Executive Summary

Smartphones, tablets and other mobile devices have become embedded in enterprise processes, thanks to the consumerization of IT and a new generation of workers raised on mobile technologies. Consumer devices and bring-your-own-device (BYOD) programs are driving a new wave of business process innovation, changing the way customers, employees and partners interact with organizations and with each other. In fact, mobile devices and applications are catching up with—and in many cases surpassing—PCs in the quality and functionality of their applications.

Mobility is changing the way health providers work with patients and the way retail organizations, banks, airlines and even car rental companies serve their customers. Increasingly, mobile applications and mobile-enabled business processes are giving enterprises a competitive edge. For example, any bank that doesn’t offer mobile banking today is at risk of losing customers to competitors. This trend is affecting government at all levels as well, giving federal, state and local agencies greater capabilities for delivering services to citizens and accomplishing their missions.

Table of Contents

2 The Mobile Landscape
3 Mobile Device Management
5 Mobile Application Management
6 Content Management
8 CDW: A Mobility Partner That Gets IT
Enterprises are struggling to keep up, not only with the demand for new mobile applications, but for ways of managing and securing valuable data and resources in the face of this mobile explosion.

Just as quickly, the focus of enterprise management and security is shifting from managing and protecting huge numbers of organization-issued and personal mobile devices to managing and securing the enterprise applications and information they hold, sometimes even in place of managing the devices themselves. Any organization that wants to take full advantage of mobile devices and applications must plan on developing a strategy and deploying the technology to manage and protect its mobile devices, applications and data.

**The Mobile Landscape**

The inundation of mobile devices in the workplace has changed how business is done. According to a November 2013 study from the technology research and analysis firm Forrester, *Workforce Personas and the Mobile App Gap*, almost half of the information workforce carries a smartphone to work, and 18 percent of workers carry a tablet, numbers that have increased dramatically in recent years.

In a late 2013 study, *Global State of Enterprise Mobility: A Look to the Past, Present & Future*, the Enterprise Mobility Exchange, an online community for global mobility professionals and business leaders, reports that 44 percent of mobile practitioners surveyed have invested in mobile applications, 40 percent in BYOD programs and 32 percent in mobile management. The study also shows that more than half of organizations surveyed plan to invest at least $250,000 in mobile management. The study also shows that more than half of organizations surveyed plan to invest at least $250,000 in mobility solutions over the next 18 months.

**Why?** More than 70 percent of practitioners cited increased productivity due to mobile technologies, and almost half cited improved operational efficiency. It’s clear that mobile devices and applications bring great benefits to organizations, as well as workers.

Mobile devices, applications and wireless connectivity help users stay connected to the office at all times, allowing them to collaborate, participate in decision-making and handle customer issues from wherever they happen to be. The benefits are increased productivity, enhanced customer relations and faster time to market, all clear competitive advantages in the perpetually accelerating business environment.

Aside from collaboration and connectivity to email and social networks, mobile devices and applications help streamline and accelerate business processes, particularly when mobile users employ applications that have direct access to back-end enterprise systems and information.

Sales and field workers use mobile devices and applications to keep pace with information such as recent leads, pricing and job scheduling, as well as to log information directly into back-end systems. Such capabilities are enhanced even further by linking them to a mobile device’s camera and GPS capabilities, which can be incorporated into fleet management systems for tasks such as tracking drivers and updating route information.

Law enforcement officers and other government officials have found numerous ways to make use of the enhanced portability, quick boot-up and access to back-end information from tablets and smartphones. For example, officers can access arrest records and mug shots more easily during traffic stops. And a plain-clothes officer at a gun show can check this information more conspicuously with a tablet or a smartphone.

Healthcare workers also have expressed tremendous interest in tablets. Doctors and nurses use tablets and smartphones to access patient record systems and imagery from the bedside or to enter patient information directly into electronic medical record (EMR) systems. They also can respond directly to patients’ requests for information.

**Application & Content Management Privacy**

Privacy is a primary consideration for organizations deploying mobile device, application and content management, especially if mobile devices are also used for personal purposes and contain personal content. The role that user privacy plays in the growing BYOD movement is evolving rapidly and has yet to be resolved completely.

Questions abound: What right does an enterprise have to monitor a user’s personal device, including personal activities, location movements, contacts, web history, social networks, email, application downloads, photos and even bank statements? What right does it have to wipe this content from the device or create a forensic image when a security breach has been suspected? How can organizations expect users to report device theft or breaches when they know it might mean that their personal data, applications and photos will be wiped?

Court decisions and regulations such as the Stored Communications Act have begun to affect these issues, but the ultimate result isn’t clear. What is clear is that these issues will have profound implications for mobile security and management.

Aside from changing the way mobile workers interact with their organizations, mobile devices are changing the way customers, clients and partners interact with these organizations as well.

Most of these mobile capabilities come not so much from the devices themselves but from the applications running on them. It’s these apps that have become so important and so much of a differentiator among today’s enterprises, with many hard-pressed to keep up with mobile application demand. In fact, many enterprises are now taking a “mobile-first” approach.
to new applications and features rather than incorporating mobility as an afterthought.

**Mobile IT Challenges**

The challenges of incorporating mobility in the enterprise are considerable, especially with the growth of BYOD programs that allow users to mix personal information with work-related applications and content on the same device. Users are also bringing their own mobile applications and cloud services as well.

With the help of content management software, many users are not only accessing back-end email systems, but also databases and files, possibly leading to sensitive information being stored on a personal device. Some users are also taking advantage of consumer-oriented file-sharing and synchronization services such as Box and Google Drive to take their work with them, which can challenge strict security policies and regulations.

Unfortunately, mobile devices can be lost or stolen, possibly placing the sensitive data they contain in the wrong hands. Many of the most serious customer data breaches have been the result of lost or stolen notebooks and mobile devices.

Further, the use of personal email, applications and web browsers can expose an organization to malware, not only on users' devices, but also on the network to which users connect. Malware is often used to initiate network intrusions, data theft and advanced persistent threats that can sit on a network for months, stealing an organization's valuable intellectual property.

IT departments also face serious management challenges, such as:

- how to detect rogue, unapproved devices on the network
- how to provision, update and manage mobile users and devices across their lifecycle
- how to prevent users from leaving the organization with sensitive and proprietary information, particularly if they're using file-sharing services meant for the consumer

**Mobile Device Management**

Many IT departments have sought to address the challenges of the mobile enterprise by deploying a mobile device management (MDM) solution. MDM solutions incorporate many of the features used to manage notebook and desktop PCs, such as device discovery, provisioning and lifecycle management. MDM adds other features that account for the special hazards introduced by mobile devices, such as device loss and theft. Those features include password protection, remote wiping and encryption.

Leading MDM vendors include MobileIron, AirWatch by VMware, Citrix Xenmobile and MaaS360 by Fiberlink. BlackBerry developed an enterprise solution for its devices and has since expanded to offer management of other devices as well. And major desktop management vendors, such as LANDesk and Altiris, started integrating MDM capabilities into their desktop management solutions. Many of these solutions have progressed beyond device management, adding capabilities to manage mobile applications and content.

Common mobile device management features include:

**Mobile device discovery and asset management**: Most MDM packages are able to detect new devices attempting to connect to the enterprise network. After devices are approved, enrolled and provisioned, MDM solutions can monitor and inventory the devices and applications stored on them.

**Enrolling and provisioning new devices**: Every MDM solution includes the capability for IT staff to enroll new user devices and connect them to the network. Most management solutions integrate with Microsoft Active Directory and allow users to self-enroll their devices so they don’t have to wait for IT staff to get around to it. IT managers can create the policy, settings and provisioning profile for each user, and users can quickly enroll devices through an enterprise portal and receive their profile and settings, all in a matter of minutes.

**Credential and password management and single sign-on**: MDM solutions provide centralized management and enforcement of device logins, personal ID numbers and account passwords, preventing lost or stolen devices from easily being accessed. Most can provide two-factor authentication and controlled single sign-on access to enterprise applications and information.

**Application whitelisting and blacklisting**: One of the hazards of connected mobile devices comes from users downloading applications that can be dangerous to the network because of malware or unapproved access to other applications and data, such as contacts and calendars. By allowing the IT team to blacklist unapproved applications or limiting applications to those that are specifically approved (whitelisting), MDM solutions can reduce the hazards of mobile apps.

**App stores**: Another way MDM allows an IT department to offer application choice while keeping careful control over users' applications is to provide an internal enterprise app store (think Apple's iTunes store or Google Play but without the transaction process). The app store offers only applications and, in some cases, cloud services that the organization has specifically approved. Once users have been connected and provisioned, IT staff can limit application access to the app store.

**Encryption and virtual private networks (VPNs)**: MDM solutions can centralize the management of device encryption to protect sensitive data on the device and provide VPN tunneling to the enterprise network with robust over-the-air encryption. A relatively new feature of some MDM programs is the provisioning of per-app VPNs or "app wrapping," which...
ensure that a VPN connection is made for a specific application transmission each time it connects to the enterprise, providing more fine-grained security and control than a VPN that spans the entire device.

**Policy enforcement:** An MDM solution also can allow the IT department to apply and enforce mobile device policies, settings and controls, based on user, group and role, including application and encryption controls. Other policies can limit or prevent jailbroken and rooted devices from connecting to the network (because these devices are more likely to have security hazards than others), and also disable Wi-Fi, device cameras, GPS, Bluetooth and other potentially hazardous features. Network access controls can also check devices to ensure they conform with all policies and updates before allowing them to connect to the network.

**Device lock and wipe:** Loss and theft, which can give outsiders access to sensitive information stored on a device or on an organization’s network, represent some of the most serious security hazards of mobile devices. Another hazard is workers who take their mobile work devices with them upon leaving the organization.

Most MDM solutions allow IT staff to centrally manage the capability to lock a device remotely so it cannot be accessed or to completely wipe all data and applications from the device. Newer features that take BYOD programs into account can perform a partial wipe of enterprise applications and data after a user leaves the organization.

**Monitoring, reporting and analytics:** MDM solutions allow centralized monitoring of devices and users, including connectivity, application downloads and use, and other functions. They can produce a variety of analytics and reports that can help the IT shop with getting a handle on mobile security, upgrading requirements and other issues involving planning for the future.

In recent years, many mobile enterprises have incorporated MDM into their management arsenal, and MDM offerings have become increasingly commoditized. A new category, called enterprise mobility management (EMM), incorporates MDM but also emphasizes management of device applications and content in addition to the device itself.

**Going Ape for Apps**

While MDM is a powerful tool in the mobile management arsenal, it doesn’t solve all or even most of the issues confronting mobility deployments. Why? Because the era of the IT department having tight control over user devices and applications in the workplace is over. Organizations recognize that they can’t limit users to devices and applications less capable than the ones they’ve grown accustomed to using every day in their personal lives.

It’s also true that BYOD isn’t truly BYOD if the enterprise exerts tight control over a user’s personal device. Organizations are bound to encounter stiff resistance and obvious legal issues if they try to prevent BYOD employees from using social media or other favorite applications that may present security hazards. And if users know that their family photos will be wiped after a certain number of failed logins, or if the device is suspected of being lost or stolen, they likely won’t report these types of incidents.

That’s why, while MDM is still considered an important tool for managing mobility in the enterprise, many organizations are moving away from tightly managing devices and simply...
blacklisting or whitelisting applications. They are providing maximum BYOD freedom while protecting applications and information. These objectives are accomplished by deploying solutions in two emerging enterprise mobility management categories: mobile application management (MAM) and mobile content management (MCM).

**Mobile Application Management**

MAM overlaps with MDM but focuses on the enterprise mobile applications that reside on the device, rather than the device itself. Some observers view the mobile device and application landscape of today as resembling the Wild West, with a MAM solution as a fort protecting enterprise apps.

Once users are allowed to bring in their own devices, applications and cloud services, two effective ways to protect the organization’s applications and data are to either wall them off inside a secure container on the device (containerization) or app wrapping. Both approaches offer a way to protect enterprise apps from interacting with other apps on the device.

In order to balance the privacy and flexibility needs of the user with the management and security needs of the enterprise, a mobile application management solution need not even provide IT staff with visibility into the personal side of a device.

Enterprise app stores are the key delivery feature of most MAM solutions, providing a catalog of links to approved applications, many of which have been enabled with management and containerization or app wrapping features. The catalog may vary for each user based on his or her identity, group, role or privileges.

The user interacts with the app store when accessing the secure enterprise container on the device. Otherwise, the user is free to access the applications he or she wishes to install on the device’s personal side. Applications that reside outside the container cannot access or affect applications and data within, including contacts, calendars and other sensitive information.

Most enterprise app stores require some form of user authentication and authorization, usually tied in with Active Directory or some other enterprise directory or identity management component. App stores often provide a mix of applications developed in-house and third-party applications with controls applied by the organization, as well as third-party applications that security administrators have deemed to be safe.

Ideally, an app store can integrate with Apple’s Volume Purchase Program and other enterprise licensing programs. This allows IT administrators to use the MAM solution to manage access to redemption links and codes for iOS software that the organization purchases.

Some enterprise app stores provide access to approved cloud software services, such as Salesforce.com, as well as virtual applications. Users may be required to download and install certain applications and are free to pick and choose from the rest. Many of these applications may be downloaded with specific settings as well.

The second essential aspect of application management is centralized control over the behavior of the organization's managed mobile applications, based on management and security policies configured by the IT department. Such policies can include robust encryption for all enterprise application data stored on the device and deployment of an application-specific encrypted VPN every time the app attempts to connect to the enterprise. These settings may also include application-specific policies regarding the use of GPS capabilities, cameras and other device-specific features, as well as controls over application interactions and data-sharing with other apps on the device.

Typically, managed applications interact with a mobile application management solution that allows the IT department to apply these policies.

Managed applications can be provided in several ways:

**Browser or email-based from MAM solution providers:**

They typically offer secure, sandboxed web browser and email client alternatives to the native applications on the device. The goal is to provide a user experience similar to the email or web browsing apps native to the device, while allowing IT administrators to apply policies and controls that protect the organization’s applications and information. These controls include multifactor authentication, app-specific VPNs, web browsing restrictions and policies to prevent data leakage.

Some MAM solutions also provide an enterprise-ready alternative to cloud-based file-sharing and synchronization solutions, such as Box. These require not only enterprise
authenticity, but also VPNs and on-device encryption. They also provide IT administrators with the ability to eliminate user access to enterprise files if the device is lost or if the user leaves the organization, and the ability to wipe any relevant files on the device.

**Software development kits:** Applications built from the ground up internally, using a MAM vendor’s SDK, have a secure layer that allows the IT department to apply policies to an application’s use via the vendor’s MAM solution. Applications developed through this process can be maintained for internal use only or go through a vendor certification and approval process and be provided to other organizations via the vendor app store.

**Vendor wrap:** The MAM vendor may provide a tool that wraps the MAM policy enablement feature around an existing application. In order to do this, the IT department usually needs access to the app binary, so it won’t be possible to apply wrapping to most native or third-party applications available on the device or via public app stores.

**Partners:** Organizations working with the MAM solution provider can offer apps developed through the SDK or that have applied a wrapping capability to their applications.

**Third party:** Some applications are available from third-party enterprise software vendors with policy configuration features built in and need no MAM platform to apply those policies.

---

**CDW’s App Marketplace**

Any organization looking to develop or acquire mobile applications should take a close look at CDW’s App Marketplace. It’s a powerful app development resource that includes a comprehensive library of resources and information, including expertise on application strategy, design, development, testing, distribution, security, support and analytics. It even includes lists of questions to consider in developing an app strategy.

Perhaps even more useful is CDW App Marketplace’s direct access to leading enterprise mobile app solutions and the developers that created them, organized by industry and app functions. Organizations can also connect with CDW’s account managers and seasoned mobile application partners, all of whom have been screened and vetted extensively to ensure they can deliver the best mobile application solutions with the least hassle. Any enterprise can harness this valuable resource to get up to speed quickly, mobilizing and transforming business processes for competitive advantage.

The obvious challenge with mobile application management is providing managed applications to users and devices running different mobile operating systems. Google Android and Apple iOS have different management and security capabilities built in. In the case of Android, some third-party platform vendors supply their own management capabilities.

For example, Samsung Knox is an enterprise-level management platform that Samsung provides for its own Android mobile devices. It offers containerization via a dual-persona architecture. Knox provides its own application programming interfaces (APIs) to create a secure work container on the Samsung device for enterprise applications and data. This platform also implements data encryption that complies with Federal Information Processing Standards (FIPS) 140-2 and offers malware protection.

Administrators can harness MAM solutions that take advantage of APIs to control interactions between a device’s work and personal environments. Knox provides its own cloud-based device and application management solution as well. Some third-party MAM solutions also provide integration with Knox.

BlackBerry provides a similar dual-persona secure container technology, for both its own devices and for Android and iOS devices, as well as via its BlackBerry Enterprise Service 10 software. Apple iOS 7 also provides similar dual-persona features that can be used by MAM solutions. Other solutions employ a hypervisor on the device to create separate virtual machines for work and personal applications.

Whatever the technique, MAM allows users to employ personal mobile devices with the freedom they’ve always had, while providing the enterprise with the security and management its mobile applications require.

**Content Management**

Application and content management overlap. However, content management focuses on the content stored on the device, as well as the device’s access to back-end enterprise information. Content management capabilities include enterprise authentication, as well as encryption of content at rest and in transit via an app-specific VPN.

Mobile content management also encompasses enterprise alternatives to consumer file-sharing applications and services, empowering workers with secure access to such resources. An effective content management solution offers the capabilities and user-friendly interfaces of consumer file-sharing and synchronization solutions such as Box, while providing powerful enterprise security and management controls.

These MCM solutions may use existing enterprise repositories, with connections to SharePoint, WebDAV and file servers. Or they may provide cloud repositories or links to other cloud services such as Box or Google Drive. In all cases, they allow IT administrators to apply a number of data leakage controls while still empowering employees with the latest information needed to do their jobs.

Some also offer content searching, versioning and other features of classic content management systems, as well as viewing of content stored in many different file formats.
They may also offer robust multifactor authentication and encrypted connections.

**ROI: Control vs. Enablement**

How does an IT administrator calculate the return on investment of an enterprise mobility management deployment? For many organizations, ROI may be difficult to quantify. One could think of security ROI, where the avoidance of a major mobile security breach could potentially save an organization thousands or even millions of dollars. Many of the security breaches of the past few years have come from stolen or lost mobile devices containing employee ID and credit card information. The costs in lost productivity and customers, remediation, customer notification, lawsuits and compliance fines can be steep. Simply avoiding one breach could potentially pay for the entire solution and more.

However, enablement is the other side of ROI. Mobile devices and applications enable business process innovations, customer relations improvements and competitive advantages that can deliver significant results in revenues, profits and time to market. A well-managed mobile deployment can empower IT shops and staff to take full advantage of these benefits safely. And, with centralized provisioning and management, users are up and running, connected to enterprise applications and content with their new devices much more rapidly than would otherwise be possible.

Depending on the capabilities of the MCM solution, along with the mobile operating system and platform involved, mobile content management data leak prevention policies can be configured to control:

**Open in:** This feature restricts the applications that can be used to open and read files containing sensitive enterprise information. If a secure container is created on the device, the MCM solution can be configured so that only applications included as part of the secure enterprise container can be used to open files. Or the solution simply may not allow them to be opened on the device at all.

**Editing:** This feature controls modifying mobile content delivered from the secure content sharing solution.

**Downloading:** This feature allows the saving of specific documents.

**Printing:** This manages the printing of files stored on the device, which can be allowed or prevented depending on the user and the content.

**Saving:** This controls file access when the user is offline.

**Watermarking:** This feature can be applied to documents to discourage screen shots.

**Geographical restrictions:** This takes advantage of location services and allows content to be opened only within a certain geographical range, depending on its sensitivity.

**Cutting and pasting:** These features manage the removal or reuse of text or images from sensitive files to email messages or other documents.

**Locking or wiping:** This secures container content if the device is lost or stolen, the user leaves the organization or after a predetermined number of failed logins.

**Secure browser and email policies:** These allow links in email or content to be opened only in a secure enterprise-provided browser. Attachment restrictions can be applied to enterprise email to permit only links to shared content files, rather than allowing attachments in the emails. This not only offers better security, but it also can save storage capacity if email with the same attachment is sent to multiple recipients.

**Synchronization:** This control allows syncing to take place only over secure Wi-Fi connections, a measure that also can help control connection costs.

**Monitoring and reporting:** These features give administrators insight into content usage. The best MCM solutions provide the ability to oversee how much and what type of content is being accessed by which users, as well as any changes made in content folders, categories, etc.

Mobile content management continues to evolve. Among the emerging features that vendors are delivering: content expiration dates; content push based on factors such as geographic location, relevancy and usage; and integrated content collaboration tools.

Mobile content management also includes granular data access controls applied to any device that connects to back-end enterprise databases and other information repositories based on user identity, group, role, device and application. Some EMM solutions provide these types of access controls, which also may be available via an application delivery controller solution, such as Citrix NetScaler.

Many incorporate access controls to ensure that a device has the latest application, operating system and anti-virus updates before it is allowed to connect to enterprise resources and access content. These controls also may restrict reading, writing, printing, saving and other actions based on location and device factors.

Enterprise mobile management is a rapidly evolving practice that is moving away from device management and toward application and content management, with more precise tools and capabilities emerging regularly.

Depending on the capabilities of the MCM solution, along with the mobile operating system and platform involved, mobile content management data leak prevention policies can be configured to control:

- **Open in:** This feature restricts the applications that can be used to open and read files containing sensitive enterprise information. If a secure container is created on the device, the MCM solution can be configured so that only applications included as part of the secure enterprise container can be used to open files. Or the solution simply may not allow them to be opened on the device at all.

- **Editing:** This feature controls modifying mobile content delivered from the secure content sharing solution.

- **Downloading:** This feature allows the saving of specific documents.

- **Printing:** This manages the printing of files stored on the device, which can be allowed or prevented depending on the user and the content.

- **Saving:** This controls file access when the user is offline.
CDW: A Mobility Partner That Gets IT

Enterprises face challenges in mobilizing employees. That’s where CDW can help quickly roll out mobile technologies. CDW maintains partnerships with leading wireless vendors, including network providers and device manufacturers, to offer a complete line of IT products and services.

We offer a one-stop shop of integrated mobility solutions consisting of software, hardware and cellular wireless activation services. Regardless of the mobile platform users choose, CDW’s dedicated experts can step in to help with activation and configuration services. CDW account managers and solution architects are ready to assist with every phase of choosing and leveraging the right mobility solution.

The CDW approach includes:
- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future design and proof of concept
- Procurement, configuration and deployment of the final solution
- Ongoing project measurements to meet service-level agreements (SLAs)
- Complete product lifecycle support
- Consolidated device and solution management platform

Working with your CIO, management team or IT department, we can design, plan, implement and support comprehensive mobile solutions built around your organization’s needs.

To learn more about CDW’s mobility solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/mobility

Citrix XenApp is a Windows application delivery system that manages applications in the data center and delivers them as an on-demand service to users anywhere. XenApp reduces the cost of application management, increases IT responsiveness when delivering an application to distributed users and improves application and data security.

Citrix XenApp enables organizations to improve application management by:
- Centralizing applications in the data center to reduce complexity and lower the cost of desktop management by up to 50 percent
- Controlling and encrypting access to data and applications to improve security
- Delivering applications instantly to users anywhere on any device
- Simplifying and automating the process of delivering or updating applications, enabling IT to focus on strategic initiatives

CDW.com/citrix

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
145520 – 140620 – ©2014 CDW LLC