

WHAT'S INSIDE:

Making it easy to find out what's new >>>

3 CHAPTER 1: Mobile Strategies: Architecture for Success

- Building a Secure Foundation
- How to Approach BYOD?
- A Roadmap to Success
- Operations Monitoring and Reporting

7 CHAPTER 2: Policy & Planning for Mobility

- Data Access Policy
- Device Policies
- Network Strategy

10 CHAPTER 3: Getting a Handle on Hardware

- Different Workers, Different Devices
- Device Categories
- Features and Options
- Choosing a Carrier

22 CHAPTER 4: Managing the Mobile Fleet

- Acquiring Mobile Devices
- Mobile Device Management
- Expense and Telecom Management
- Security and Mobile Devices

26 CHAPTER 5: All About the Apps

- Application Stores
- Mobile Application Management
- Security and Apps

29 CHAPTER 6: The Network: Connecting All the Dots

- Assessment and Planning
- Controller-based Management and Monitoring
- Mobile VPNs
- Cloud and the Mobile Network
- Security and the Network

33 CHAPTER 7: Providing a Helping Hand

- Help Desk Options
- Warranty Services
- MDM Customization Services

35 INDEX

29 THE NETWORK: CONNECTING ALL THE DOTS

FOR MORE
INFORMATION
ON MOBILE
SOLUTIONS, VISIT
CDWG.COM/MOBILITY



GET **M.CDWG.COM** ON THE GO
M.CDWG.COM is now available anywhere with our new mobile-friendly website or download the CDW-G app for your iPhone from the App Store.
GET IT at **M.CDWG.COM**

WHAT IS A CDW-G REFERENCE GUIDE?

At CDW-G, we're committed to getting you everything you need to make the right purchasing decisions – from products and services to information about the latest technology. Our Reference Guides are designed to provide an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

MOBILE STRATEGIES: ARCHITECTURE FOR SUCCESS

A productive mobile program starts with holistic research and planning.



Digital technology continues to innovate. Mobile devices and the infrastructure supporting them have ushered in a third wave of end-user computing. First, the desktop PC revolutionized who could use computers (nearly everyone). Next, the notebook PC demonstrated where computing could take place (nearly anywhere). Now, mobile devices are making computing completely ubiquitous.

Technological advances have enabled mobility and mobile solutions. But the reason mobility has truly taken hold lies in its power to transform the organization it serves. Mobile endpoints and the infrastructure supporting them not only offer the potential to reduce computing costs, they also offer the potential for making the entire organization more efficient. Mobile endpoints keep getting lighter and more capable – whether smartphones, tablets or any of several classes of portable PCs and systems.

With always-on, always-connected devices, workers can remain productive

in more situations and time frames that suit them – often speeding communication and the delivery of work. The new generation of mobile endpoints enables each function within a private- or public-sector organization to combine unified communications, enterprise applications and data access, and domain-specific applications into one device.

It wasn't long ago that the idea of mobile devices as full-access network endpoints was, to say the least, a novelty. If an IT team considered the notion, it faced numerous obstacles, such as a lack of global wireless bandwidth, few tools for porting enterprise apps to small screens atop unfamiliar operating systems and immature policy development surrounding the adoption of super-portable devices. Plus, IT and compliance staffs faced additional tricky challenges around how to maintain cybersecurity and mitigate the risk inherent in lost or stolen devices.

All those hurdles have been overcome.

Mobile endpoints and the components needed to support them at an enterprise level have matured. What's required for success with enterprise mobile solutions is the right level of enterprise commitment coupled with a sound policy, strategy and execution plan. This reference guide lays out a roadmap to help with each of those items.

Building a Secure Foundation

Security must undergird any mobility solution. When mobility strategies started to become something distinct from those governing telework, and the bring-your-own-device (BYOD) trend began to take hold, many CIOs and chief information security officers (CISOs) focused almost exclusively on the devices themselves. That's because for many, the most basic enterprise app, email, was first rendered mobile

with the proliferation of BlackBerry handhelds. The email system associated with the devices used native encryption, making it safe for widespread use.

Eventually, the device market became more diffuse, with user demand driving a growing variety of devices and OSs. As workers increasingly sought to use their personal devices on the job, CIOs and CISOs feared bleed-through from personal apps and data that shared memory and storage with organizational information.

But these fears were addressed. The swift evolution of mobile architectures and tools available for managing wireless devices has made those problems largely avoidable or manageable.

Security in the increasingly common any-device environment derives from embedding security best practices in all phases of the mobile-wireless lifecycle,

from selecting and provisioning devices to eventually deactivating them. But security thinking also must encompass the wired and wireless networks that portable and mobile devices access, access and identity management controls, and policies and training for users and technologists.

In fact, security integration continues to be one of the main technical challenges in rolling out and managing an enterprise mobility solution. That's why it's important to view mobility holistically, rather than as a series of siloed technologies.

Many organizations start with a device-centric view and work outward – from the apps and data to the device ports, and then finally to wireless and wired networks. This approach has one advantage: It acknowledges and compensates for

IS BYOD RIGHT FOR YOUR ORGANIZATION?

The following questions can help determine if a bring-your-own-device initiative is right for the organization.

➤ Who or which functions will be entitled (or required) to participate in the BYOD program?

Keep in mind, the desire of workers to have cool devices doesn't necessarily align with organizational needs.

➤ What will the cost trade-offs look like?

For instance, some devices that workers want to use likely will function as their only endpoint. Others may also need an organization-supplied desktop or notebook computer. The number of devices will affect software licensing, IT support and acquisition budgets. The various voice and data plan options also must figure into cost strategies.

➤ Is the IT organization prepared to support BYOD?

Depending on the specific device policy, the technology team will have to support new OSs, apps and hardware configurations. It may have to set up a user self-provisioning app site as well.

➤ Which devices are the organization willing to support in terms of OSs and models?

Apple iOS devices all look alike in terms of support, but Android comes in many flavors.

➤ What are the physical security and cybersecurity changes that will be required?

The parameters of the existing security program and how the IT team monitors user security networkwide will need to be reviewed and possibly enhanced.

the fact that mobility and wireless access pretty much obliterate the classic enterprise perimeter, once easily guarded by a firewall.

How to Approach BYOD?

Few questions have produced as much debate and angst as the BYOD model. In trying to fashion a BYOD policy, an organization confronts the proverbial onion. As decision-makers look deeper into the question, fresh questions arise.

Still, the principle of using personal devices for professional purposes has become well established in the minds of workers, whether in sales, marketing, engineering or finance. Therefore, in designing a mobility framework, organizations should at least consider various approaches to BYOD as part of their overall solution.

The IT department will have to evaluate the two basic BYOD approaches: organization-issued devices authorized for personal use, and worker-purchased devices approved and configured for enterprise use.

While most organizations currently conceptualize BYOD initiatives as programs that involve smartphones and tablets, a few are extending this thinking to BYOC, or "bring your own computer."

A Roadmap to Success

Enterprise mobility is a state of being, but it's also a measurable, repeatable process. Approaching mobility from a lifecycle standpoint will help an organization focus on optimizing each stage of the process. Having some guidance on what to expect at the different points of the mobility lifecycle is valuable for planning purposes. Such a roadmap should cover the following:

- **Planning and policy development**, from device selection through eventual deactivation, including which types of workers most benefit from a BYOD program



- **Mobile device management (MDM)**, either hosted on premises or as a cloud service, and security as a managed service using leading vendors such as AirWatch, MobileIron, MaaS360 by Fiberlink, McAfee and Symantec
- **Application management**, including setup, license management and operation of an in-house app store
- **Data center and network optimization** to handle anticipated growth in bandwidth and storage requirements caused by the influx of new wireless devices
- **Help desk and warranty services**, plus monitoring of wireless plan usage and carrier billing (based on knowledge-driven advice on adjusting plans to achieve the most efficiencies)

Whether contracting with a vendor or keeping the initiative in-house, using a holistic roadmap approach also benefits the IT team by identifying potential roadblocks that can stymie a mobility implementation. For example, traffic can overwhelm the network as many users

start to utilize multiple wireless devices in the workplace. Network upgrades may need to encompass not only the wireless segments but also the core network.

Additionally, because it is relatively easy to unify communication channels on mobile devices, users might also drive up bandwidth demands through apps such as video conferencing. The use of a forward-looking roadmap helps define such issues and then plan for changes accordingly.

Similarly, security and endpoint protection challenges are also surmountable with proper planning and use of the latest techniques in containerization and dual-identity device configuration. But strategizing for mobility must include modeling of the ways that enterprise apps and data potentially can be compromised. Again, a roadmap approach offers a way to make sure all security bases are covered.

Operations Monitoring and Reporting

An effective enterprise mobility solution requires ongoing knowledge of

how all of its elements are performing and whether users and devices are conforming to policy. MDM systems are key here, providing knowledge that falls into three main buckets: whether endpoints are policy-compliant with respect to permissible apps and usage; how networks and wireless plans are being used; whether devices and use conform to security requirements.

The ability to manage and control apps is foundational to successfully overseeing mobile devices and their performance. The app portal or download site is essential to maintaining policies.

An emerging subfunction of MDM, mobile application management (MAM), ensures that downloaded apps are equipped with security add-ons such as “wrappers” that can isolate them and their associated data from the other contents of a device. This works in reverse as well, so that if an onboard app needs to be remotely wiped, the MDM solution can accomplish this without necessarily obliterating the user's personal data.

An organization can exercise significant cost control if it monitors wireless usage per device, workgroup and department. By analyzing this information (such as who or what apps tap extensive bandwidth, where and when certain wireless use is heavy and how allotted minutes are consumed) the IT team can adjust apps, services and the network to provide for optimal and efficient use.

On the security front, users and administrators both have responsibilities. Users must set strong passwords, avoid any attempts at installing prohibited apps and immediately report lost or stolen devices. The IT staff must, based on MDM-generated reports, be sure the latest updates and security patches are in place for apps and OSs. ■

THE PORTAL PREMISE



For any organization with more than a few people, workers know where to go for certain needs, such as human resources or business travel services. That's because those functions have their own operations. But, increasingly, those functions are also becoming self-service.

This approach is taking hold in IT with mobility solutions centers on web portals that workers can visit to onboard devices, obtain wireless services, download apps and receive support services.

For desktop and notebook systems, software distribution generally takes place by simply burning each system's hard drive with a standard enterprise image. Distribution occurs either through the Ethernet network or desktside using a master DVD.

Vendors also deliver computers already loaded with the multiple configurations for an organization's various departments and users. To conform to enterprise cybersecurity policies, configurations typically don't provide administrative

rights, meaning users can't load personal or other third-party software or patches.

Mobile devices require a slightly different model of software distribution, more in line with the way consumer apps install on devices – that is, wirelessly, after accessing a download site. Following this model, organizations are building their own portals from which their users can obtain apps to provision either to their own or to enterprise-issued devices.

CDW can customize and operate a portal as a service. Keep in mind that a portal must do more than simply offer apps. It must also enforce policies that classify who can download particular apps.

Some organizations choose to offer a range of popular outside apps, such as Evernote or Skype, partly as a convenience to users and partly in an attempt to standardize apps on workers' devices. Portal communications run in two directions, so that the IT group can receive information from devices as well as push apps and updates to them.

POLICY & PLANNING FOR MOBILITY

An effective program hinges on understanding the current infrastructure and crafting a plan to achieve mission-driven goals.



Exciting though the mobility revolution may be, private- and public-sector organizations must be careful to plan and establish the right policies before launching a mobile program. It's important to establish with users the notion that the fun and games they might indulge in with personally owned devices are distinct from the use of the devices on the job.

At the same time, well-plotted and well-executed policies can enhance users' work experience, spurring collaboration, creating a highly reliable network and providing device performance that allows flexibility in how, when and where users work. Policies also ensure that the organization's data and business processes remain secure while enhancing the service being delivered to end users through mobility.

Data Access Policy

Today, nearly every organization has at least some workers using

smartphones. This isn't surprising, given that nearly two decades have passed since the BlackBerry debuted and email went mobile. What has changed rapidly in recent years is the use of mobile devices for accessing productivity and mission apps and data.

At the most fundamental level, the data access policy must establish whether the organization allows work data on personal devices, or personal information on enterprise-distributed devices. The decision depends on whether it can be done safely, and that in turn depends on whether containerization software is installed that sequesters different classes of data from one another.

Some solutions take this separation down to the chip level, requiring reboots with separate logins to toggle between enterprise and personal device "personalities." The new BlackBerry Z10 supports dual personalities running simultaneously, accessed by certain motions on the touch screen.

Another option is to split app access from data storage, so that no enterprise data is never stored on a device. In effect the mobile endpoint becomes a wireless thin client or terminal. Conversely, a containerized setup can let devices store data, with the proviso that the organization confers on its IT shop the means and authority to remotely wipe a device should that become necessary.

It's also possible to configure devices so that specified data cannot be copied to other apps, such as Evernote or Dropbox, or copied or forwarded in any manner. In short, data access necessary to performance of work must be accompanied by policies – and then enforced in configurations – to protect the data.

Device Policies

Carefully crafted device policies form a foundation for enterprise mobility solutions. Having the right devices used correctly simply makes mobility work for both users and the IT department that must administer them.

The policy should start with device selection itself. Too much latitude in allowable devices can complicate administration with multiple OSs and manufacturers. Popular collaboration apps work on all three mainstream OSs – iOS, Android and Windows. But porting custom enterprise apps to any of these OSs may represent a cost the organization doesn't want to take on. Plus, many device control apps are specific to certain OSs and can therefore be a driver in setting device policies.

On the other hand, it's unlikely that a single type of device will be suitable for everyone. Traveling staff, field workers, receptionists, tech support teams, financial staff, teleworkers – the list goes on – all have requirements unique to their jobs. For that reason, an organization will need to base its approved device list on a review of the services that various devices will support.

Whether to adopt a BYOD approach or supply all devices will also affect policy. The IT and management teams will have to determine the level of support needed for mobile devices, whether owned by users or by the organization. The options run the gamut: complete support for all devices, support only for an organization's apps – and sometimes, no support. Few choose the last option, because with support comes buy-in from users as well as enhanced ability to enforce policies.

Some other items to cover include:

- **Passwords and certificates:** For example, passwords should have a minimum level of strength and should be changed regularly.
- **Prohibited uses:** The policy should state clearly what uses are not allowed on mobile devices.
- **Geographic restrictions:** Using a technique called geo-fencing, device functionality can be limited to prescribed locations, the monitoring of which employs the devices' own location services capability. Certain apps may be allowed at the organization's offices.

- **Procedures for lost or stolen devices:** The policy needs to detail the steps that must take place should a user suspect that a device is irretrievably misplaced, including procedures for temporarily locking the device as well as wiping all or part of its contents.

Network Strategy

Upgrading the enterprise network will ensure that devices and apps perform well and that mobile workers are productive – justifying the organization's mobility investment.

It's critical that network optimization is not an afterthought because the addition of mobile devices will burden the network. Once mobile-enabled, staff will more readily use bandwidth-hungry apps. Without attention to wireless segments, network service overall may begin to degrade.

To plan for the effects on network traffic, the IT department first should conduct a survey of planned uses for mobile devices. Once this information has been gathered, the team can conduct a site survey of the existing network infrastructure.

Virtually all mobile devices have Wi-Fi capability. Cellular carriers' data plans favor the use of Wi-Fi in two ways. They don't count data over Wi-Fi against monthly data limits. The carriers presume that uploads and downloads over Wi-Fi will ultimately use the organization's (or the public Wi-Fi provider's) wired infrastructure as the primary data access means, so

DATA ACCESS MUST BE ACCOMPANIED BY POLICIES AND THEN ENFORCED IN CONFIGURATIONS TO PROTECT DATA.

THE CYBERSECURITY FRONTIER?



As organizations increase their use of mobile operating systems, the more likely these OSs will become malware targets. The Android OS market in particular has seen an exponential rise in malware.

But to some degree, all mobile devices are susceptible to tampering and attack. One new hack method unique to mobile devices is a variant of email phishing – text phishing, in which dangerous links are embedded in SMS messages.

For these reasons, organizations need special mobile security policies to protect enterprise assets against this new potential vector of attack and data loss.

The security policy should ensure that all devices use mobile virtual private networks (VPNs) to access apps and data, and that no device without containerization (to separate enterprise and personal data) is allowed access in the first place.

In planning the security policy, also consider:

Two-factor authentication: This will prevent access should a device fall into the wrong hands. The second factor, after a password, can be a biometric or a one-time-use password issued by a security server delivered via text message.

Remote access: The ability to remotely access a device lets the IT team push security services to devices so that all users remain compliant with security policies. It also provides the ability to wipe a device in the event of loss or theft.

Strict prohibition against jailbreaking:

A jailbroken device (one that has been made open to another carrier's network) automatically nullifies security controls. Thankfully, an MDM tool can alert the IT team or security operations center should a user jailbreak a device.

the data usage is already paid for.

Plus, the carriers sometimes throttle down the cellular bandwidth available to piggish apps, so performance is worse for a given app on cellular than over Wi-Fi.

All of this means, in addition to having policies that encourage the use of Wi-Fi whenever possible for cost and performance reasons, the IT department needs to give major attention to wireless infrastructure.

The site survey (along with a rough idea of how many devices the IT team estimates will be in use at any given time) will likely reveal a need for more access points, some of which may require more power than an Ethernet cable can provide, or may require two Ethernet connections. It's also necessary to understand the mix of apps that will use the network to gain understanding of

the quality of the expected traffic.

Beyond sheer capacity, to fully support mobile apps, the wireless LAN must also have app-awareness and the ability to prioritize simultaneous traffic. This allows latency-sensitive apps such as Voice over IP (VoIP) to receive priority over apps such as text messaging or email. It may be necessary to upgrade the switching and routing infrastructure to handle both the volume and type of traffic.

But here's the crux of mobility: Boosting Wi-Fi capacity will buy nothing if an organization fails to expand the wired back end leading to the data center. Continuous mobile connectivity requires high performance at both the edge (the wireless LAN) and the core (the wired network).

To accommodate the increase in traffic resulting from mobility, organizations must adapt their

networks in the same way cellular carriers are adapting theirs. Namely, the networks must become less focused on packet traffic and more focused on app performance.

Optimizing networks for mobility requires ensuring the core network meets four qualifications:

1. A uniform user experience, whether workers access resources wirelessly or when plugged in
2. A unified and flattened (two-tier versus three) wireless LAN (WLAN) and core network architecture
3. Orchestrated management to lessen the administrative burden of provisioning users
4. A routing and switching infrastructure with quality-of-service capabilities sufficient to manage collaboration and geo-location-rich mobile apps ■

Different Workers, Different Devices

Device Categories

Features and Options

Choosing a Carrier

GETTING A HANDLE ON HARDWARE

With a myriad of choices, the key is selecting devices that meet both end-user needs and organizational goals.



There are so many mobile device options that choosing or approving devices for users can seem overwhelming at the start.

Ultimately, no single mobile device fits every worker and every use case.

Rather than starting with devices, it's more useful to begin with the users and their tasks. And the first question is: What will each core group of workers do on a mobile basis? In this way, strategy will lead the device selection and not the other way around.

Different Workers, Different Devices

Some use cases are more obvious than others. Office workers such as those in marketing, finance and accounting departments need access to multiple apps when in mobile mode. They typically need devices that can present materials or view and manipulate spreadsheets and documents.

These workers can range from entry-level to executive, and they likely will need at least two devices. For example,

they might use an ultralight PC for enterprise apps and a smartphone for email and telephony. The larger device may be accompanied by a docking station or port connection for use with a standard monitor and keyboard when in the office, and it should have an Ethernet port for when it is docked.

Another common group is onsite but highly mobile workers. They typically spend their time in the same location, but don't sit too long at a desk. These jobs cover a diverse range of functions such as IT, healthcare providers, warehouse operations and public outreach.

Workers in such positions need persistent connectivity in a highly portable device, with a battery that will stay charged through the length of a shift. That's why a growing number of organizations, particularly in retail, hospitality and food service, are putting enterprise apps on tablets. Workers can then interact with people and apps, driving up both productivity and service.

Field workers such as onsite customer installation and service representatives,

delivery drivers, law enforcement officers, inspectors and case workers have device needs similar to those of mobile workers. But in addition to Wi-Fi connectivity, they also tend to need cellular service to transmit data from wherever they are, instantaneously.

Often they are capturing sensitive or personal data, so apps may need to be configured to not store data on the device. But at the same time, these users might need additional storage to handle local versions of codes, regulations and technical manuals. The choice of tablet or notebook will depend partly on the input requirements. Are these users checking off boxes in forms or filing detailed text reports, which would require a physical keyboard?

After establishing each worker's use case, the IT staff can then take the next step: choosing the right device and OS.

Device Categories

It wasn't all that long ago that computers came in two basic styles: clunky desktop and hefty portable. Desktop systems have evolved, but today's incredible variety of portable computing devices (with regularly dropping prices) means most workers have more than one.

Here is a quick overview of current mobile device options, categorized by screen size.

Smartphones

Although these are the smallest, smartphones in some ways sparked the mobile revolution. These are essentially pocket-size computers equipped with telecommunications. They typically have touch screens and either virtual or physical keyboards, and screens that measure up to 5 inches diagonally.

Most smartphones use a descendent of the original ARM reduced instruction set chip available from several manufacturers, and have solid-state storage of up to 128 gigabytes. They

are capable of running enterprise apps, but they are only productive if the app interface has been optimized for a small screen. Still, most workers who have to access data while on the move now have a smartphone in addition to one of the following.

Tablets

These ultraportable devices tend to use the same OS and chip architecture as their smartphone brand counterparts. It's worth noting that some manufacturers, such as Microsoft and Apple, have been converging their desktop and mobile OSs over time.

Tablets typically lack telephone capability because of their size, with screens in the 6- to 9-inch range, making them awkward to use as a phone held to the ear. But they can be equipped with Skype or similar apps for simple video conferencing exchanges, and most of the latest tablets have front-facing cameras for full-fledged video conferencing.

Tablets also have solid-state disk drives, with capacities of up to 256GB. Smartphones and tablets, with no more than a fourth of the storage capacity of standard notebooks with terabyte drives, are designed to work in conjunction with data center or cloud storage.

The largest smartphones, such as the Samsung Galaxy Note III with a 6.3-inch screen, are getting close in size to the smallest tablets, such as the Galaxy Tab with a 7.7-inch screen. Because they are functionally similar, it becomes a matter of user preference and use case whether to have one or both.

Hybrid PC-tablets

With touch screens, these "tweeners" come in several styles. Among them is the highly ruggedized Panasonic Toughbook, heavy but weatherproof and drop-proof, with stylus input capability. The Microsoft Surface

provides another approach. With its 10.6-inch screen and running Windows 8, the Surface comes in two tablet formats (one being lighter and thinner; the other being heavier, faster and thicker with more storage), which plug into a thin keyboard that doubles as a cover.

Netbooks

These mini-notebooks, from manufacturers such as Asus, HP and Lenovo, continue to hold their niche in the marketplace. At \$300 to \$500, they are low-cost devices designed for basic office productivity apps and email. Because these devices have conventional keyboards, use mice and have displays up to 11 inches, they can be ideal for teleworkers, office workers who travel occasionally or field workers.



Ultrabooks

These are full-size (11- to 15-inch) notebook PCs that are substantially lighter and thinner than standard notebooks. Apple pioneered the form factor with its MacBook Air, but now several manufacturers make ultrabooks.

They differ from standard notebooks in having a metal shell that's lighter but also more expensive to produce than plastic. The devices weigh between 2 and 4 pounds. They have fast processors, solid-state drives up to 256GB and battery life of up to 7 hours. Many feature long standby battery life (days or weeks as opposed to hours) for instant- or always-on use.

Ultrabooks are popular with traveling office workers because they are lightweight. They feature high-definition displays and often high-quality sound suitable for presentations without external speakers.

Notebooks

Notebook sales have exceeded desktop sales for some time now, since catching up with them in performance. Full-range suppliers such as HP and Lenovo offer machines with screens that measure up to 17 inches diagonally, with the fastest available processors and graphics accelerators, coupled with memory capacities of up to 16GB and rotating hard drives of up to 1TB.

Standard notebooks, although heavy (weighing as much as 6 pounds) compared with ultrabooks, are high performers that can handle pretty much any computing task. Some models have solid-state drives of up to 180GB.

Unlike ultrabooks, standard notebooks typically have built-in optical drives and multiple USB and other ports. Mainstream prices run from about \$350 to more than \$1,500. By comparison, ultrabooks can run up to \$2,000.

Features and Options

While screen size tends to define mobile device types, it also affects the suitability for various tasks. Many universal communication tasks work fine on the smallest of screens, including email, one-to-one video conferencing and messaging.

Productivity apps may run on smartphones, but it's not an effective experience. Tablets, with nearly full-size keyboards, are somewhat better, but the lack of mouse support can make navigating some documents tricky. On the other hand, tablets are practically ideal when it comes to form and data entry.

For example, office workers handling or creating PowerPoint, Excel or Word documents will benefit from larger screens (9 inches at a minimum) with a mouse and keyboard (or touchpad and keyboard). For those who work with engineering drawings, large maps, graphics or web design, the bigger the screen, the better.

Other factors to consider include the following:

Battery life: This feature varies, even on a single machine, depending on how it is used. It's most critical to field workers who may have difficulty accessing AC outlets. Consider training users in battery conservation

techniques and provisioning devices with available power-saving apps.

Bluetooth: This feature remains an important option for all types of workers so they can use wireless headsets and portable keyboards. It is becoming less important for printing as more organizations adopt mobile print solutions based on Wi-Fi and cellular connectivity through secure cloud services.

Built-in cameras: These devices have largely replaced the need for many field workers and office workers to carry a separate digital camera. Front-facing cameras, including those on notebooks and netbooks, are required in enterprises that use video conferencing as part of their UC mobility offerings. HD video capability is a nice-to-have feature for many office workers but could be critical for staff in the field who gather video for needs as diverse as processing insurance claims or analyzing crime scenes.

Browser quality: The differences between different browsers on mobile devices have narrowed. Browsers bundled with smartphones and tablets are optimized for each OS. So the choice might come down to which browser the organization's enterprise apps mainly use.

Connectivity options: Mobile devices have a variety of connectivity options, ranging from Wi-Fi only (which might be suitable for mobile workers on a campus) to 4G cellular. If office and field workers use high-bandwidth apps, 4G is a smart option now that the major carriers have rolled out this capability. No Ethernet

**MANY UNIVERSAL COMMUNICATION TASKS WORK
FINE ON THE SMALLEST OF SCREENS, INCLUDING EMAIL,
ONE-TO-ONE VIDEO CONFERENCING AND MESSAGING.**



adapters exist for iOS devices, although USB-to-Ethernet adapters may work for a few other brands. A simpler solution for office workers is to add a Wi-Fi device to their office LAN outlets.

Choosing a Carrier

Broadband coverage in the United States is continuously improving. But selecting a carrier is largely a matter of ensuring the organization has coverage wherever its workers roam. In practice, most enterprises use two or more carriers, both for coverage and for negotiating leverage. Simple though that may sound, carrier selection is anything but once the IT and network staff gets into the details of an organization's unique requirements.

Another selection criterion is whether the carrier offers devices that the organization wants to procure. Verizon and AT&T support iOS, Android, Windows and BlackBerry devices. In April 2013, T-Mobile added iPhones for the first time.

A third consideration is the network technology the carrier uses.

For international mobile travelers, devices using the Global System for Mobile (GSM) Communications will have an easier time in Europe. That's the technology AT&T and T-Mobile use. Verizon uses Code Division Multiple Access for its 3G network, as does Sprint. CDMA is also found in parts of Asia.

In the past year, Apple, Research In Motion and Samsung have introduced a fleet of new phones with 4G LTE technology. The benefits of 4G speeds accrue when transmitting video or other large files. It's still possible to acquire 3G smartphones, and some models include free plans.

But, it is important to note that not every user may need a smartphone. Very inexpensive phones can handle email, text messaging and photo gathering for workers who do not need mobile access to enterprise apps.

There are even specialized phone devices. For example, there are Motorola rugged phones with barcode readers, physical keyboards and SIM cards for conversion to international use.

Carriers offer much more flexibility in voice and data plans for businesses, government, education and other institutions than they do for individuals and very small businesses. This is why it's necessary to aggregate expected use of both voice and data, by department or workgroup, or for individual locations, before beginning negotiations. Once underway, the organization must monitor actual use so that it can adjust plans as needed.

Don't overlook bidirectional data in calculating data volumes either. Also, don't forget to consider services that users tend to use and that can also drive cost, namely text messaging and roaming charges.

Customer service should also figure into the selection. Large organizations can insist on specific, assigned individuals to help troubleshoot issues. The service-level agreement (SLA) should detail support specifics. ■



THE SECURITY DILEMMA

In the early days of bring your own device, when it was basically just an idea, many large organizations rejected BYOD programs out of hand because of security concerns associated with adopting consumer devices. The exception tended to be

BlackBerry devices because they had onboard email encryption and secure private networking for the transmission of email worldwide.

Now mobile device security is a matter of organizing the available security technologies and making sure they work in conjunction with one another. This implies restricting device choices to those that support such technologies.

Devices should be encryption-enabled and capable of compartmentalizing enterprise applications and data (to keep it separate from the user's personal contents) by using individual app containers or a secure folder for all organizational apps. An MDM program will let the IT department ensure that each user employs strong passwords, both to access the device itself and to tap enterprise apps.

It's important, however, to set security policies before instituting BYOD. These policies should prohibit jailbreaking or rooting and any other unsafe practices, such as use of consumer cloud backup for the organization's data and use of consumer data-sharing apps for the same data.

MANAGING RISK WITH MDM



33%
PERCENTAGE OF ORGANIZATIONS ENGAGING IN "BRING-YOUR-OWN-DEVICE" INITIATIVES THAT SAY THEY ARE NOT COMPLETELY CONFIDENT THEY ARE EFFECTIVELY MANAGING RISKS.

Source: 10 Lessons Learned From Early Adopters of Mobile Device Management Solutions, Forrester, September 2011
Reported by cmswire.com

In a 2011 IDC study, IT decision-makers report that, on average, 34 percent of their employees access applications from smartphones. But 69 percent of employees surveyed indicated that they use their smartphones for work-related activities. Why the discrepancy? The difference is likely because many employees are bringing their own devices to work, for work, whether it's formally permitted or not.

The issue is not so much whether a device is company issued or property of the employee – it's the fact that IT may be in the dark about who is using mobile devices to access company data. These portable devices can more easily be lost or stolen (relative to notebooks and especially desktops), can link into private networks and perhaps can even store sensitive information. Consequently, organizations need to manage devices, regardless of where they come from, and keep information out of the hands of the wrong user.

To get in front of this unmanaged access to corporate information and regain control of the mobile Wild West, more organizations are turning to mobile device management (MDM) solutions.

When evaluating a mobile device

management solution, you'll want to examine your existing resources, policies, compliance and security to see how a solution needs to fit in. You'll likely need one that provides quick, easy ways for employees to get access to applications. You'll have to figure out what kinds of analytics and reporting options you'll need. And that's just the start: there are many other factors to consider as you begin navigating your MDM options.

With all of the different variables, it can seem daunting to choose a right-fit solution for your unique needs. There's a sea of mobile device management vendors that approach the discipline in different ways. But you don't have to do it alone. CDW·G can help.

CDW·G has partnerships with the leaders in mobile device management. We'll assist you with selecting the best products for your ever-changing mobile needs. Based on our deep expertise in this solution area, our solution architects ask a series of questions that help uncover your MDM requirements. Whether you turn to us for an end-to-end services solution or just a little extra help choosing the right solution, you'll have experienced, knowledgeable professionals to support you the entire way.



AirWatch provides a complete Enterprise Mobility Management (EMM) solution. The solution enables you to quickly enroll devices in your environment, configure and update device settings over-the-air, securely distribute organizational content and resources and support personal devices accessing your network, email and apps.



The MobileIron Mobile IT platform secures and manages apps, docs and devices for global organizations. It supports both organization-liable and individual-liable devices, offering true multi-OS management across the leading mobile OS platforms. MobileIron is available as both an on-premises system through the MobileIron VSP and a cloud service through the MobileIron Connected Cloud.

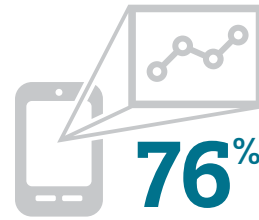


MaaS360 by Fiberlink simplifies mobile device management (MDM), mobile application management (MAM), and secure document sharing in the BYOD era. MaaS360 enables mobile policies that boost productivity, protect staff privacy, and secure sensitive data across smartphones, tablets and notebooks. Built on a highly scalable cloud architecture, MaaS360's on-demand mobility management can be deployed in minutes and seamlessly integrates with existing infrastructure, extending enterprise systems to a mobile environment.



CDWG.com/sap

SAP Afaria brings its device and application management solution to the cloud, providing a low-cost, high-returns model for deploying comprehensive enterprise mobile strategy. You will get the app management, multi-OS and BYOD flexibility that every organization needs without losing robust on-premises features such as no-touch application management, access to real-time analytics and centralized administration.



PERCENTAGE OF ORGANIZATIONS SURVEYED THAT ALLOW WORKERS TO USE PERSONAL MOBILE DEVICES FOR WORK RELATED TASKS.

Source: CDW IT Monitor, January 2012

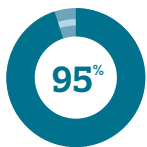
MOBILE DEVICE MANAGEMENT

It's easy to get overwhelmed when you're dealing with your organization's multiple mobile devices. That's why we offer you more than just the products. We offer you the people and the plan to turn them into real solutions. The breadth and depth of our product and service offerings are extensive. And with decades of experience, our solution architects can help develop a plan that's both manageable and practical.

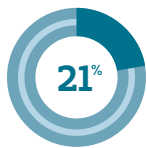


LEARN MORE ABOUT MOBILE DEVICE MANAGEMENT AT
CDWG.COM/MOBILITY

PROCURE AND PROVISION FROM ANY CARRIER



**95% OF
ORGANIZATIONS
ALLOW
STAFF-OWNED
SMARTPHONES
AND TABLETS.**



**ONLY 21% OF
ORGANIZATIONS
WILL INCREASE
INTERNAL STAFF
TO SUPPORT
MORE END-
USER DEVICES.**

Source: Cisco, IBSG Horizon Study, May 2012
Source: Building the Case for a BYOD Program,
Forrester Research, Inc, October 2012

CDW·G partners offer a wide variety of carrier agnostic technology options to ensure network access control, compliance, internal risk minimization, management and support. Our account managers and solution architects will help you pinpoint the roadmap for each vendor option, determining and prioritizing the right solution for your organization.

With the Mobility Management Portal, a cobranded procurement portal, you can manage all of the strategic and tactical components associated with a successful procurement and provisioning program. Our automated process allows your staff to order from a predefined catalog of mobile devices and accessories, perform upgrades or make changes to existing services – all in accordance with your governance policy.

The portal provides access to:

- Customized carrier inventory, contract terms
- Other procurement tools
- Preapproved ordering
- Carrier negotiated discounts
- Real-time order status, ticket histories
- Management reports

Selection: Depending on your organization's policy, employees can

select from a full scope of mobile devices ranging from smartphones to tablets to notebooks from any manufacturer.

Cross-Carrier Activation:

Activate devices with the carrier of your choice, and track expenses and usage consistently across each carrier and every usage plan.

Configuration: Configure user profiles, geofencing, time-based profiles, account access, applications and content on each and every device. Additionally, CDW·G will manage device kitting with company-specific literature for end users, as well as laser etching for company logos and personalization.

Deployment and Delivery: No matter how large or dispersed your organization, our deployment professionals ensure your mobile devices are carefully loaded, tested and delivered to the appropriate users as well as provide ongoing support upon deployment.

Your Trusted Advisor

With a dedicated account team and help desk, CDW·G offers a single point of accountability and support for all of your mobility needs. Contact your CDW·G account manager or visit CDWG.com/mobility to learn more.



Sprint mobility solutions integrate wireless into your enterprise communications, allowing complete productivity, tighter cost control and greater call redundancy and coverage. Your workers will be accessible and efficient, since their desk calls can be routed to their mobile phones, and you'll lower costs by reducing PRIs, minimizing trunks and eliminating desks for the highly mobile.



The business with the best technology rules.

Learn how Verizon Wireless provides powerful mobility communications solutions so you can maximize opportunities. Keep your team productive and their mobile devices connected at all times with an always-accessible shared Internet connection from Verizon Wireless. Contact your CDW•G Mobile Wireless Specialist for details, activation and support.

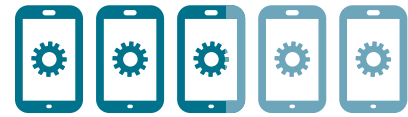


Mobility is transforming the way we work. Advances in wireless technology and smart devices are enabling organizations of every size to compress information latency and turn location-specific knowledge into an operational advantage. When enabled by affordable and reliable mobile solutions, organizations can improve performance in cost control, speed and process quality.

With a fast mobile broadband network and a wide variety of mobile devices and applications, AT&T can help you mobilize your organization and change the way you perform functions.



Keep your organization and workers connected with the latest in mobility technology and services from T-Mobile. With advanced smartphone products and T-Mobile's account management tools, staying on top of your work and your budget has never been easier. CDW•G offers T-Mobile's latest hardware products and can even handle activation.



64% OF ORGANIZATIONS ARE FOCUSED ON BOLSTERING MOBILITY SUPPORT FOR EMPLOYEES, PARTNERS AND CUSTOMERS.

Source: Benchmarking Your Enterprise Mobile Device Operations Initiatives and Plans, Forrester Research, Inc., October 2012.

PORTAL POWER


The CDW•G Mobility Management Portal and its related services are designed to be a custom administrative portal to help you manage security policies and compliance across your mobile user base. Featuring procurement and provisioning from any carrier, mobile expense management tools, and MDM and BYOD support, the portal creates a foundation for driving productivity and innovation through mobile applications.



THERE'S MORE TO CDW•G TOTAL MOBILITY MANAGEMENT THAN OUR PORTAL. LEARN MORE ABOUT WHAT WE HAVE TO OFFER AT CDWG.COM/MOBILITY

WE GET CONFIGURATION SERVICES

PRECONFIGURED I.T. SOLUTIONS SAVE YOU TIME AND MONEY



CDW
CONFIGURES
OVER
800,000
DEVICES
EVERY YEAR

No one likes to sacrifice productivity by taking talented in-house IT staff away from mission-critical projects to load software on new PCs, tweak systems to conform to network standards, or repackage defective equipment to return to the technology provider.

Instead, imagine being able to open your delivery and unwrap the "perfect" technology solution, already preconfigured to your exact specifications and ready to plug and play.

That's exactly what happens when you rely on our Configuration Services to help you build a preconfigured solution in our state-of-the-art, ISO 9001:2000-certified Configuration Center.

Fast, Accurate and Convenient

With CDW-G's configuration services, you get the right solution to fit your needs – right away. Our highly trained, industry-certified technicians build solutions to your exact specifications, quickly and accurately, without delaying shipment. In fact, we can usually install hardware and software, test the installation and ship your order the same day it is placed.

No downtime, no wasted resources and no need to hire outside consultants mean you save time and money – plus you enjoy faster deployment because your solution arrives fully loaded and ready to be installed.

A Full Spectrum of Configuration Services

CDW-G can partner with you to manage your IT implementation starting on day one and continuing throughout the lifecycle of your technology equipment. Our complete range of configuration services include:

- **Hardware Configuration** | We can install the key components you need: memory, hard drives, ROM drives, NIC cards, modems, video cards and other peripherals into your desktop PCs, notebooks, printers,

smartphones and mobile carts.

- **Software Configuration** | Simplify software deployment by having us install your operating system software and applications – and configure the settings to your exact requirements – all prior to shipping.
- **Custom Imaging** | We can preload your custom images onto your systems so that all personal settings, software and hardware are ready for deployment when the equipment arrives at your door.
- **Asset Management** | Keeping track of your IT infrastructure can be a difficult endeavor; our customized asset tagging makes it simple. We can label every piece of hardware with a unique asset number, which can be easily tracked online in your Account Center.

We Deliver the Right Configurations, Right to Your Door

Free up your IT resources – rely on us to make sure your new technology is ready to go when it arrives at your door. Ask your account manager how our Configuration Services can make life easier for you.



CDWG.com/asus

ASUS offers a broad portfolio of products that includes notebooks, mini notebooks, tablets, motherboards, graphics cards, displays, servers and workstations, multimedia, wireless solutions and networking devices.

Advanced ASUS design and engineering create extra-stylish and ultrathin artistic notebooks measuring under 1" in profile to deliver a balance of advanced and powerful features, premium materials, artistic designs and the greatest freedom of mobility.



CDWG.com/lenovo

Enter Lenovo. The Think brand is world-renowned for its security as well as reliability, durability, mobility and manageability. Lenovo has a full suite of products for all organizations. From notebooks and tablets with innovative touch screens for on-the-go professionals. For more information log on to cdwg.com/Lenovo TODAY.



CDWG.com/hp

From powerful and secure notebooks to convertible tablet PCs, HP offers a wide range of mobility solutions designed to keep organizations moving. Stay connected anywhere with HP's extensive wireless connectivity options and keep data secure using HP ProtectTools security software.



CDWG.com/samsung

Samsung notebooks are made to fit you and offer a wide range of mobility options to help meet all types of daily computing needs.

Samsung's notebook line offers the latest technology including Intel Core family processors and numerous configuration options. Samsung's netbook and tablet products offer an ultraportable option without sacrificing performance.



BY 2015, THERE WILL
BE AN ESTIMATED
15 BILLION
MOBILE DEVICES.

Source: Cisco, Visual Networking (Index Forecast), June 2012.

CDW CONFIGURATION CENTER – GREAT NEWS FOR I.T.

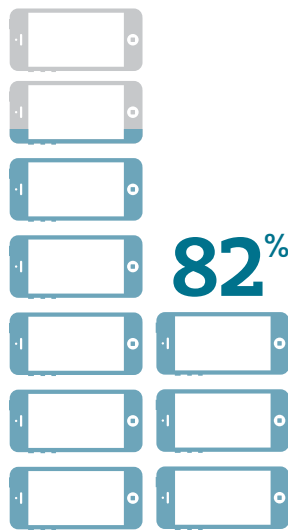
CDW's Configuration Center is one of the most advanced technology configuration centers in North America. With over 50,000 square feet of space in two cities, CDW, can customize, configure, install and implement technology products for just about every kind of network. So when you order from CDW, you get products configured the way you want them and ready to integrate into your enterprise, right out of the box.



LEARN MORE AT
CDWG.COM/CONFIGURATION

WE GET APPLICATION MANAGEMENT

INITIALIZE THE RIGHT PLAN



THE PERCENTAGE
OF INFORMATION
WORKERS WHO
CHOOSE THEIR OWN
SMARTPHONES
FOR WORK.

Source: Survey Staff's to Target Mobility Improvements,
Forrester Report, April 25, 2012

Managing a growing number of mobile devices – and the apps they contain – can be a daunting task. Today, workers are using their own phones to manage their work. That means you have to manage a variety of operating systems. And a growing number of mobile applications. In addition, you have to offer mobile end users applications like email, calendars and contacts, not to mention, collaboration and social apps. And now sales, CRM and HR apps have to be available too. Add these to the personal applications on your team's devices, and you'll find that keeping track of things can get a little hairy.

The good news is, there's an increasing number of sophisticated mobile management and security solutions that can help you keep tabs on your applications. Choosing the right solution can help deliver applications version control while providing purchasing storefronts and security.

Mobile Device Management (MDM)

MDM provides over-the-air configuration tools to help administer and control device settings. It also provides a real-time inventory of installed applications and security configuration. And, troubleshooting and intelligence enable staff to manage mobile

environments and remote control to take over devices and see what users see.

Mobile Application Management

MAM is a necessary component of an MDM solution. You should prepare for future mobile requirements by adopting technologies with strong application management and security features. An MAM solution can also allow you to create a secure container for organizational data and applications while sectioning off sensitive information from the rest of the device's operating system.

Enterprise App Stores

Many organizations are deploying enterprise application storefronts to provide team members with access to a user-specific catalogue of mobile applications. These internal app stores are managed by MDM software and provide a single point of distribution. These internal stores also allow for managing the distribution of different app versions based on specific department needs. Access controls tied to your organization's policies can simplify both application and content distribution.

Your CDW·G account manager and solution architects are ready to assist you with every phase of choosing and leveraging the right mobile solution for your IT environment.



BlackBerry Enterprise Service 10

Regulated-level Enterprise Mobility Management (EMM) control options are available for BlackBerry 10 smartphones to enable compliance for secure, government and regulated environments. Where a high degree of granular control over device features is required and for organizations where work-only use and application management policies are in place, BlackBerry 10 smartphones and BlackBerry Enterprise Service 10 combine to provide an outstanding device management solution for high-security mobility.



CDWG.com/sap

Meet the diverse challenges of enterprise mobility head on – with SAP Afaria. This scalable MDM and MAM solution is built on over 20 years of enterprise mobility experience – and can help you secure organizational data, control support costs, and automate ongoing tasks such as tracking assets, configuring apps and distributing data.



CDWG.com/trendmicro

With the growing popularity of high-end mobile devices, many workers are opting to use their consumer-grade personal devices – such as PCs, tablets and smartphones – in the workplace. Trend Micro suggests you embrace consumerization and securely manage your workforce without limits. Mobile Security is a fully integrated mobile device management and security solution within a security framework that spans physical and virtual, PC and non-PC devices. It protects data by enforcing the use of passwords, encrypting data and remotely wiping data from lost or stolen devices.

**76.9
BILLION
MOBILE APPS
ARE EXPECTED TO
BE DOWNLOADED
BY 2014.**



Source: IDC, The Application of Everything, 2010

MOBILE APP MANAGEMENT

Notebooks. Smartphones. Tablets. It seems like every day there are more and more mobile devices to keep track of. And with each of those devices comes a different operating system. Each using their own version of an application. So various users in various departments are using multiple versions of the same app. It sounds confusing because it is. You need a way to get a handle on the growing complexity. Putting a mobile application management solution in place can help you get control of your organization's various apps. It also enables a more collaborative and productive workforce.



**SEE HOW WE CAN HELP YOU
GET A HANDLE ON ALL OF IT AT
CDWG.COM/MOBILITY**

Acquiring Mobile Devices

Mobile Device Management

Expense and Telecom Management

Security and Mobile Devices

MANAGING THE MOBILE FLEET

IT departments need to apply a lifecycle approach to administering mobile devices, starting with procurement.



What enterprise resource planning became to logistics for large enterprise operations, mobile device management is becoming for effective enterprise mobility use.

Today, IT departments are deploying MDM programs to acquire, issue, provision and track users' devices. The first link in this management chain is acquiring the devices.

Acquiring Mobile Devices

Consumer demand has been the primary driver of mobile and portable computing device adoption in the workplace. Although manufacturers continue to market these devices mainly as consumer items, an organization doesn't have to acquire them that way.

The price tag for an individual device may be small and inexpensive relative to a desktop computer or large peripheral, but when acquiring them by the hundreds or thousands, mobile devices represent a substantial investment. More important, they are productivity tools in the hands of users and gateways

to critical information resources. Therefore, the IT team must execute mobile device procurement carefully and in a manner that allows secure device configuration and tracking.

Mobile Device Management

Choosing an MDM solution can present a bigger challenge than choosing the mobile devices themselves. As the mobility market has exploded, so has the sheer quantity of MDM software from both startups and established enterprise providers.

Basically, MDM maintains awareness of mobile devices and how they are being used. But more than that, it gives the IT department the capability of distributing software to devices and of disabling or wiping devices remotely should the need arise. MDM provides the operational manifestation of mobility policies, including those covering BYOD and cybersecurity. Most MDM packages provide the IT team access to a solution's functions through a web browser.

The MDM solution should cover the

DEVICE ACQUISITION FROM CDW·G

The major carriers offer enterprisewide, self-service device ordering by an organization's workers. CDW·G can go one step further and customize the acquisition process in ways that carriers may not be geared to do.

CDW·G, for example, offers comprehensive services for device procurement and lifecycle management. As it does for other computing resources, it will create an online procurement portal that covers multiple carriers, which simplifies administration for organizations.

By entrusting procurement portal operations to a third party, the enterprise's IT department can also be less concerned about nonstandard or special orders that typically require more time and resources.

Plus, this approach can also support BYOD programs. Users can log in to the portal regardless of whether they or the enterprise's is paying for the device. By having BYOD workers purchase their devices this way, both they and the organization benefit.

Workers can easily add options, such as extra memory, if they anticipate using apps or accessories that wouldn't ordinarily be supplied by the organization — just as if they walked into a carrier's store. The enterprise can maintain a chain of custody for ensuring security and access controls. Digital ID certificates can be properly loaded before devices actually get into users' hands.

The IT department should acquire organization-issued smartphones and tablets the same way it does desktops and other technology devices — that is, preburned with the enterprise software loaded, and affixed with an asset code. CDW·G can perform these and other services, such as etching devices with the customer's logo, at any of several secure, ISO 9000-compliant configuration centers.

mobility lifecycle, from provisioning through deactivation of devices, while controlling app distribution and security when devices are in use. Preferably, a single MDM solution can encompass the OSs for all devices used within an organization — Android, BlackBerry, iOS and Windows 8 at a minimum — as leading packages from AirWatch, MaaS360 and Citrix's new XenMobile do.

BYOD creates special MDM demands, and vendors have responded. Devices may come to the enterprise already containing a user's personal apps. The organization's BYOD policy must protect the individual's data and privacy, as well as the enterprise network and data.

To support BYOD, an MDM solution must, upon enrollment but before granting a device network login privileges, download the containerization app and other protective measures. The tools include

the ability to selectively wipe to remove enterprise (but not personal) data or the ability to disable memory cards.

The IT department may need to notify users that if the MDM agent detects any blacklisted apps, either the device won't be allowed or the app will be removed.

When licensing MDM solutions, there are two other basic decisions to be made: whether to go with a cloud or on-premises implementation, and whether to license on a per-user or per-device basis.

If the organization anticipates a great deal of customization or if total control is to remain in the IT department, then an on-premises setup may be preferred.

Cloud service might be the optimal approach for rapid deployment and fast scaling. AirWatch, for example, can handle more than 100,000 enterprise devices. The cloud option may also be more convenient for multiple-location organizations. MDM providers

typically offer multitenant cloud iterations in secure facilities.

Whether to go with per-user or per-device licensing depends on the number of devices the organization anticipates each user will carry. With a high percentage of office workers, more people are likely to have multiple devices, favoring a per-user arrangement. But with mobile and field workers, who are more likely to have a single tablet or ultrabook, a per-device license might be more economical.

Expense and Telecom Management

End-to-end management of a mobility solution would be incomplete without a clear and ongoing picture of telecom expenses: voice minutes, data usage and roaming. Plans vary, as do user behaviors. By actively monitoring and continuously adjusting service,

>

MUST-HAVE MDM FUNCTIONS

FUNCTION	WHAT IT DOES
Enrollment/ authentication	Enrollment of mobile devices and authentication using Active Directory or other credentials (MDM solutions often use a standard known as Simple Certificate Enrollment Protocol to issue digital certificates.)
App provisioning	Provision of devices with enterprise or departmental software apps, including email and other collaboration tools, along with configuration for functions such as contacts and calendaring
Security	Enforcement of security policies (See the sidebar <i>Why Jailbreaking Must Be Barred</i> later in this chapter for more information.)
Remote management access	Remote diagnosis of problems and the ability to find missing devices through geo-location services
General management	Privacy setting, software usage and license monitoring, as well as the maintenance of app whitelists and blacklists
Enterprise data	A dashboard providing enterprisewide usage data and audit reporting

an enterprise can maximize its return on telecommunications investments.

Comprehensive MDM packages include an expense management module, but there are also point products for the express purpose of tracking costs. A third option comes from the carriers themselves, who offer expense tracking and management as a service.

Because rates depend on volume, an organization will want to match a rate plan with each user's or user group's actual consumption. At the same time, managers will want to limit consumption to reasonable levels.

Expense management is best unified in a dashboard accessible by the IT team

and program and finance managers — basically, anyone who oversees expenses. Dashboards can ingest carrier invoices for examination, as well as analytics. An organization will want to be able to aggregate usage and expense data, and also drill down to individual devices if patterns indicate excessive or rogue usage.

Security and Mobile Devices

Security is an important issue, particularly when cybersecurity threats against organizations come increasingly from sophisticated groups who are pursuing theft of financial or intellectual property rather than making mischief.

Even so, with planning and proper use of available tools, the IT department can establish strong security for mobile workers and their devices.

It starts with understanding two principles. First, security efforts need to be directed more at data and enterprise apps than at devices themselves. Second, mobile devices require a different approach to security than do desktop systems on a LAN. Mobile devices tend to be always connected, must be reached wirelessly and need different configurations than their PC counterparts.

A fundamental first step is defining a policy regarding whether to store enterprise data on mobile devices. Many IT departments architect systems such that certain classes of data cannot be stored locally after being used by an app. Coupled with strong access controls, this approach ensures that if a device is lost or stolen, no unauthenticated user can easily gain access, even if app icons are visible on the device's screen.

But that alone doesn't equal a comprehensive security approach. Users' contact and calendar data, while less sensitive than other information that may be on the device temporarily, can also lead to problems if it falls into the wrong hands. Therefore, at the least, all device configurations should include lockout features. In some cases, it may be necessary to also enable iris or facial recognition as authentication mechanisms if the devices allow.

All devices with onboard encryption should have it enabled. Apple iOS and the newest versions of the Google Android OS rely on strong Advanced Encryption Standard techniques. For practical purposes, the AES algorithm is uncrackable, but devices are still vulnerable because of weak passwords and users' susceptibility to phishing attacks that ask for

EXPENSE MANAGEMENT FROM CDW·G

Some organizations choose to outsource expense administration to third parties. CDW·G offers this service as part of its mobility solution. Our experts focus on expenses – specifically, deciphering and interpreting trends in complex and highly detailed carrier invoices. The CDW·G team will pinpoint areas for savings, ranging from reining in users to negotiating lower rates for high-volume data or voice usage based on a particular group's needs.

personal or account information. Organizations' principal tools against such weaknesses are awareness campaigns and user training.

Another key security layer, besides on-device encryption, is the use of mobile virtual private networks. VPNs establish a trusted, encrypted data channel between device and enterprise core networks over the Internet.

First used mainly by field and mobile workers, mobile VPN software is finding its way onto the notebooks and mobile devices of office workers. Workers can use standard VPNs for remote login from a fixed location, whether wired or wireless. But mobile VPNs don't time out or disconnect if a user moves from one wireless network to another.

Consider two-factor authentication for users logging in via mobile VPNs (or any VPN, for that matter). The options for the second factor include biometrics (although biometric readers are more readily available for PCs than

for smartphones and tablets) and one-time, random passwords generated by a remote server and sent via text message or viewed within an app.

Finally, containerization is also critical and is becoming a de facto standard for protecting enterprise data on mobile devices. It's a way to isolate enterprise apps and data on a device from a user's personal material. The MDM solution can be configured to remotely erase selected data files while leaving personal data intact.

Containerization takes three basic forms:

- **Sandboxing:** An encrypted folder is created within a device's memory, into which the organization's apps and data fit.
- **App-wrapping:** Each app, along with associated data, receives its own encrypted zone.
- **Virtualization:** By installing a hypervisor on the device, all of the enterprise material is, in effect, combined into a logical second device.

Geo-fencing, yet another emerging security technique, disables apps or whole devices if they leave (or enter) defined locations. Geo-fencing relies on smart devices' built-in Global Positioning System programs. For example, a hotel chain might want to disable apps used for guest services once the user takes a tablet off the hotel property.

Mobile devices have demonstrated vulnerability to malware, and instances of mobile malware are rising rapidly. It may arrive via phishing email and texts, or through rogue apps or websites. QR codes also have become sources of malware. The major antivirus makers now offer specific mobility suites that include antivirus software for mobile OSs. These suites sometimes come bundled in deployment and monitoring packages that perform as security-oriented MDMs. ■



WHY JAILBREAKING MUST BE BARRED

Although hackers have figured out how to separate smartphones from their native networks, so-called jailbreaking (iOS) and rooting (Android) pose serious security threats. Any mobile security policy must disallow these actions.

The carrier associated with the phone is an integral part of the data exchange between the phone and the organization's network. Therefore, unauthorized switching of carriers could disable the ability of enterprise servers to identify and authenticate a device. It could also allow side-loading, which is the installation of unregistered or unlicensed software.

The leading MDM packages can detect jailbroken phones, wipe their contents and bar them from accessing the organization's network.

ALL ABOUT THE APPS

Enterprise applications are taking up a growing area of the mobile management dashboard.



The purpose of any computer, whether a smartphone or a supercomputer, is to run software.

Mobile devices and their stand-alone operating systems have brought a renewed focus to applications. Today, organizations need to think through their app choices.

For an end-to-end mobility solution, IT management must choose the apps that will be part of the enterprise bundle as well as those that will be used only by specific users or groups of users. That's why apps fall into two general categories:

- **Enterprisewide:** These apps are used universally: email, office productivity tools, web browsers, social media interfaces and collaboration tools such as SharePoint or Salesforce.com. Also, the organization may include utilities such as security, calendaring, contact lists and photo libraries.
- **Mission-specific:** These apps, commercial or custom-developed, serve a subset of users for a particular function, such as engineering or finance.

The choice of which apps to put on which devices depends mainly on the type of work to be done on each device. Office workers may need the full bundle so they can read (and perhaps edit) documents. Mobile workers, who might also have a cubicle and office somewhere, often can make do with the mission-specific apps in addition to the communication and collaboration programs. Field workers, in addition to their mission-specific apps, will likely need the collaboration apps and utilities.

The IT team can simplify administration and provisioning by creating a single enterprise image containing everything except the mission-specific apps. Each user would then choose from the app repository, with access based on role.

The need to develop custom apps for internal use has been decreasing rapidly as the major software makers continue to develop mobile versions of even complex software packages. For public-facing apps, not having mobile versions creates a distinct competitive

disadvantage for corporations and can reflect poorly on government and other public-serving organizations. For internal custom apps, not having a mobile version can limit the utility (and therefore the ROI) of a mobility solution.

But a mobile app should not be developed as a separate entity from the web app being replicated for customers' or constituents mobile devices. Instead, an organization should use an impending mobile rollout to modernize applications so they are endpoint-agnostic and optimized for the unpredictable performance of public networks outside of the organization's control.

Application Stores

Self-service has spread to so many spheres, it's almost hard to recall life before people booked their own travel or paid their water bills online. In enterprise life, workers routinely encounter self-service apps for human resources, financial and health benefits. And because nearly everyone is accustomed to downloading apps from popular online stores, many organizations are deploying branded app stores so that workers can self-provision their mobile devices.

Some MDM solution providers include app store modules, or an organization can use stand-alone tools to construct a store. The app store itself can work via the web on desktop and notebook systems or wirelessly on mobile devices. Users can download apps to their PCs and then add them to mobile devices when they next sync, or they can load them directly onto mobile devices wirelessly.

An enterprise app store should include a wide range of whitelisted companion apps that may also exist at consumer app stores. That will provide a convenience to users and help them avoid rogue apps, and it will ensure that the IT shop can log the apps on each worker's device.

But distinct differences exist between public and private app stores. An organization's store must

<i>MOBILE APP MANAGEMENT</i> FUNCTIONS	
FUNCTION	WHAT IT DOES
Wrapping	Secures third-party or in-house apps by wrapping them in individual logical containers that prevent data exfiltration or interaction with blacklisted or even other whitelisted apps
Delivery	Automates configuration, maintenance and updating, and maintains role-based app bundles for different types of workers who provision their own devices – in effect, orchestrating the pushing of apps to users once they log in and authenticate their devices
Store and remote management	Changes controls, removes and adds apps to the online library, and removes apps remotely from devices if the user has changed roles
Authentication and reporting	Controls downloads and users' individual app collections by authenticating users and devices, and generates reports on downloads and usage

keep track of software licenses, and it must limit downloading of some apps only to authorized users.

Managing licenses is critical so that the IT department can avoid underlicensing, which can expose the organization to payments and punitive fines from a license audit. A best practice, therefore,

is for the security or financial staff to conduct periodic audits of the in-house app store to ensure compliance with all licensing agreements.

How does an organization decide whether to establish a public-facing app store? Countless retail, transportation, nonprofit and educational organizations

>



DEVICE PROVISIONING FROM CDW·G

CDW·G can deliver devices with provisioning tailored to each worker. Users simply take the device from its box, do an initial login to enroll and download their identity certificates – and they are ready to go.

offer mobile apps from their websites, but far fewer make them available at places such as the Apple App Store or the Android Market. The decision depends on a combination of how many apps the organization offers and whether revenue from commercial apps will be enough to justify the infrastructure to support the store.

Mobile Application Management

An app store or download web page is only one component in an organization's mobile app management strategy. MAM is emerging as a separate category of software alongside MDM, although the major MDM vendors currently include MAM capabilities in their offerings. But MAM is gaining prominence as mobile use continues to grow, because organizations have begun to realize that app management is distinct from (even if highly similar to) device management.

Full-featured MAM solutions let an organization build an app store and equip it with device enrollment and certificate-issuing functions. The MAM also serves as the repository for app-use policies and as a mechanism for the IT department to maintain whitelists and blacklists.

Mobile apps have their own lifecycles, distinct from the devices they run on. MDM focuses on devices and their access to enterprise data; MAM focuses on internally developed apps being valuable intellectual property. Because each instance of a third-party app potentially represents a license, each download must be logged and registered with the organization's software asset management system.

In addition to securing and pushing apps to devices, most MAM programs also have a reach-back function to report on app usage, to fetch updates and apply them to apps, and to maintain configurations. MAM solutions also deliver analytics about whether and how individual workers use given apps.

Security and Apps

Safe mobility calls for a layered approach to security. To secure apps, the IT team first must make sure the devices themselves are handled securely.

An organization needs, at minimum, to take four actions should a device fall out of security compliance. The MDM solution should warn the administrator, send a message to the user with the action that must be taken, block the user's access to email or other enterprise apps until the situation is remedied, and if necessary, remove the organization's apps and data.

Plus, the IT department should have policies in place that enforce the use of strong passwords and device encryption.

Still, a number of threats can place apps at risk. All mobile apps to some degree – but especially

Android apps because of the multiple manufacturers of Android hardware – are susceptible to malware threats.

App infections may come in via mobile web browsers or links in phishing email and texts. They may come from apps downloaded from unauthorized sites. Occasionally, malware comes in by way of bugs exploited in the software controlling the baseband cellular communications processor on a device.

Mitigating these threats requires containerizing organizational apps or creating logical sandboxes on user devices and preventing cell-wall crossover of personal data.

Security best practices should also take into account the always-present threat of lost or stolen devices. Remote wiping of enterprise apps and data should be a first – and not last – resort. ■

HOW TO MANAGE MULTIPLE EMAIL ACCOUNTS

Most users have at least two email accounts, one for work and one for personal messaging. But many people have more than two. The security challenge becomes how to separate the organization's email, with its confidential attachments, from someone's Gmail or Internet service provider accounts.

Best practices for protecting enterprise email and its associated data include requiring device encryption before letting users access work email.

Here are three other steps to take:

- 1 Set the MAM program to prevent attachments from being opened in unauthorized apps or by apps outside the container or sandbox. Also establish the reverse condition: No personal email or attachments may be opened in secured, organizational apps.
- 2 Disable the ability to copy and paste among email accounts and to forward messages out of the enterprise account or into it from personal accounts.
- 3 Extend these restrictions to photos, links, files and attachments in workers' personal social media accounts.

THE NETWORK: CONNECTING ALL THE DOTS

Within the infrastructure, the rollout of an enterprise mobility solution requires a thorough review of network services.

The enterprise network supports all activities within an organization. After spending two decades building out and optimizing LANs and backhaul wired networks, IT staffs are turning serious attention to wireless LANs onsite and within buildings. The rise of mobile computing is driving WLAN investment, just as WLAN technology is gaining speed.

Assessment and Planning

Early enterprise WLANs were confined to conference rooms and visitor areas, mainly for the use of guests with Wi-Fi-equipped notebooks. Now, most users' devices have wireless receivers. Office workers are less cubicle-bound. And organizations serving the public directly have a twofold need for more wireless bandwidth. The public expects Wi-Fi, and more apps depend on roaming workers with wireless devices, typically tablets.

The result is a need for blanket coverage with sufficient bandwidth to accommodate all devices requiring

simultaneous access. In some situations, it's wise to deploy two WLANs, one for the organization's own use and one for public use. That's one way of ensuring needed quality of service for both as well as adequate security for enterprise data assets.

Mobility support means deployment of the 802.11n standard, with a path toward upgrading to 802.11ac (still to be finalized). The Wireless N standard tops out at a theoretical rate of 600 megabits per second, while 11ac tops out at 1 gigabit per second in multilink situations and many times that for a single link. So far, 802.11ac functionality is being slowly added to devices.

Before conducting a network site survey, the IT and network teams will need an idea of anticipated upload and download volumes, together with a clear idea of the application mix to be supported on the WLAN. For example, heavy streaming video or VoIP will require a harder network than one devoted mostly to email.



PLACEMENT OF ACCESS POINTS WILL DEPEND ON ANTENNA VECTORS AND THROW DISTANCE, AND ON THE AVAILABILITY OF ETHERNET CABLING AND POSSIBLY AC POWER.

The site survey should take into account physical barriers, such as kitchens or copy centers built in the middle of otherwise open floor space, as well as stairwells, alcoves, furniture and so forth. Placement of access points (APs) will depend on antenna vectors and throw distance, and on the availability of Ethernet cabling and possibly AC power. Assuming the location has at least first-generation Wi-Fi coverage already in place, the site survey should include a walkabout to measure current signal strength.

Organizations that have multiple buildings at a single location or buildings with courtyards, patios or plazas where people might work will need special attention. The IT team will have to set signal coverage to avoid bleeding into nearby public areas. Even on password-protected networks, best practice dictates not broadcasting AP existence but still ensuring seamless coverage for workers moving from location to

location in these types of environments.

Wireless equipment manufacturers such as Cisco Systems, along with third-party service providers, offer network planning and design services for their customers. This includes how to configure and integrate a controller so the IT shop can monitor what's going on within the WLAN infrastructure.

Controller-based Management and Monitoring

A wireless LAN controller lies between the wireless APs and the backbone network. It enables the network administrator to issue firmware and security updates to the APs and to monitor the performance of the WLAN. The controller enforces access and security policies with support for authentication processes and encryption.

There are two chief benefits of these specialized appliances. They ensure performance levels and availability of WLANs, and they simplify administration

of WLAN installations that tend to grow in complexity as they scale for an increasing number of users.

Controllers typically take the form of a 1U or 2U rack or stand-alone appliance that plugs into the main switch chassis. High-end, enterprise-grade controllers, such as the Cisco 8500, can handle up to 6,000 APs and 64,000 clients representing one large or hundreds of small WLANs. Smaller controllers also come in blade form factors for installation directly in a switch cage. Some organizations use multiple controllers, one each for data, multimedia and guest traffic.

Newer controller models are optimized for mobility — Brocade even calls its devices “mobility controllers.” WLAN controllers support multiple and simultaneous VPN sessions.

Features also include roaming from AP to AP without repeated reauthorization for a given user, which ensures fewer work interruptions. Newer controllers also provide plenty of headroom, with 10Gbps connections between the controller and the backplane or WAN links, which helps avoid degradation in WLAN traffic rates.

Controllers also monitor the APs, sensing if one fails and providing instant switchover to the nearest working one, while sending an alert to the controller web interface. Plus, they encompass location services that use third-party software to help the IT team keep track of mobile endpoints using 802.11 or radio frequency ID (RFID) technology.

A second type of WLAN controller is designed for branch offices. Under these circumstances, the local APs connect to a WAN link at the organization's data center via the controller. Should the WAN link fail, local WLAN traffic would continue.

Mobile VPNs

If an organization wants its mobile workers to be as productive as



TIPS FOR TRAFFIC OPTIMIZATION

Getting the most from a wireless LAN infrastructure starts with understanding the traffic on it. Some traffic, particularly streaming video, can quickly consume most of the bandwidth if not managed appropriately.

Besides sheer byte volume, it's also helpful to understand the nature of traffic directionality. For example, here are two typical patterns:

- Video surveillance has numerous endpoints gathering data and sending traffic to just a few others. Live digital playback is the opposite: a few servers transmitting to many endpoints. These are both multicast uses, but under different models.
- Desktop collaboration occurs under a many-to-many model, but usually at much smaller data volumes than video.

Different apps also have varying latency and packet-loss tolerances. High-definition telepresence is very sensitive among video apps, but video on demand is not as sensitive to these issues. Email, text messaging and data have higher tolerance for temporary glitches.

Most network switches support quality of service (QoS) by sensing the type of traffic in

use and giving higher priority to types that can't withstand latency. Therefore, adjusting for video QoS may cause slight delays in the delivery of other types of traffic.

But users are less likely to notice those delays than if their video appears jittery or keeps stopping and starting. Achieving optimum performance typically requires an iterative process of data analysis of apps and use patterns, followed by adjustments in the WLAN and policy settings, and then another round of testing and analysis.

IT departments can enhance throughput on 802.11n WLANs by using multiple-input, multiple-output technology. In some access points, MIMO requires auxiliary power beyond what is available over the Ethernet cable, but it raises the signal-to-noise ratio, leaving more bandwidth available for useful purposes.

Finally, don't overlook multimedia extensions to the Wi-Fi protocol that prioritize Voice over IP and video. However, when employing them, be sure to reserve some bandwidth for other apps under the “best-effort” delivery category.

possible, it must equip them with mobile VPNs. Because it is encrypted, the connection between the device and the network acts logically as a private link, even though it actually runs over the public Internet.

Mobile VPNs differ from fixed VPNs in that they remain open as the endpoint moves from network to network. The device (and the user operating it) can move among segments of a WLAN or between a WLAN and the cellular network. Remote or point-to-point VPN sessions terminate if the device moves out of range of the WLAN segment through which it made its initial connection.

Regular IP security (IPsec) and browser-based Secure Sockets Layer (SSL) VPNs that serve remote users well can't tolerate the constant changes in bandwidth that mobile devices encounter.

The distinction between "remote" and "mobile" is an important one to understand. In theory, a user in motion could use a standard VPN, but it would require constantly

reestablishing the tunnel connection and reauthentication, which is a drag on productivity and counter to the idea of true mobility. Along the same lines, a mobile VPN can remain in operation on a notebook PC even if the machine goes into sleep mode. This is important if a user needs to save battery power during a work interruption.

Some solutions combine IPsec, from which they derive the encryption capabilities, with a mobile VPN engineered to virtualize the IP addresses so they don't appear to change. This approach can be awkward.

A better choice is a purpose-built mobile VPN client. These work at Layer 4 of the network protocol stack, enabling them to enforce security at the application Layer 7 and the network Layer 3. The tech specifics can be a bit complicated, so it is worth the time to test mobile VPN client software in the organization's own environment.

Cloud and the Mobile Network

Organizations can look at how mobility and cloud computing interact in two ways. As described in Chapter 4, enterprise mobility management can itself be a cloud application. This approach eases scaling up of mobile deployments in part by doing away with separate management consoles for each type of device or OS.

But what about accessing cloud-hosted enterprise IT resources using mobile devices? Many organizations are using a combination of public and private clouds. In a typical setup, they may use public, multitenant clouds for noncore apps.

The solutions provider NetApp defines these apps, such as email, office productivity or order entry, as important but nondifferentiators for an organization. Some are inherently cloud apps, and manufacturers no longer offer shrink-wrapped or locally hosted versions.

The organization is more likely to host mission-critical apps or those that directly affect end users and constituents in private clouds — in their own data centers.

Access gateways, such as Citrix Access Gateway and Microsoft Forefront Unified Access Gateway, manage users' connections to remote resources. (The term *access gateway* can also refer to products that control communications among servers and storage.) They let the administrator set policies for remote and mobile access at the application level.

Security and the Network

No organization should be running any security protocol on its WLANs that predates the 256-bit Wi-Fi Protected Access 2 encryption standard. It's worth checking for old APs that might have been overlooked by previous updates and that use only the weaker Wired Equivalency Privacy standard.

Don't overlook teleworkers who use their home routers to access the organization's assets. They should hide their networks by turning off the identifier broadcast, changing the default identifier and making sure encryption is enabled.

For use of public Wi-Fi hotspots, which typically send warning messages that they are open and unencrypted, use the MDM program to verify that workers' mobile devices default to encryption mode and use of VPNs when in these areas.

While it can be discussed at many levels, managing network security is often a matter of layering in the basics:

- Ensure all endpoints have the latest OS versions and patches.
- Use the newest encryption standards on APs and enforce strong passwords.
- Use endpoint antivirus tools.
- Maintain firewalls so that they are loaded with the latest threat signatures. ■



WEBINAR IS YOUR NETWORK BYOD READY?

View this webinar that focuses on the ideal solutions for integrating and securing mobile devices on the network:

CDWG.com/mobilityguide1

PROVIDING A HELPING HAND

Along with hardware and software considerations, organizations embracing mobility must also think through support implications.



Mobile devices ultimately are computers, and all computers and software have support needs.

These devices have characteristics that require the specialized expertise of the tech team, and possibly specialized training and support for users.

Therefore, to help ensure the success of a mobility rollout or an update to mobile services, the IT team should include planning for support from the beginning.

Help Desk Options

Any new device rollout will incur an initial increase in help desk calls or trouble tickets. Users might have concerns or issues when setting preferences on the devices, for instance, or when syncing them with desktop or enterprise services. Some users might be unfamiliar with touch-screen devices or with the mobile versions of enterprise apps.

For some organizations, the support requirements are a chief reason they opt for a BYOD program: Users are likely to be familiar with devices

they have purchased and set up to meet their personal preferences.

Even so, based on the established mobile policy, the IT team will need to be prepared to meet users' needs and provide the expected support.

Given the broad adoption of mobile computing, wireless infrastructure providers such as Cisco Systems offer certification for supporting wireless technologies.

In addition to preparing the support team, providing intuitive self-help will minimize help desk calls. Available apps can provide help through FAQ documents and access to users of the same devices or apps. Detailed online walkthroughs of how to set up and provision devices can also minimize the number of people who need to escalate support to a trouble ticket or phone call.

For app support, an organization can establish a two-pronged strategy. First, it can provide tutorials and other self-help options for common commercial apps that have been made available through an internal app store.

That way, the organization can devote more IT resources to the support of enterprise and mission-critical apps, whether commercial or customized.

Clearly, a key question then becomes whether to use staff for help desk services or to outsource that requirement.

Using staff lets the organization choose its own people. But it's also easy to underestimate the added load that a mobility deployment can create for the IT staff, given devices that may be unfamiliar, the burgeoning number of apps and the wireless mesh infrastructure that also requires monitoring and repair.

Outsourcing can be more economical because of the economies of scale the enterprise can leverage through a service provider. By fashioning an SLA that covers products and expected response times, the IT staff will not be adversely affected should support demands spike.

The more sophisticated third-party providers use data analytics based on their experience with a wide range of devices and apps. By monitoring the organization's mobile services and comparing that against its data, the provider can quickly resolve problems as they arise, as well as make adjustments on the fly and notify the organization about the need for possible changes before a service hiccup occurs.

Warranty Services

Manufacturers offer standard warranties on mobile devices that generally run from 90 days to 12 months, depending on the device and the manufacturer. Standard phone support plans also vary, but generally run as long as the parts and labor warranties.

MDM Customization Services

Once the IT team has decided whether to host an MDM system on

WARRANTY SUPPORT FROM CDW·G

It's possible to offload the administrative headaches of device return, provisioning of replacements and getting devices back into users' hands. CDW·G, under its Total Mobility Management services, can manage standard warranties for whatever devices an organization issues. In addition, these services can be augmented with options such as 24-hour emergency device replacement.

premises or use a cloud service, it also must decide whether its tech staff will run the program or whether to have a third party remotely manage the MDM service.

The size of (and demands on) the IT team will be a factor. Considering the amount of configuration and monitoring involved with MDM, it might prove beneficial to take the managed services route.

MDM as a managed service includes configuration of security and wireless access policies; setting, issuing and tracking security certificates; and creating individual and group profiles.

It's difficult to separate operational control of the MDM from other provisioning services and policy management because these are embodied in the MDM setup. Plus, the parameters constantly change to meet evolving operational requirements. By engaging a vendor to manage acquisition, provisioning and troubleshooting, an organization can streamline mobility deployment and lifecycle support.

The MDM solution's delivery services can also include app and related update pushes to devices from the organization's secure portal. These MAM configurations, a subset of MDM, are set to ensure each user's device receives the correct collection of apps according to the established user or group profile.

To be complete, an MDM system

must have the capability of extending services to BYOD systems. When users enroll their devices, they invoke policies according to the MDM settings. In that way, the devices' security features and other configurations are visible to the IT team through the MDM interface. ■

REMOTELY MANAGED MDM: CDW·G AT YOUR SERVICE

As part of CDW·G's Total Mobility Management services, organizations can opt for remotely managed mobile device management services.

CDW·G works directly with multiple partners who provide MDM solutions as well as with a wide range of carriers, alleviating the day-to-day mobile administrative burdens on an organization's IT department.

Some of the services offered include:

- Self-service procurement portal
- Help desk and remote MDM support
- Expense management

Visit CDWG.com/mobility for more information on our remotely managed MDM solutions

Disclaimer

The terms and conditions of product sales are limited to those contained on CDW-G's website at CDWG.com. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given.

For all products, services and offers, CDW-G® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. CDW®, CDW-G® and The Right Technology. Right Away.® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. CDW and the Circle of Service logo are registered trademarks of CDW LLC. Intel Trademark Acknowledgement: Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Ultrabook, Viiv Inside, vPro Inside, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. Intel's processor ratings are not a measure of system performance. For more information please see www.intel.com/go/rating. AMD Trademark Acknowledgement: AMD, the AMD Arrow, AMD Opteron, AMD Phenom, AMD Athlon, AMD Turion, AMD Sempron, AMD Geode, Cool'n' Quiet and PowerNow! and combinations thereof are trademarks of Advanced Micro Devices, Inc. HP Smart Buy savings reflected in advertised price. Savings may vary based on channel and/or direct standard pricing. Available as open market purchases only. Call your CDW-G account manager for details. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a \$250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding mobile solutions. CDW-G makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding mobile solutions. Furthermore, CDW-G assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication. The content contained in this publication represents the views of the authors and not necessarily those of the publisher.

©2013 CDW Government LLC
All rights reserved.



Index

App categories.....	26-27	Mobile device management (MDM).....	4, 9, 13, 22-25, 27, 28, 32, 34
Application portal/store.....	6, 23, 34	Mobility roadmap.....	5
Bring your own device (BYOD)	4-5, 8, 13, 22-23, 33-34	Netbooks.....	11
Carrier choice.....	13	Network strategy.....	8-9
Cloud computing.....	5, 11, 12, 13, 23, 32	Notebooks.....	12
Containerization.....	5, 7, 9, 23, 25	Security, app.....	28
Data access policy.....	7-8	Security, mobile.....	4-5, 9, 13, 24-25
Device acquisition	22-23	Security, network.....	32
Device features.....	12-13	Security policy	9
Device policies.....	8	Smartphones	11
Device user categories	10-11	Tablets	11
Expense management.....	23-24, 25	Traffic optimization.....	31
Geo-fencing.....	8, 25	Two-factor authentication	9, 25
Help desk.....	5, 33-34	Ultrabooks.....	12
Hybrid PC-tablets.....	11	Virtual private network (VPN), mobile.....	9, 25, 31-32
Jailbreaking	9, 13, 24, 25	Wireless assessment/planning.....	29-30
Mobile application management (MAM).....	6, 28, 34	Wireless LAN (WLAN)	29-32
		WLAN controller.....	30-31

ABOUT THE CONTRIBUTORS



JASON BROWN is the Technical Field Mobility Solution Architect for CDW, helping inform customers about the ever-changing mobility landscape. He works closely with a team of internal and field solution architects, assessing customer needs in all aspects of the mobility workplace. With over 18 years of technical experience, he brings a wealth of knowledge to the team, researching mobility updates from CDW vendor partners and helping provide successful solutions for education, healthcare, government and small, medium and large enterprise environments.



STEPHANIE SULT is a Mobility Solution Architect with CDW, specializing in the healthcare industry. In her role, Sult develops and implements comprehensive enterprise mobility solutions for CDW's healthcare customers. She specializes in enterprise mobile management, mobile device management, carrier activation services, telecom expense management and mobility IT help desk services. Sult holds a bachelor's degree in business administration from Saint Mary's College (Ind.) and currently resides in Chicago.

LOOK INSIDE FOR MORE INFORMATION ON:

- Building out a holistic mobile strategy
- Purchasing the right devices for workers' job needs
- Fine-tuning MDM to better meet organizational needs
- Getting a handle on app management



SCAN THIS!

Check out the CDW Technoliner and find out when this tricked-out tech experience is coming to your city.

