



MOBILITY AT WORK: MAKING PERSONAL DEVICES A PROFESSIONAL ASSET

September 9, 2013

800.800.4239 | CDW.com/MobilityAtWork

INTRODUCTION



Half of U.S. adults connect to the Web through either a smartphone or tablet,* and many are looking for ways to increase efficiency and effectiveness on the job by using those devices. Millions of workers are now bringing their own devices to work and using them to connect to their employers' networks, complicating already-complex computing systems.

Mobile computing taps and taxes every aspect of information technology management, and the Bring Your Own Device (BYOD) phenomenon represents one of the greatest challenges for IT professionals: empowering worker choice and productivity while protecting the organization's network, data and assets.

To examine this critical issue and better understand how to successfully integrate personal devices into total mobility management, CDW surveyed 1,200 workers that use personal tablets and smartphones for work and 1,200 IT professionals across eight industries. The resulting report identifies key needs to address in ensuring security and success, and outlines a path to total mobility management.



*Pew Research Center's Project for Excellence in Journalism, http://www.journalism.org/analysis_report/future_mobile_news

FIVE PILLARS OF MOBILITY MANAGEMENT



- This report uses the following icons to tie research findings and recommendations to the five critical facets of mobility management:



Planning: Laying the groundwork for success with policies and plans for security and an end-to-end network strategy



Enabling: Procuring and provisioning devices efficiently, whether employer- or employee-owned



Protecting: Integrating security and real-time centralized management of mobile devices, applications and content, as well as real-time monitoring and expense management



Supporting: Supporting help desk services for end users, supporting employer- and employee-owned devices alike, and administration and management tools for IT



Empowering: Enabling employee collaboration, productivity and efficiency with cross-platform integration, applications, browser-based access and virtualization

UPHILL CLIMB

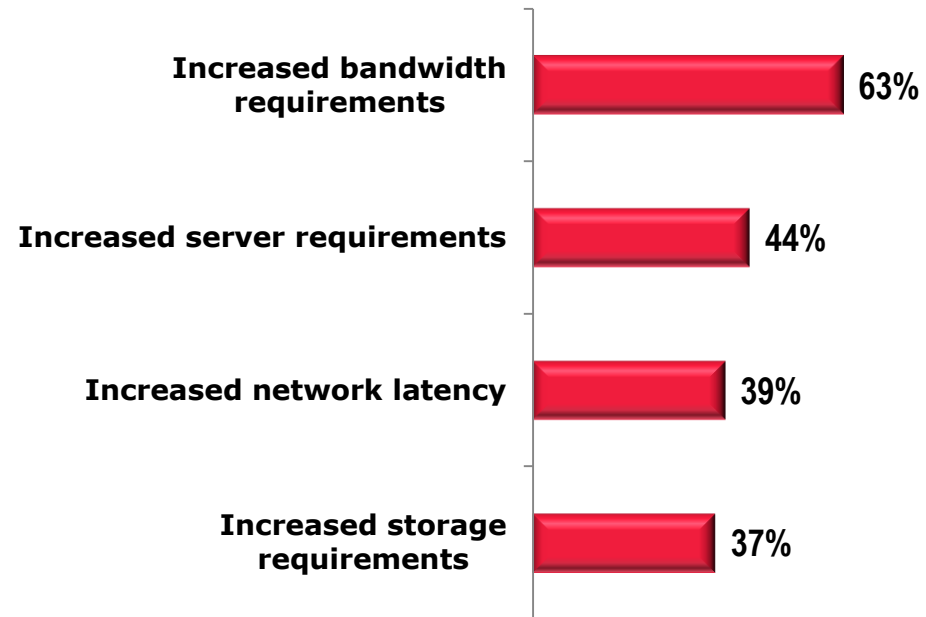
- IT professionals expect the number of personal smartphones and tablets accessing their networks to **more than double** in the next two years. **But**, the devices are only a fraction of the challenge:



92% of IT professionals surveyed say their organization has **encountered challenges** with personal device adoption.

Top challenges include securing data on personal devices (55%), securing network access (54%) and network performance (39%)

Looking ahead, nine out of ten expect the growth of personal mobile devices to have **major network impacts**, primarily:*



*Respondents asked to select all that apply

DATA (AND ORGANIZATIONS) AT RISK

- Increased access means increased risk:

54% of BYODers say they use their devices for business applications beyond phone calls and email



86% of BYODers say they access or save work-related information on their mobile device

52% of BYODers say they use more than one device

And **5%** have lost the personal mobile device they use for work, or had it stolen



That's a **one in 20** chance for a leak

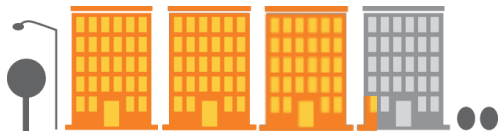


INITIAL EFFORTS IN PLACE

- Organizations are trying a variety of very basic measures to increase security:

According to IT:*

76%



More than three quarters implement guidelines for the use of personal mobile devices

69%



More than half require a user password for network login

42%



And, nearly half enforce the use of a screen lock on personal mobile devices



*Of those respondents whose organizations have security policies or measures in place

BUT THERE'S MORE WORK TO DO

- There are many other, more effective measures, but their adoption is more complex and they lag even further behind the simpler ones. Several examples:

According to IT professionals,* only:

15% use partitioning, or securing and controlling a portion of personal mobile devices



22% limit the applications employees can load on personal mobile devices



24% use location tracking to recover lost or stolen personal devices



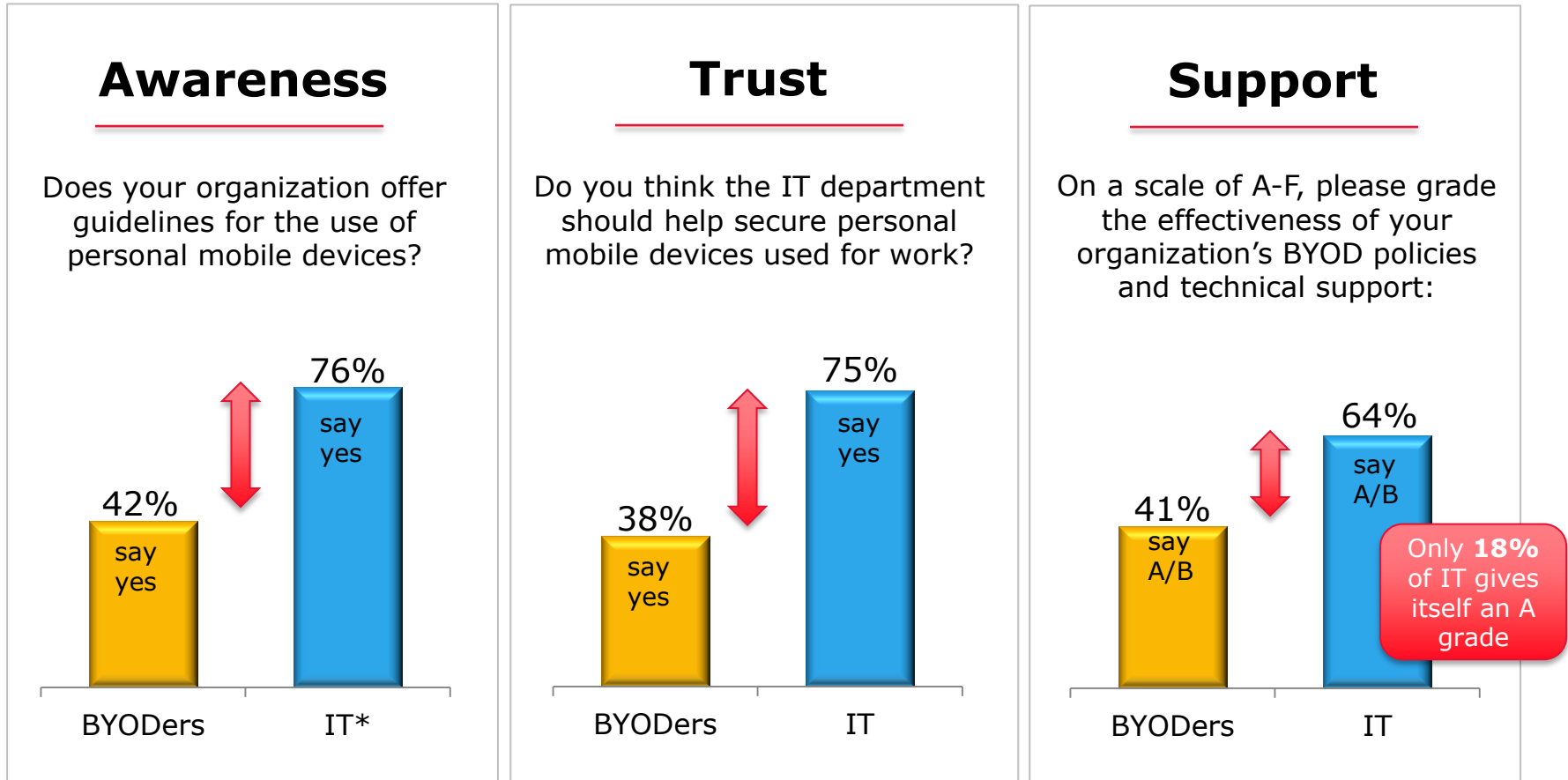
Additionally, more than half of IT professionals say their department recommends specific mobile applications or devices for employee use.



*Of those respondents whose organizations have security policies or measures in place

THREE CRITICAL MANAGEMENT GAPS

- Broad mobility programs require A-level support, but even IT says that is hard to provide:



*Of those respondents whose organizations have security policies or measures in place

WHY YOU NEED A PLAN

- Smart devices need genius infrastructure:

BYODers: How can IT better support you?



“Have a site on the agency intranet to **explain what is allowed** and instructions on uses. **Security backup** would be great”



“Make it clear how IT can be of **assistance** with a personal device if it is being used for work purposes”



“**Allow us to access apps** which could be used for work so we aren't **as dependent on our PCs**”



“Improve IT's **availability for technical issues**, including faster response times”



“Offer **training** to show what devices are available and how to use them (including software, apps, devices) to **make my job easier**”



“Employ **better IT security** and **encrypt** work-related data and information”

Bottom Line: Employees need support and empowerment





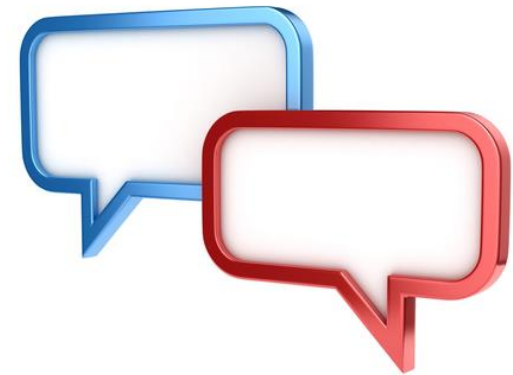
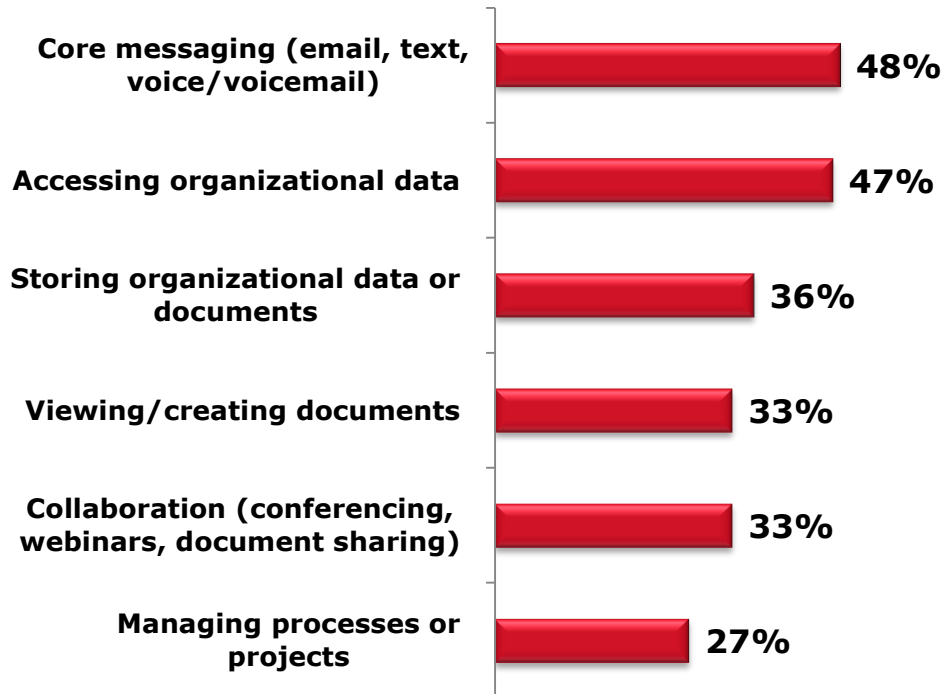
RECOMMENDATIONS

STUDY USER NEEDS; PLAN LASTING SUPPORT



- IT professionals have concerns, but lack real dialogue with users:

What functions is your organization most concerned with supporting via the personal mobile devices employees use for work?*



But, **only half** (51%) of IT professionals say they actually **talk** with employees about how they use personal mobile devices



*Respondents asked to select all that apply

SECURITY SOLUTIONS SHOULD BALANCE EMPLOYER AND USER CONCERNS

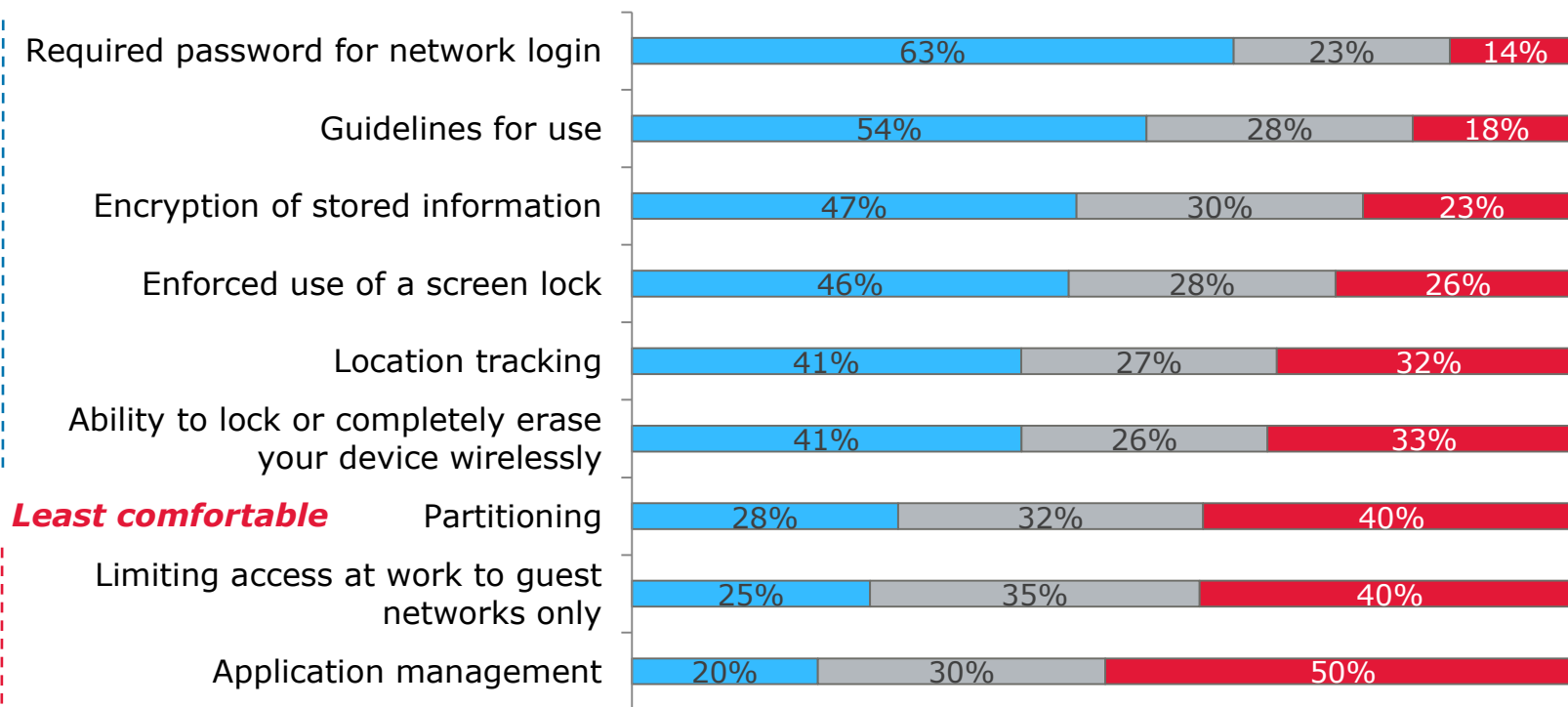


- BYODers are open to additional security measures, but some of the most effective measures make them the most uncomfortable:

BYODers: How comfortable would you be with your employer taking or requiring the following steps to secure your personal mobile device(s)?*

Most comfortable

■ Comfortable ■ Neutral ■ Uncomfortable



Least comfortable

*Full definitions provided to survey respondents; see slide 17 for details

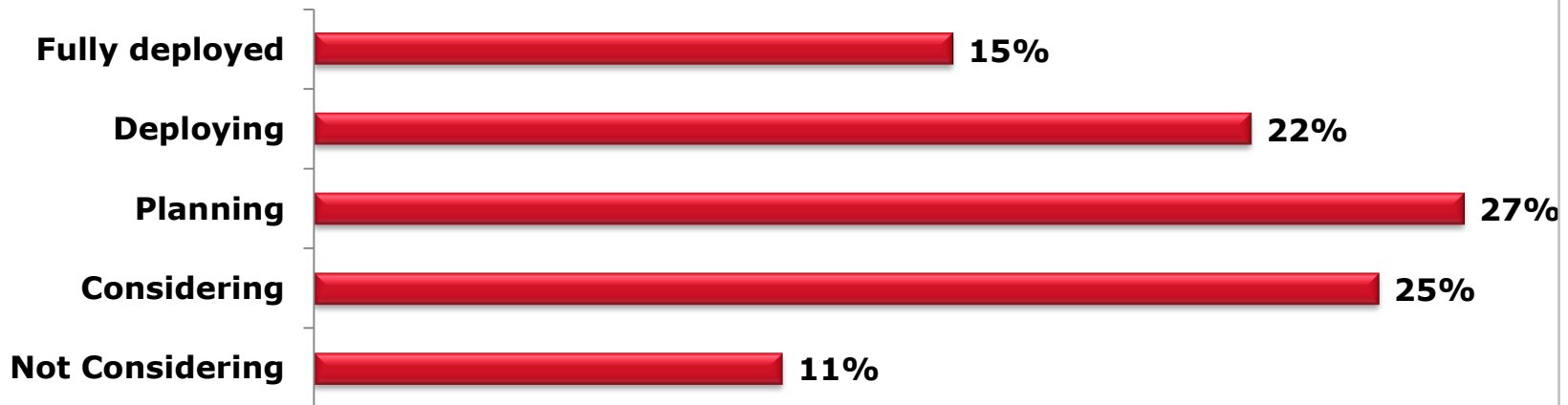


IMPLEMENT COMPREHENSIVE MOBILITY MANAGEMENT



- Current efforts fall short – **36%** of organizations have not planned or deployed an MDM solution:

IT: Where does your organization stand with Mobile Device Management?



Currently, **half** of the existing or planned MDM systems do not cover personal mobile devices

Of those not considering an MDM solution, **20%** plan to prohibit the use of personal mobile devices and **32%** plan to do nothing

Slightly **more than one-third** of respondents (**36%**) are currently deploying or have completed deployment of a mobile application management (**MAM**) solution

Of those considering or making a plan for an **MAM** solution, just **11%** will begin deployment within the next 6 months



INTEGRATE, INTEGRATE, INTEGRATE








- Develop an integrated management solution to:
 - » **Identify** impacts of mobility adoption on your IT infrastructure and address them in your plan through dialogue with users and across IT
 - » **Address** the impact on your IT team's time of procuring and provisioning devices and supporting mobile users; simplify use of mobility for employees to gain the most return on investment
 - » **Optimize** your voice, data and text plans to minimize expense
 - » **Integrate** commonly used mobile apps with your core applications, but do so securely
 - » **Monitor** how many devices are accessing your network and what they are doing there
 - » **Improve** mobility's ROI through development and use of custom apps to address key internal processes
 - » **Capture** the leverage that mobile apps can give you with your customers



MANAGING THE FUTURE OF MOBILITY



- Consider an integrated management solution addressing the five critical components of mobile adoption:
 -  **Planning:** Only half of IT professionals say their department actually speaks with users to understand how they use personal mobile devices – but that is essential to development of a mobile strategy and technology road map, data and device policies, security and network integration
 -  **Enabling:** Implement your policies through automated procurement, provisioning and deployment of devices, all integrated through a management portal tailored to your needs
 -  **Protecting:** Integrate security and real-time centralized management of your mobile devices, applications and content, with real-time monitoring and expense management
 -  **Supporting:** Live and self-service help desk services for end users, supporting employer- and employee-owned devices alike, as well as MDM administration
 -  **Empowering:** Enabling employee collaboration, productivity and efficiency with cross-platform integration, applications, browser-based access and virtualization



METHODOLOGY & DEMOGRAPHICS

- CDW surveyed* 1,200 IT professionals and 1,200 non-IT professionals who use a personal smartphone and/or tablet for work purposes at least once a week. The total sample for each group represents eight industries and equates to a margin of error of $\pm 2.7\%$ at a 95% confidence level. Individual industry samples equate to a margin of error of $\pm 8.0\%$ at a 95% confidence level:

BYODers	Personal mobile device	Gender	Age	Industry
100% of respondents use a personal mobile device for work purposes at least once a week	43% smartphone 9% tablet 48% both	44% male 56% female	7% 18-25 24% 26-35 18% 36-45 23% 46-55 21% 56-65 7% 66 or older	Small business n=150 Medium business n=150 Large business n=150 Federal government n=150 Healthcare n=150 Higher education n=150 K-12 public school district n=150 State and local government n=150

IT professionals	Title	Industry
100% of respondents work in a role involving the oversight, management or support of mobility initiatives or devices	CIO/CTO Deputy CIO/CTO IT Director/Supervisor IT Manager Network Administrator Data Center Manager Other IT management	15% 4% 23% 29% 13% 4% 12%
		Small business n=150 Medium business n=150 Large business n=150 Federal government n=150 Healthcare n=150 Higher education n=150 K-12 public school district n=150 State and local government n=150

*Research conducted by O’Keeffe & Company

SECURITY DEFINITIONS



- Below please find the full security comfort question, including definitions, referenced on slide 12:

How comfortable would you be with your employer taking or requiring the following steps to secure your personal mobile device(s)? Please rate each of the following on a scale of 1-5, where 1 is "very uncomfortable" and 5 is "very comfortable."

- a. Guidelines for use
- b. Enforced use of a screen lock on your device(s)
- c. Required user password for network login
- d. Encryption of information stored on your device
- e. Location tracking (ability to track or locate your device if it's lost or stolen)
- f. Ability to lock or completely erase your device wirelessly if it's lost or stolen
- g. Limiting your *personal* device's access at work to guest networks only
- h. Partitioning (your employer secures and controls the portion of your mobile device that supports work applications, while you control the rest)
- i. Application management (your employer limits applications you can install, OR deploys, secures and maintains specific work-related applications on your mobile device, leaving you in control of all other applications and functionality of your device)



THANK YOU.

FOR ALL MEDIA QUESTIONS AND INQUIRIES, PLEASE CONTACT:

***KELLY CARAHER
CDW PUBLIC RELATIONS
847-968-0729
KELLYC@CDW.COM***

***MARTY NOTT
O'KEEFE & COMPANY
585-271-1141
MNOTT@OKCO.COM***

800.800.4239 | [CDW.com/MobilityAtWork](https://www.cdw.com/MobilityAtWork)