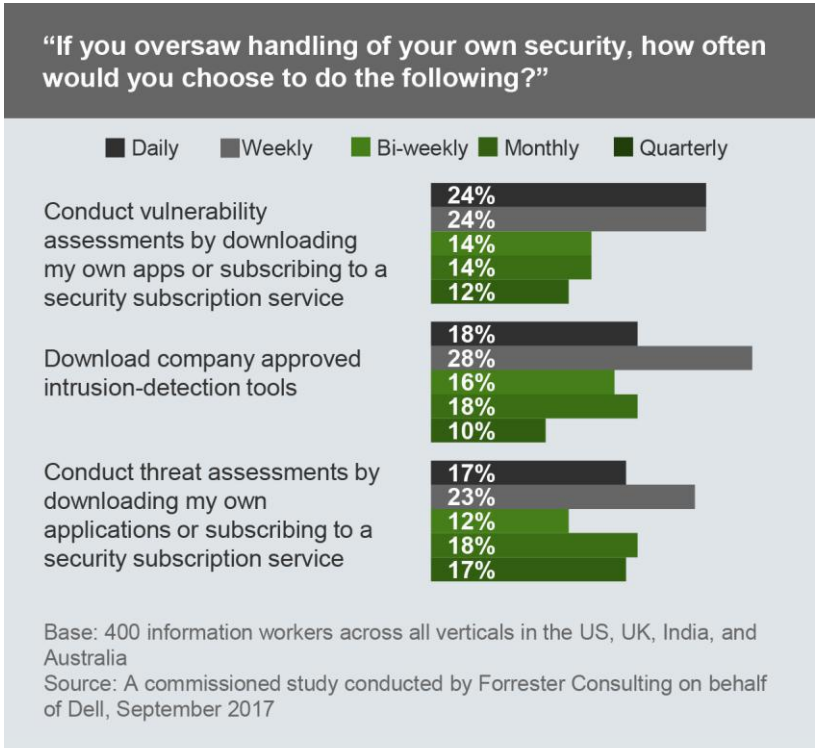
Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

1 2

Given The Authority And Tools, Workers Would Take Ownership Of Security

There's no denying that current approaches to security are extremely fragmented when looking at the different types of work personas. Workers appreciate security, but they want security to be less intrusive in their daily tasks. The less intrusive security is, the more workers will welcome it. But if IT impedes their productivity with authentication processes or sets restrictions around certain apps and tools to get their jobs done effectively, workers will become nomadic in their approach.

However, workers also understand that security is not an easy task; worker attitudes change because they are empathic with security teams. This explains why, given the control, employees would conduct vulnerability assessments at least monthly. The goal is to find the right balance between giving workers too much control and being less intrusive with security policies. Embedding file protection within the natural flow of work processes and installing malware protection is key to enabling workers to be productive and remain secure. A variety of security solutions can leverage this behavioral data to correlate potential threat activity at other layers (endpoint, network, physical/geographical) or make more informed decisions about the riskiness of a given transaction or behavior.



Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

1 2

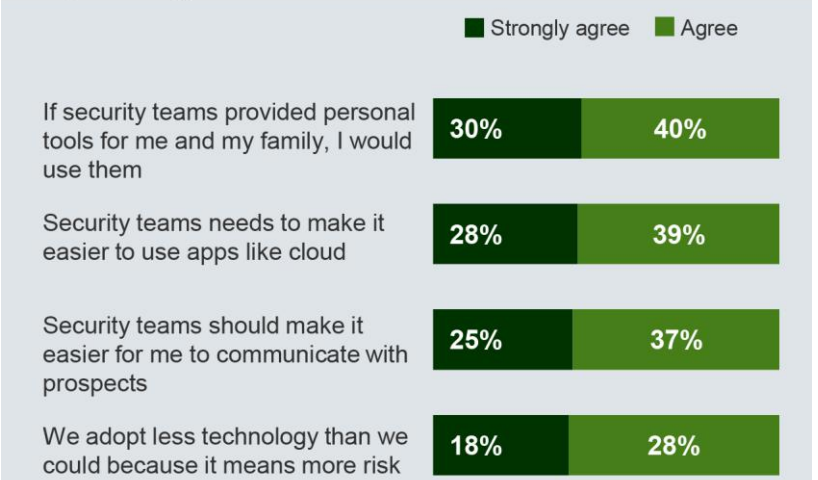
Security Teams Can Become A Workforce Enabler By Offering The Right Tools

Technology diversity and changing employee workstyles open the door to a host of security issues that threaten the brand and security of your organization. For instance, increased employee need for application and data access will push security teams to ensure that new workforce technology doesn't put sensitive information at risk yet still allows unfettered access for authorized employees, regardless of whether the company owns the devices they're using.

It's no surprise then that workers want personal security tools (70%) and access to apps in the cloud (67%). Providing security tools to all types of employees enables workers to practice better caution when accessing sensitive information.

Firms that look for security solutions that enable workers to collaborate effectively and safely will protect the business in the long run. To improve security without inhibiting productivity and business outcomes, security pros should enable workers to look after themselves with better tools and guidance. IT security teams' role should be to trust but also verify.

"How much do you agree with the following statements about the teams managing security protocols on the devices you use for work?" (Showing "Strongly agree" and "Agree" only)



Base: 400 information workers across all verticals in the US, UK, India, and Australia
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2017

A Custom Technology Adoption Profile Commissioned By Dell | October 2017

Evolving Security To Accommodate The Modern Worker

Consider All Employees: Security Needs For A Better Employee Experience

Technology is transforming how and where employees are working. Security teams must keep up and accommodate all types of workers. The study found three key findings:

› **Security teams must serve and protect non-office workers.** On one hand, office workers have lower security requirements and less exposure to risks since they're protected through the facility or office they're in. On the other hand, non-office and IP workers are more likely to be neglected. Firms must also accommodate them and understand a one-size-fits-all approach simply will not work for everyone.

› **Information workers circumvent security to be productive, not malicious.** Today's digital environment requires workers to act quickly. Evidently, security isn't helping them, especially workers who are outside of their company's offices. In order to get what they want in their moment of need to better serve customers, they circumvent security policies.

› **Worker habits amplify poor security practices.** Different persona types will perform and conduct their jobs in a way that is natural to their role. For example, non-office and IP workers have to share data with colleagues and third-party personnel, but a USB or a CD can get lost. In other words, the risk is in the insecure device, and work habits amplify them.

METHODOLOGY

This Technology Adoption Profile was commissioned by Dell. The custom survey questions were fielded to 400 information workers across all verticals in Australia, India, UK, and the US.

The custom survey began in July 2017 was completed in October 2017. For more information on Forrester's data panel and Tech Industry Consulting services, visit Forrester.com

Project Director

Tarun Avasthy
Market Impact Consultant