WHITE PAPER

CDW PEOPLE WHO GET IT™

MANAGING MOBILITY FOR THE ENTERPRISE

The right EMM solution brings control over devices, apps, content and identity.

EXECUTIVE SUMMARY

The number of mobile devices managed by enterprises increased 72 percent from 2014 to 2015. This onslaught of technology such as notebooks, smartphones, tablets, watches and gadgets has transformed the way users work.

These devices provide users in just about every sector with access to the information and tools they need to do their jobs, wherever and whenever they need them. They're free to work at their desks, in conference rooms, while visiting clients on the road or during a child's baseball practice. They can input data directly into a medical chart, an order form or an inspection report, rather than doubling their work by transcribing handwritten notes later in the day.

But the growth in mobile devices at work also presents challenges for organizations. IT administrators can't just open the floodgates to all users and all devices. In order to maintain network uptime, quality and security, enterprises need advanced tools to manage their corporate-owned and bring-your-own-device (BYOD) mobility programs. As mobility continues to grow and the line between personal and business devices blurs, many organizations are turning to a holistic approach that combines the management of mobile devices, applications and content. This approach is known as enterprise mobility management (EMM).

The Evolution of MDM to EMM

Enterprise mobility management builds on the capabilities offered by mobile device management (MDM) solutions.

Before the days of smartphones and tablets, IT departments had full control of the authorized devices that connected to enterprise networks. They set policies for which types of computers could be used in the workplace, how they could connect to the network and what types of protections they needed to remain secure.

That control was upended by the mobile revolution. Enterprise devices were connecting to the network alongside the personal devices of users and visitors. Different types of devices — tablets, smartphones and notebooks — ran a hodgepodge of operating systems, and they presented varying degrees of security. While users loved the new capabilities their smartphones and tablets offered, this change created a nightmare for IT staff to manage.

105.4 million

The projected size of the U.S. mobile workforce in 2020 — equal to 72.3 percent of the total U.S. workforce — up from **96.2 million** in 2015*

MDM brought calm to the chaos. With MDM software, IT departments were able to monitor and secure devices, whether they were organization- or user-owned. They could establish policies, such as requiring passwords, that users had to comply with before connecting devices to the network. They could encrypt devices, and if one was lost or stolen, MDM software gave administrators the ability to manage it remotely, including locking it or erasing its content.

Today, MDM is nearly as ubiquitous in offices as copiers and coffee machines. But as the mobile revolution has continued to evolve, organizations have learned that it's not enough.

Mobile devices today are as indispensable in users' personal lives as they are in the workplace. They're just as likely to use them to text with friends about weekend plans as they are to schedule conference calls with colleagues. The anytime, anywhere capability of mobile devices has blurred the lines between work and home. Rather than stay late at the office to finish a project, a user can go home, have dinner, then stretch out on the couch with a tablet and wrap it up.

Considering the convergence of personal and professional lives, it made sense that users would employ the same devices at work as they did at home. It simplified matters for users and, in many cases, boosted their productivity. But it introduced new challenges for the IT team.

The initial response to users bringing their personal devices to work was to establish BYOD policies. BYOD can cut down on equipment costs because users already own the devices. And it gives them access to enterprise data and workloads on devices they're comfortable using, which can boost their satisfaction and productivity.

But along with the pros of BYOD came several cons. The wide assortment of devices, operating systems, applications and security controls strained IT departments, which had to figure out how to keep track of, maintain and secure all these new devices on the network. And what happens to enterprise applications and data on personal devices when users leave the organization?

Another problem arose. While IT departments were charged with keeping their networks secure, it became hard to justify requiring complete control of devices that the enterprise didn't own. Besides, it's not the devices themselves that an IT department is trying to protect — it's the content on the devices that's valuable.

In some cases, such as with contractors or board members, IT administrators can't have any control over devices, even though the devices can be used to access enterprise data. So organizations began to rethink their mobile strategies. Rather than taking a solely device-centric approach, it made sense to build a mobile strategy around protecting content, as well as the applications that access that content.

Leading EMM solutions, such as AirWatch, MobileIron and MaaS360, reflect those evolving needs by offering both mobile application management and mobile content management capabilities.

Mobile Application Management

MAM solutions can help administrators control which applications to make available to employees, how they're licensed and delivered, and what policies govern their usage. With MAM, users can employ their personal devices the way they choose, but give IT administrators control over the applications they use for work.

MAM begins with the distribution of applications. Organizations can push out apps to users, or establish their own app stores and stock them with applications that users need to do their work. The applications can be made available through role-based access, which permits users to download only those apps appropriate for their specific jobs.

Either distribution strategy makes it easy to track which applications are used and to manage licenses. License management is particularly important at companies with BYOD or corporate-owned, personally enabled device policies, because users can't take those apps (and the corporate data on them) when they leave the company. The licenses stay with the enterprise, which can deactivate apps and transfer their licenses to other users if needed.

MAM can also secure the applications that access enterprise data without restricting users from their personal apps. A MAM solution can apply updates and patches to applications, keeping them protected from vulnerabilities, and can create application whitelists and blacklists. Administrators can limit enterprise data only to applications that are licensed to the organization, so that users aren't accessing sensitive information via unsecured applications.

***SOURCE:** IDC, "IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020," June 2015

IT departments can also use MAM to track which applications are downloaded and to compile usage statistics to fuel future purchase decisions. Usage statistics can also indicate the need for additional training in certain applications.

Mobile Content Management

MCM adds another layer of control over mobile deployments. While MDM focuses on the device and MAM provides protection at the application level, MCM controls the very data that organizations work so hard to protect. It offers users a secure way to access and share content.

Containerization creates a separate space on a device where users can securely work with content and specific applications. Containerization authenticates users before they access the material in them, and it encrypts data in transit and at rest.

As more users employ their smartphones and tablets to work, it may be tempting for them to use file sharing, email or other apps that aren't secure. This could pose a threat if they use these apps to access enterprise data. So while they may still choose to use those apps for personal tasks, organizations can set up containers that house approved apps with settings and policies configured by IT administrators.

MCM is an important tool to guard against data loss. As with MAM, it can enable administrators to limit certain actions, such as copying, pasting or printing sensitive data. MCM can also be used for geofencing, which relies on a mobile device's GPS capabilities to establish a geographic boundary within which the device must remain while an app is running. If the device goes outside this boundary, a predetermined action is automatically taken. For example, if a truck driver ventures outside his or her prescribed route, the routing app may send an alert to a dispatcher.

In addition to mobile device, application and content management, organizations may benefit from several other useful features of enterprise mobility management, including:

- **Cloud delivery**, allowing enterprises to roll out solutions quickly without costly infrastructure and to scale solutions up or down as needed
- **Unified management consoles**, which provide administrators with centralized management of all the devices, applications, content and users on a network
- **Identity/authentication tools** to ensure that users are who they claim to be
- **Single sign-on**, simplifying mobility for users by allowing them to use the same login credentials to access various devices and content
- **Security reporting**, helping the IT group monitor the network for threats and vulnerabilities
- **Encryption of data at rest and in transit**, which keeps it protected in case a device or data is compromised
- **Automatic device configuration**, enabling workers to access resources quickly and easily
- **Integration with back-end systems**, so mobile devices give users access to the resources they need

The Growing Importance of Apps and the Data Behind Them

As organizations have shifted from MDM to EMM, many are realizing that the devices themselves aren't the most important factor in the mobility equation. IT departments can password-protect devices, equip them with VPNs and encrypt their contents, but it all boils down to one goal: managing the data on them.

That's why applications are so critical to an effective mobile deployment. They access, organize and secure data — the way these apps are chosen, configured and managed can make or break a mobility plan. Organizations, therefore, need to give careful analysis to the apps they use as they adopt an EMM approach.

Supporting BYOD

When the Indiana University of Pennsylvania sought to support a bring-your-own-device initiative for 14,500 students, it began using AirWatch by VMware for basic mobile device management functions.

"The AirWatch tool lets us remotely wipe lost or stolen devices and push VPN settings to the devices. It was very straightforward to set up and met our needs," says Ben Dadson, IT coordinator of desktop services for the university.

The university also uses the solution to push academic applications out to tablets that it provides to students for temporary use in classrooms. For example, one student may use a tablet to interact with an app for a history class, then return the device so it can be used in the next class by literature students. The university is looking into extending this capability so students can load academic applications onto their personal devices.

IUP also uses AirWatch's Secure Content Locker feature, which protects local data and user content stored on mobile devices.

There's an app for everything. Apps can track expenses, schedule appointments, create newsletters, slay zombies and repel mosquitoes. While email is the most widely used app, developers have created myriad tools to help users do their jobs. Between Apple's App Store and Google Play, millions of apps are available to users, and they're downloaded by the billions.

Regardless of the type of device — be it a smartphone or tablet, Apple-, Android- or Windows-based — scores of apps can perform any number of valuable functions. They can help users communicate via email, voice, video or text. They can scan, share and store documents and photos. They can capture information, create presentations and analyze data. Apps serve as a bottomless tool chest for workers wherever they go.

The utility of mobile applications underscores why a well-crafted app-deployment strategy is essential to any mobile deployment. Organizations have a variety of application options, including:

Off-the-shelf: Millions of off-the-shelf (OTS) apps are available for all types of devices and operating systems, and many are geared toward work-related functions. Organizations have what seems to be a limitless supply of apps for email, secure messaging, databases, note taking, project management, scheduling, document scanning and so on. Competing OTS apps offer different features, so enterprises looking for apps that perform common tasks are likely to find what they need on the OTS market. If this is the case, OTS apps make sense because they're faster and easier to deploy, and they're often relatively inexpensive. There are cases, however, when organizations can't meet their specific needs with OTS apps.

Custom: When organizations are looking for apps that perform unique or mission-specific functions, they may need to develop their own. Some enterprises may need an app that fulfills a specific purpose and may not be able to compromise on some details for the sake of convenience. Custom mobile apps, however, tend to be more expensive than OTS apps. They also can be complex to design and often take longer to deploy. An enterprise looking to deploy custom apps should work with a developer with specific expertise in designing apps for smartphones, tablets or other devices.

Partially customizable: In the middle ground between OTS and custom apps reside platform apps that allow for some customization. They tend to cost less and are faster and easier to deploy, and they also deliver some control over functionality. For instance, many database and form-building apps can be customized. In fact, Apple and IBM together offer a series of apps, called IBM MobileFirst for iOS, that are customizable for specific industries.

Virtualized applications: Instead of creating apps that are downloaded onto a device, organizations can opt to virtualize apps. App virtualization is the process of virtually reproducing specific apps so that they run locally on a client device but are not actually installed on the device in the traditional sense. Rather, the app and its associated data are encapsulated in a package that is separate from a device's operating system. This decoupling from the operating system allows cross-platform operability, and can also improve security. However, some apps (such as those that require a device driver) cannot be virtualized, and others (such as those requiring heavy integration with a specific operating system) are difficult to virtualize.

To learn more about how to build and deliver the right applications for users, read the CDW Technology Insights Guide "Mobile Apps: Enhancing Productivity."

1.5 million

The number of apps available in Apple's App Store*

1.6 million

The number of apps available in Google Play store**

Cloud: Like virtualized apps, cloud apps are not stored locally on mobile devices. Rather, they are accessed online via a user interface. Because cloud apps work on any type of device, an organization with a BYOD policy may find it easier to deploy a cloud app as opposed to several versions of a native app. However, although this can save time and money on app development and management, native apps often have greater functionality. This is because they can access other features on a device, such as a camera, without relying on an application programming interface. Another disadvantage of cloud apps is that they can't be accessed without an Internet connection.

Each of these application options has advantages and disadvantages. Enterprises must determine what their goals are with apps and how they'll use them before deciding which approach to take. CDW can help an organization determine which approach best meets its needs and guide it through app deployment. The CDW white paper "The App Roadmap: Mobile App Strategy for the Workplace" has more information on deploying apps strategically.

How Organizations Can Manage Their Application Ecosystems

Deciding which types of apps to make available to users is the first of many steps toward building a strong mobility ecosystem. Organizations must also determine how to distribute, manage and secure these apps. Mobile application management, which has become an essential solution for many organizations, can help.

Using MAM, administrators can create and enforce policies and security procedures regarding application distribution. They can control app availability and features based on users' roles, whether they're managers, support staff, contractors or suppliers.

***SOURCE:** Apple, July 2015

****SOURCE:** Google, July 2015

One strategy for protecting enterprise mobile applications is app wrapping, which applies a management layer to custom apps, allowing administrators to configure user privileges and settings within applications. With app wrapping, administrators can also:

- Require apps to access the enterprise systems via a virtual private network
- Enable single sign-on for different applications
- Set multifactor authentication, requiring factors such as a password, personal information number or thumbprint to access applications
- Detect compromised devices or applications and deny them access to the network
- Protect against data loss by blocking certain features within apps, such as copying, pasting, emailing, backing up to cloud services or printing

10

The average number of enterprise mobile apps that organizations plan to deploy in the next two years*

Another important step in application management is to create an enterprise app store. This provides users with a self-service option for selecting tools that will help them do their jobs better, which generally improves user satisfaction, and it also gives IT departments control over the apps from which users can choose. This means IT staff are not required to support a limitless number of apps. And it also ensures that users will employ beneficial, secure apps that are likely to boost productivity and effectiveness, without introducing security vulnerabilities.

When it comes to app stores, enterprises have two options. The first is a private-branded enterprise app store. Organizations can build their own stores or purchase an enterprise app store solution from a vendor such as IBM or Citrix. Many times, an app store is included within a larger EMM solution. Enterprise app stores can be hosted onsite or through a cloud provider.

These stores are beneficial because they give IT departments a comprehensive solution to control access to apps, distribute them, track their usage and distribute updates and patches.

The offerings in an enterprise app store can be custom apps developed by the organization or off-the-shelf apps available publicly. Unlike public app stores, they can even house apps for different operating systems, providing a one-stop shop for iOS and Android users.

For organizations that don't have the resources or the desire to create their own app store, a second option is to deliver managed apps through a public store. Apple's App Store offers a Volume Purchasing Program, and Google Play allows enterprises to set up private channels. These options let organizations purchase apps and assign them to users through a managed solution. IT administrators can create role-based access, authenticate users, manage the apps purchased through a store and reassign apps to other users if needed.

Regardless of which approach organizations take, CDW can help. They can work with you to devise application management strategies, including selecting the apps that will be most useful to employees, developing apps, determining how best to manage and secure them, setting up enterprise app stores or managed app programs, or selecting the right third-party solutions to meet organizational needs.

Centralized Management

One of the biggest challenges organizations faced when mobility first emerged was the Wild West atmosphere it created. Users would connect notebooks, smartphones and tablets with iOS, Android and Windows operating systems to enterprise networks. Some password-protected their devices; others didn't. Some had carefully curated app libraries, others downloaded apps willy-nilly.

IT departments that always had complete control over the devices that connected to their networks had no idea

Hitting the Streets

The city of Philadelphia improved field workers' ability to collect data by issuing them smartphones to replace inefficient clipboard and paper methods.

Users for the city's Community Life Improvement Program carry Samsung Galaxy Tab phablets (a hybrid smartphone/tablet) for real-time access to work order data. Philadelphia IT staff deployed the IBM/Fiberlink MaaS360 MDM solution to improve the city's ability to control the devices.

"The users don't have access to the web browser," says Francisco Galarza, senior solution architect for the city. "We don't want the device to become a distraction — the goal was to make it as easy as possible for the fieldworkers to use."

The MaaS360 solution allows IT administrators to wipe lost or stolen devices, as well as push out applications and update apps remotely. For additional security, the city uses MaaS360 to create a white list of the apps city workers can run.

***SOURCE:** 451 Research, "2015 Enterprise Mobile Application Report," June 2015 what to expect. They didn't know if devices would introduce vulnerabilities onto the network. They didn't know how many users were connecting, what they were doing or how much bandwidth they would need.

EMM has brought order to mobility. Using a central console, administrators can see exactly what's happening on their networks. They can control which devices connect to the network, which apps they use and what content they can access.

EMM consoles can quickly and easily enroll new or reconfigured devices and manage a variety of operating systems, including Android, iOS, BlackBerry and Windows Mobile. Some can even manage desktops. This can save a tremendous amount of time and effort for IT staff, who had to manage those tools separately in the past.

EMM central management consoles, which often have simple interfaces, can even be accessed remotely, allowing administrators to update device settings and policies. They can, for instance, create different groups within an organization and set policies appropriate for those groups.

The console can be hosted either on-premises or in the cloud. Several managed service providers offer cloud-based EMM tools. Turning to a cloud-based vendor not only keeps enterprises from starting their mobility deployments from scratch, but it also enables them to expand their toolkits as needed because of the scalability of the solutions. Some service providers, such as CDW, can even manage the cloud EMM deployment, removing these responsibilities from in-house IT staff and allowing them to focus on enterprise initiatives.

Another advantage of the cloud is that it saves organizations the expense of laying the infrastructure needed to deploy mobility management solutions. Instead, they can purchase a cloud-based service, which reduces costs and moves payment from a capital to an operational expense.

➔ ***To learn how a comprehensive policy can help organizations get the most out of mobile technologies, read the CDW white paper "Building an Effective Mobile Policy."***

Administrators can configure a management console to keep them apprised of what's happening on the network. They can set up alerts for any violations of mobile policies or regulations. They can also get real-time updates of network and device activity.

EMM solutions include preconfigured reports that pull data and analytics from the system to enable real-time reporting and detailed auditing. For instance, administrators can run reports on the cost of devices by user, call usage by organizational group, or application analytics by date.

The Importance of Identity

One of the biggest challenges of any mobility deployment is striking a balance between giving users easy access to the resources they need and keeping mobile devices — as well as the content on them — secure.

This has always been a conflict for IT departments. But as more users employ more types of devices and applications on more Wi-Fi networks to access enterprise resources, the challenge has grown. A survey conducted by Kaspersky Lab in 2015 found that while about half of workers say they use the same device for work and personal tasks, only 11 percent have serious concerns about keeping enterprise data safe from cybercriminals.

Meeting Security Challenges

When the international healthcare company GlaxoSmithKline set out to deploy 31,000 Apple iPad devices to its users, the goal was to boost productivity. Even more critical, however, was keeping patient data and the company's intellectual property safe.

The company, which makes prescription drugs, vaccines and health products, turned to the AirWatch enterprise mobility management (EMM) solution to ensure the safety of its data.

The EMM system helps GlaxoSmithKline IT staff create device and user profiles that dictate who can get access to which resources. Users receive a corporate application catalog that lists more than 200 internal applications designed specifically for different units within the company.

Users can also access documents and data through the AirWatch Content Locker, which authenticates users with Active Directory. Because laws and regulations differ throughout the many countries GlaxoSmithKline operates in, access to resources is tailored to specific regions.

Since deploying the tablets with AirWatch EMM, GlaxoSmithKline has seen an increase in productivity that it attributes to greater collaboration among users, the ability to take digital notes rather than handwrite them and transcribe them later, and easier access to product information for sales staff.

The system has given IT staff a simple, central, web-based management console so it can manage the mobile devices that are helping users do their jobs around the world.

How can IT departments manage and secure access to data without impeding the user experience? That's a question that most IT managers struggle with.

To securely deliver the experience users demand, organizations must manage identity and access along with devices, applications and content. Integrated with an EMM solution, identity and access management (IAM) software can ensure that the right users get access to the appropriate content and applications. It can also track who is using which resources.

IAM can automate onboarding, the process of giving a user access to enterprise resources. It can control access to different resources depending on the user's role, then link that user with all of the relevant devices, apps and content he or she needs. It can also handle offboarding, removing users' access to enterprise resources if they leave the company or lose their devices.

In addition to its security advantages, IAM can help IT staff analyze how apps and data are used, which can be useful in terms of app management and planning future purchases.

IAM, which can be delivered on-premises or via the cloud, can boost productivity by enabling users to employ single sign-on technology to access different resources via their devices; or, for more sensitive applications and content, it can require multifactor authentication. Enterprises can choose from a variety of authentication methods, including:

Biometrics: This form of authentication, which is becoming increasingly common, uses biological characteristics to verify identity. For instance, it can require retina scans or fingerprints to gain access to devices, applications or content. Other types of biometric authentication include voice, facial, hand, ear shape, odor, heart rate, keystroke, DNA, finger vein ID or signature recognition.

For more information on how CDW can help build a comprehensive EMM solution, visit CDW.com/EMM.

Tokens: One way to identify users is to issue smart cards, key fobs or other physical devices that they present to gain access to resources. But this requires that they carry an extra object. Since users already have their mobile devices with them most, if not all, of the time, it makes sense to use them as tokens. Mobile device authentication uses cryptographic keys to identify users.

Passwords: This age-old authentication method is used to access everything from desktops and networks to online accounts and applications. The key to strong passwords is complexity — using a long combination of uppercase and lowercase letters, as well as numerals and symbols. This can be particularly tricky on a mobile device.

Multifactor: Mobile devices are particularly vulnerable because they're small and portable and, therefore, easily lost or stolen, and because they connect to various networks, which can have varying degrees of security. These risks make strong authentication, particularly of sensitive applications and content, an essential element of an organization's mobile security posture. Because no authentication method is foolproof, a robust IAM program incorporates multifactor authentication, which combines two or more methods to identify users. For example, an access management system may require a user to present both a biometric identifier, such as a fingerprint, along with a password or token to gain access to sensitive information.

Regardless of the type of authentication, a strong IAM plan is the lock that keeps an organization's entire EMM strategy secure.

The Future of Passwords

Some people never learn. Despite daily headlines of hacked databases, stolen identities and financially crippling malware, countless users still have "password," "123456" or their grandkids' names as the lock to secure their devices and accounts.

However, even more complex, sophisticated passwords are open to attack. That's why passwords are likely to go the way of VHS tapes and car phones in the not-too-distant future.

While many devices and accounts still rely on passwords, other forms of authentication have recently become more commonplace. For instance, users can set up Apple's iPhone 6 so that a thumbprint scan unlocks the phone instead of a password, but after several unsuccessful attempts, it requires the password. Windows Hello in Windows 10 uses multifactor biometric authentication, and Google combines passwords with tokens for its two-step verification.

Some vendors are testing behavioral-based biometrics for authentication. So, for instance, instead of relying on a thumbprint or retina scan, the authentication system would gauge the way a user interacts with a device — the way he or she looks at it, speaks into it or types on it. MasterCard is deploying new technology that relies on users blinking before a camera to identify themselves.

Another form of identification relies on the devices a person uses to authenticate him or her. It may use biometric authentication — a thumbprint, for instance — but also require that the user log in from a particular device.

Whatever the future of authentication holds, it's a safe bet that it won't be as easy as 123456.

CDW: A Mobility Partner That Gets IT

Enterprises struggling to keep pace with mobility are in good company. The technology in the mobile space moves at unprecedented speeds. Many organizations find that it makes sense to turn to CDW for help creating a mobility strategy that is comprehensive enough to meet the demands of today's workers. It must be built on proven technologies and scalable so it can grow with the organization and today's changing technologies.

CDW partners with mobility leaders to bring the best technology solutions to its more than 250,000 customers. Its account managers, solution architects and engineers work with organizations of all sizes and across all industries to understand their challenges and needs, and help them design solutions to meet their goals.

They can explain the nuances of the different EMM solutions on the market and help organizations determine which would work best for them. They can help plan mobility deployments; select, configure and deploy devices and management tools; and plan security strategies. They can also assist with custom app development, with setting up branded app stores, and with making choices such as which authentication methods to use for different resources.

CDW can also manage an organization's EMM deployment. Its expertise in managing mobility can allow an organization's IT staff to focus on more important tasks.

CDW offers its clients knowledgeable, in-depth advice to help them plan, deploy and manage mobile solutions today and into the future.

The CDW Approach

ASSESS

Evaluate business objectives, technology environments and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services; document technical architecture, deployment plans, ''measures of success,'' budgets and timelines.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. 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.

Together we strive for perfection. ISO 9001:2000 certified

airwatch by vmware

CDW PEOPLE WHO GET IT™