The Ultimate Guide to Enterprise Mobility Management

v1

MobileIron

Table of Contents

Executive Summary

Ready or not, the global mobility trend is forcing enterprises to enable a mobile workforce with business productivity tools on any device, regardless of the underlying operating system. As mobile users increasingly demand the ability to use their own devices for everything personal and work-related, IT is quickly losing control over end-user technology decisions. Enterprises can no longer ignore this reality, especially given the explosive global demand for mobile devices. According to IDC, "the worldwide smartphone market reached a new milestone in the second quarter of 2014 (2Q14), moving past the 300 million unit mark for the first time in its history." IDC also found that BlackBerry shipments were 78 percent lower than the previous year, which followed three consecutive quarters of sequential decline. It's clear: The heyday of the locked-down corporate device is over. How can organizations prepare for what's coming?

Avoid fear and loathing in the era of enterprise mobility

Rather than avoid or deny the mobility juggernaut, this guide is designed to help enterprise leaders securely empower mobile users to achieve business transformation. As desktop anti-virus and locked-down corporate devices lose their relevance in the modern enterprise, companies need new strategies and technologies to confidently move forward on the Mobile First journey.

Enterprise Mobility Management (EMM) is a comprehensive solution that helps organizations support a multi-OS environment that allows employees to use their preferred devices to access corporate apps and data while meeting critical security and compliance requirements. The three components of EMM — Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) — help provide a secure, scalable, and enterprise-ready architecture that puts the user experience first.

Why prioritize the user experience?

The success or failure of any mobility initiative depends completely on user adoption. Therefore, every EMM platform should allow the enterprise to enable critical business processes through mobile apps that are easy to access and use on any device. But EMM is not just about keeping users happy. It should also make the job of IT easier by simplifying access control and authentication, and allowing users to manage their own devices and easily troubleshoot problems without relying on the help desk.

Accelerate the Mobile First journey

In addition to describing how EMM works, this guide also illustrates a typical implementation journey that explains how an organization goes about deploying and managing all the pieces of an EMM solution. By providing a detailed, best-practice deployment process and recommendations for finding the right EMM provider, this guide offers practical, step-by-step insight that can help any organization accelerate their journey to becoming a Mobile First enterprise.

Introduction

Enterprise mobility: What's driving the evolution?

The PC era is over

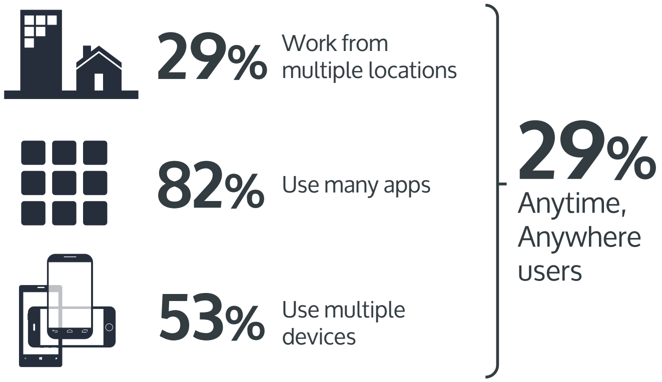
The global adoption of mobile devices has occurred at a rapid pace, and the trend shows no sign of slowing. In fact, by 2015 tablets are predicted to outsell PCs for the first time, marking the beginning of the end of the PC era.[1]

This and other consumer technology trends are clearly driving the evolution of enterprise mobility. As consumers (i.e. employees) become more mobile, they want their work lives to be just as flexible and responsive to their needs. They want to be able to use their own device — instead of a company-issued device — for all their personal and business-related responsibilities. As a result, consumer choice is now the driving force behind mobile enterprise decisions, and demand for the traditional locked-down enterprise device is rapidly decreasing.

Mobile content is exploding

The development and distribution rate of mobile content, from digital documents to viral videos, is unprecedented. It will continue to grow as the ability to create and manage more enterprise apps and content becomes easier, more cost-effective, and critical to business productivity. In fact, in the period from 2005 to 2020, the volume of digital information is expected to grow by a factor of 300.

Rise of Anytime, Anywhere Users



29% Work from multiple locations

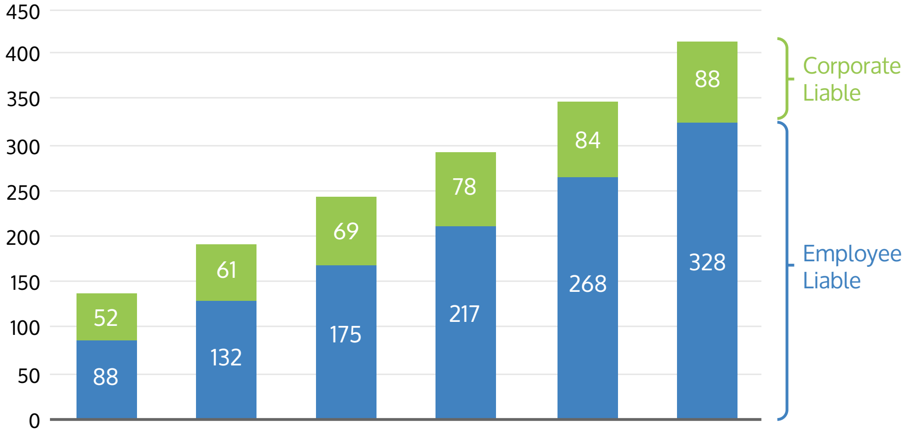
82% Use many apps

53% Use multiple devices

29% Anytime, Anywhere users

Forrester February 2013
"2013 Mobile Workforce Adoption Trends"

BYOD is in Full Swing



IDC December 2013
"Worldwide Business Use Smartphone 2013-2017 Forecast Update"

[1] IDC press release, "Worldwide Smartphone Shipments Edge Past 300 Million Units in the Second Quarter; Android

Multi-OS is here to stay

As the mobile technology market continues to change, multi-OS environments are becoming the norm. End users want to be able to choose which device they want to work on which means that enterprise IT now needs to be able to secure and manage multiple mobile operating systems. Before the mobile transformation, IT would think of the end user computing world as Windows and Blackberry only and management was simpler. But now the rate of change is enormous. To put things in perspective, there is a new version of Windows now every few years and the speed is accelerating. There are many flavors of Android, and iOS and also Windows Phone are rapidly coming into the enterprise. This means that IT needs to become more agile than ever before to quickly accommodate the range of constantly-evolving mobile devices. However, the challenges of predicting how this technology mix will evolve can make it difficult for IT to know which devices to support. The answer is easy: Find out what's hot in the consumer market. When you know what your employees are buying, then you can design your mobile strategy to support those devices.

Mobility management: Know the challenges

Supporting device choice

The mobile era is dramatically shifting the role of IT in the enterprise. Instead of dictating which technologies employees will use, IT now needs to implement the diversity of technologies that employees are bringing into the enterprise. IT organizations that don't support mobile users or their preferred devices will quickly find themselves marginalized because mobile employees can simply go around unresponsive IT organizations.

Mobile app and content management

The growth of mobile apps is just beginning. By the end of 2017, 4.4 billion people will be using mobile apps, an increase of nearly 30 percent every year.[2] Today, Google Play and Apple's App Store together provide more than 1.6 million apps, and the market is expected to triple by 2017.[3]

What does this mean for the enterprise? The demand for mobile apps is clearly exploding, and end users expect to have more than just corporate email on their smartphones. Employees want to be able to access all of the critical business processes and content they use for work every day. And, as more platforms such as iOS 8 increase support for enterprise app development, the demand will only increase. To meet this demand, enterprises can no longer take the approach of first developing for a PC-based world and then transitioning to mobile. All app and content development going forward must be enabled for mobile first.

[2] McCafferty, Dennis. "12 Amazing Facts about Mobility." CIO, Sept. 1, 2014. http://www.cioinsight.com/it-strategy/mobile-wireless/slideshows/12-amazing-facts-about mobility.html/ 3 McCafferty, Sept. 1, 2014.

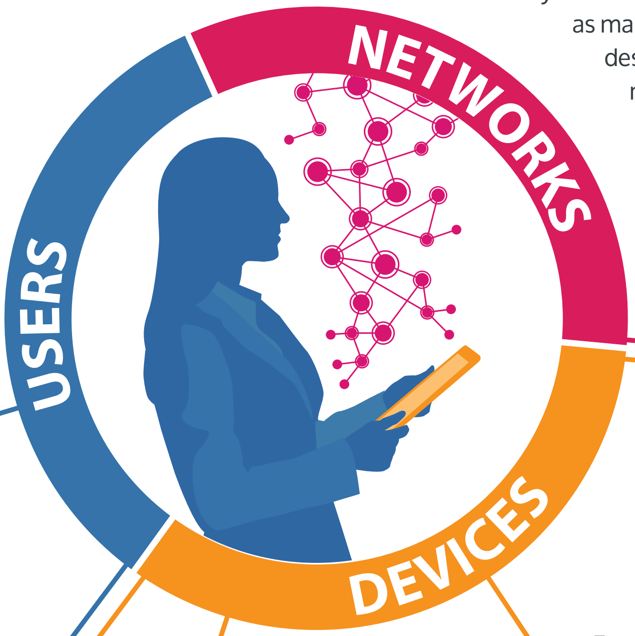
[3] McCafferty, Dennis. "12 Amazing Facts about Mobility." CIO, Sept. 1, 2014. http://www.cioinsight.com/it-strategy/mobile-wireless/slideshows/12-amazing-facts-about mobility.html/

Security and compliance

One of the biggest mobile challenges IT must solve is securing data and apps (including third- party apps) on all mobile devices without impacting the native user experience. Before the mobile era, the biggest security risks were malware and viruses due to the vulnerability of open file systems and an unprotected kernel. Today, mobile operating systems have a sandboxed file system and protected kernel, so traditional security threats present less of a concern. However, mobile technologies face three other types of threats: user-based, device-based, and network- based.

Threat Vectors on Mobile are Different From PC

Sandboxed mobile operating systems are secure. Threats, such as malware, are mitigated by OS design. Preventing data loss on mobile requires focus on a different set of risk vectors.



Data Loss

Data loss to cloud services and productivity apps via ***open-in, copy, paste*** *and forwarding functions*

Device Tampering

Exploit OS vulnerabilities to ***jailbreak or root devices,*** *bypass security, and install malicious apps from un-authorized app stores*

Malicious or Risky Apps

Collect and share data such as ***personally identifiable information (PII)*** *and device location with third party advertising and analytics systems*

Form Factor

Portable form-factors make mobile devices susceptible to ***loss or theft***

Always-On Connectivity

Mobile devices are hyper-connected and often access sensitive data over untrusted networks, increasing the risk of data loss through ***Wi-Fi sniffing, rouge access points and Man-in-the-Middle (MitM) attacks***

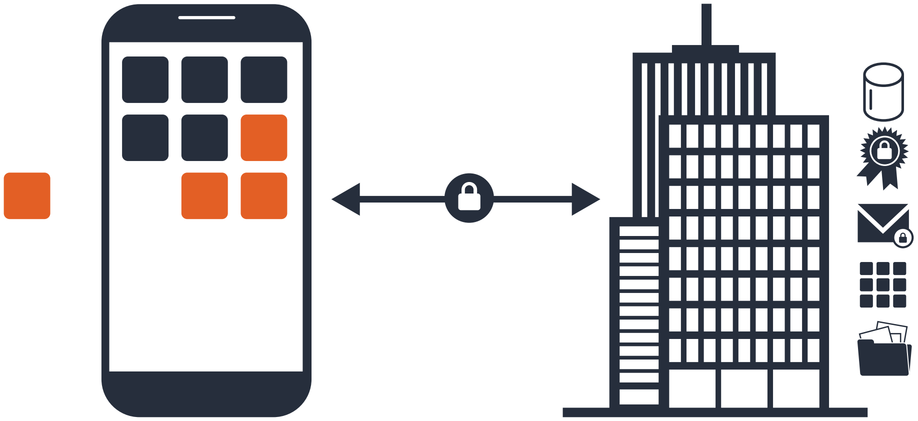
To address these security risks, IT must employ a proven and consistent approach that can:

- Securely provision mobile devices to users.
- Allow users to authenticate on their devices.
- Configure business apps and ensure they run only on authorized devices.
- Establish data loss prevention (DLP) controls to maintain compliance.
- Provide secure tunneling to the enterprise.
- Delete business apps and data when needed without compromising end-user privacy and personal data.

Enterprise Mobility Management (EMM)

What is it?

Enterprise mobility management (EMM) is a comprehensive solution for managing mobile devices, applications, and content across the entire organization. EMM solutions are designed to help companies leverage mobile technology as a tool for business transformation by empowering end users to be more productive wherever they are, on any device, while enabling IT to meet critical security and compliance requirements.



The three components of EMM

Mobile Device Management (MDM)

MDM provides the foundation of any EMM solution by allowing IT to:

- Enable employees to be productive on the devices they love to use.
- Secure and manage mobile devices across multiple operating systems.
- Provide secure corporate email, automatic device configuration, and certificate-based security.
- Selectively wipe enterprise data from the device without impacting personal data.

Mobile Application Management (MAM)

MAM capabilities enable IT to:

- Build and maintain an enterprise app storefront.
- Secure applications on any device.
- Authenticate end users on the device.
- Separate business and personal apps on mobile devices.

Mobile Content Management (MCM)

MCM capabilities enable IT to:

- Secure corporate data on mobile devices without compromising the end-user experience.
- Provide an intuitive way to access, annotate, and share documents

from email, SharePoint, and other enterprise content management systems as well as enterprise and personal cloud services.

- Establish DLP controls to protect corporate content from unauthorized distribution.
- Encrypt email attachments to ensure they can only be viewed using authorized applications.

Benefits of EMM

Provide a secure, scalable, enterprise-ready architecture

Although mobile technologies are immune to traditional PC-based viruses, they face other types of threats. Managing these threats requires a layered security approach that protects enterprise data without impacting user productivity or the native device experience.

EMM solutions are designed to handle the unique security requirements in mobile enterprises by providing:

- **Security for enterprise email, apps, and content** without monitoring or modifying personal data on the device.
- **Certificate-based identity management** to ensure only authorized users can access the device.
- **Secure multi-user profiles** to securely allow users to share a single device.
- **App containerization** that enables data within each app to be encrypted, protected from unauthorized access, and removed from the device without harming personal user data.
- **Per-app VPN technology** that provides corporate network access to authorized apps only.
- **DLP features** that allow IT administrators to define open-in and copy/paste functions.
- **Closed-loop automation** features that automatically trigger notifications, quarantine, and other access control actions when devices fall out of compliance or violate policies.
- **Self-service features** that simplify IT management by giving users the tools for registration, compliance checking, remediation, and other device management and troubleshooting capabilities.

Support end-user choice with a native device experience

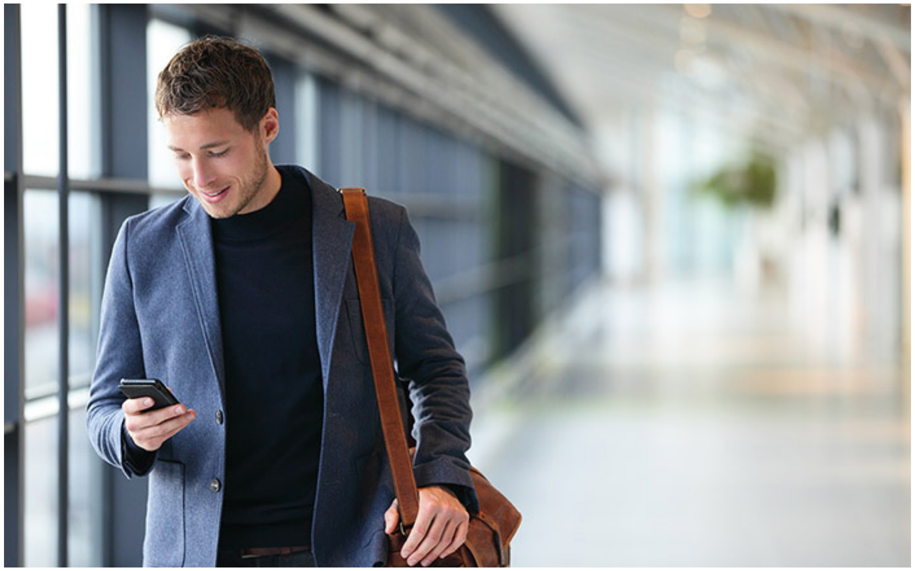
To ensure mobile employees stay productive at work, the user experience must be the top priority of every mobile initiative. To support this goal, EMM solutions are designed to:

- **Enable a multi-OS environment,** so employees can use their preferred device, whether it's iOS, Android, or Windows Phone.
- **Allow users to find and install critical enterprise apps,** such as corporate email, calendar, and other productivity apps.
- **Separate and manage highly sensitive personal and corporate data** on mobile devices without impacting the native device experience.
- **Implement security measures** that are highly effective but invisible to the end user.
- **Help users** maintain compliance with corporate policies

EMM Platform Requirements

Develop and design with the user in mind

The user experience must be at the center of any mobility initiative. If the device, app, or content is not something users want or are able to use, then it simply won't be adopted no matter how much your IT organization pushes it. So the EMM platform must be able to support the following user requirements:



Enable choice of device and OS

To support the devices employees want to use, IT must implement and support a multi-OS EMM solution. As mentioned previously, consumer choice will drive enterprise IT decisions, not the other way around.

Provide secure access to mobile apps and data

Employees don't want to carry around different devices for work and personal business. So instead of separating devices, it's the responsibility of IT to separate business and personal apps and data on the device. Because users increasingly rely on their devices to manage highly personal information, it's critical for IT to maintain the privacy and security of that data. For example, if an employee leaves the company, a full device wipe could be catastrophic for that user. Therefore, the EMM solution should enable selective application and data management, a proven approach to protecting corporate apps and data and end-user privacy by keeping them separate on the device.

Ensure EMM features are easy to use

Perhaps most important of all, the device and app management features of the EMM solution should be easy to use. For instance, users should be able to quickly authenticate and gain seamless access to corporate apps and data from their devices. Users should also have access to self-service tools that help them manage basic device features and troubleshoot problems quickly.

Simplify IT management

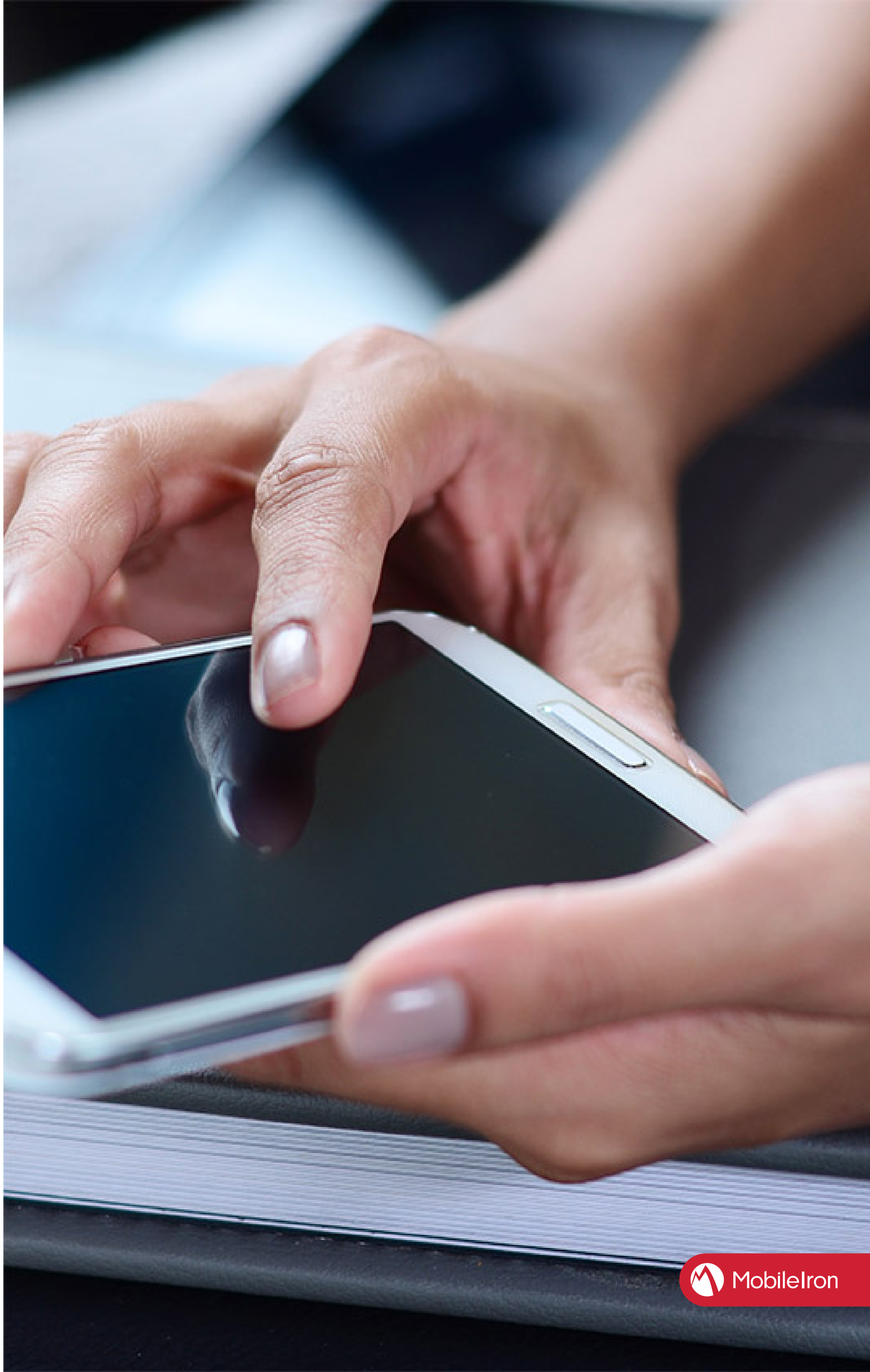
Complexity is one of IT's biggest concerns with mobile management. The ability to administer and secure a multi-OS environment with a range of devices, apps, and content is no small task. For this reason, every EMM solution should enable IT to:

Simplify access control and authentication

Giving users access to the apps and content they want on any device requires the ability to not just authenticate the user on the device, but to protect access to individual enterprise apps as well. However, requiring the user to enter a password every time they want to open an app or access a corporate document is tedious and will quickly frustrate users. Therefore, the EMM solution should enable IT to authorize users as quickly and painlessly as possible.

Enable critical business processes

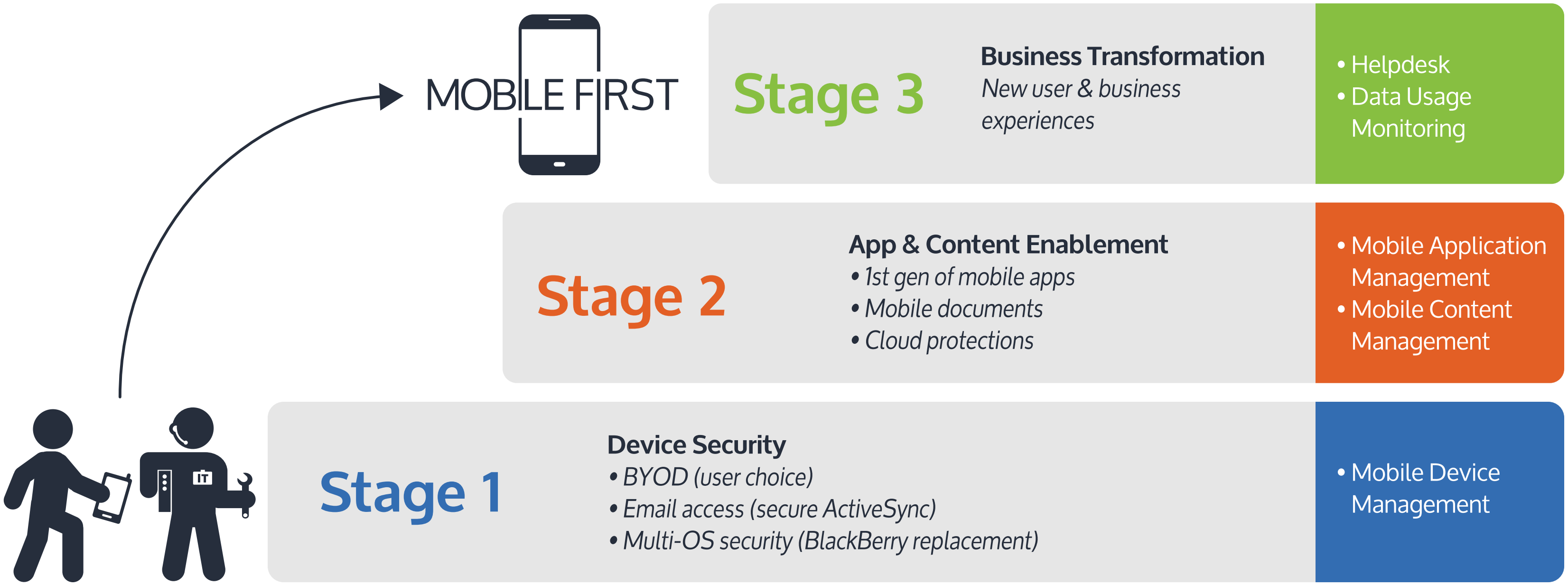
The most important mobile apps are ones that enable employees to have essential data at their fingertips to make core business decisions. For example, in a retail environment, sales associates can use mobile apps to assist customers throughout the store. They can look up inventory or complete customer purchases, which eliminates long lines at cash registers and keeps customers happy. Therefore, IT should use an EMM solution to deploy enterprise apps that drive business productivity by empowering users to access the critical processes they need every day.



The EMM Implementation Journey

Most organizations begin their enterprise mobility journey by first providing access to email and device configuration. For organizations new to enterprise mobility, starting small to gain both experience and the trust of end users is critical to ensuring success on the rest of the EMM journey. However, the true benefits of EMM happen when the mobile platform becomes the primary IT infrastructure for the delivery of applications and content. This is how mobility becomes a catalyst for real business transformation.

A Journey in Stages



Stage 3

Business Transformation
New user & business experiences

- Helpdesk
- Data Usage Monitoring

Stage 2

App & Content Enablement

- *1st gen of mobile apps*
- *Mobile documents*
- *Cloud protections*

- Mobile Application Management
- Mobile Content Management

Stage 1

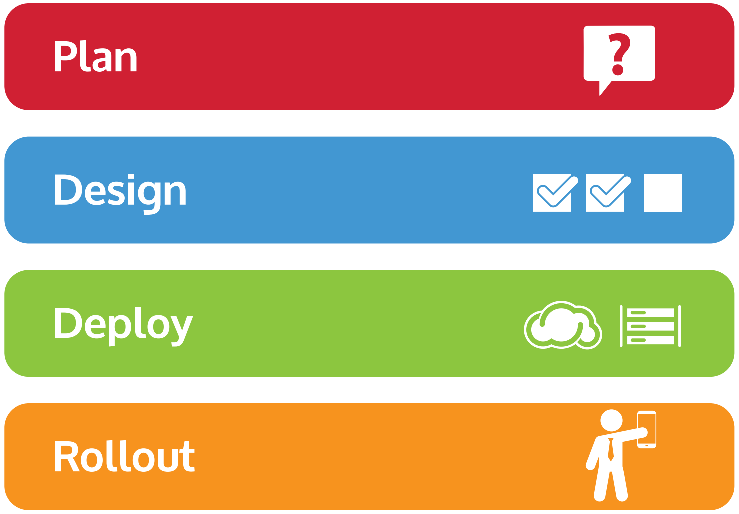
Device Security

- *BYOD (user choice)*
- *Email access (secure ActiveSync)*
- *Multi-OS security (BlackBerry replacement)*

- Mobile Device Management

EMM Deployment Best Practices

Deploying an EMM solution is best achieved in the four-step process (Planning, Design, Deployment, and Rollout) described below.



Plan

Design

Deploy

Rollout

Plan

To begin the planning process, it's important to first know what success means for your organization, and how quickly you expect to achieve it. Gathering feedback from key stakeholders across your enterprise will be critical in the planning stage. For example, some companies define success as a fairly straightforward deployment that provisions security, email, and Wi-Fi profiles to users. In a basic deployment, device registration is handled largely by IT staff who are familiar with mobile operating systems and their features.

Companies that plan to go beyond a basic EMM deployment will need to address the following questions in the planning stage:

1. Are your employees experienced with mobile technology?

Technically savvy users will be more self-sufficient than those who are new to mobile. Users with less technical experience may require more IT support.

2. Which mobile operating systems and devices will your organization support?

The answer to this question requires knowing which devices are most popular among employees. While you may not be able to support all of their preferred devices in the beginning of your rollout, the last thing you want to do is allocate resources to support devices few employees use.

3. How complex is your network infrastructure?

A single data center rollout with an internal set of network services will require fewer resources than a multi-site rollout with complex networking and infrastructure. Outsourcing IT services will require additional planning.

4. How mature is your IT governance framework, policies, and processes?

Effective IT governance usually results in on-time, on-budget program development and solution delivery that meets organizational goals. Organizations that lack an established or mature IT governance program may require more time and staffing resources to implement their EMM solution.

5. How effective are your employee education and training resources?

Companies with existing training and education frameworks and infrastructure can accelerate an EMM rollout and program adoption for both employees and help desk staff. Building an employee education initiative will require more up-front effort, but will pay off with the development of more mobile-savvy workers and fewer help desk calls.

6. Does your IT team have experience with certificate authentication?

Certificate authentication is becoming a standard feature in mobile initiatives. Having internal expertise in this area will help accelerate the deployment and set-up process.

7. Can your IT organization develop and deploy mobile enterprise apps?

Anyone who develops apps for your company should have the experience and know-how to deliver an outstanding mobile user experience. This will be critical to ensuring the success of your mobile strategy. If you don't have skilled app developers in-house, you will need to outsource this key function.

8. What are your company's security requirements?

Information protection and data security on mobile devices are critical components of any EMM deployment. Companies in highly regulated industries will likely have a lower tolerance for risk (and therefore more security requirements) than companies with a higher risk tolerance.

Design ☑ ☑ □

This phase of EMM deployment is all about defining the policies that govern your mobility strategy. This phase has four steps, which are outlined below:

1 Define Roles	2 Define Visibility	3 Assign Actions	4 Manage Distribution
How many admins? What responsibilities?	*Which users/devices do each admin view and report on?*	*What actions each admin can take*	*What apps, policies, configurations each admin can distribute to users/devices?*

1. Define Roles:

First, determine how you want to organize administrative tasks like help desk support, user registration, and device configuration management. For example, how many levels of help desk support do you need? Who will develop and manage your in- house apps — existing staff or third-party developers? Who will manage policy and configuration processes?

2. Define Visibility:

Second, you will need to determine which users and devices each IT admin will manage and how much control and visibility they will have. Also, your device and user management policies may vary according to business unit or geographical region. For instance, some countries have stronger privacy regulations than others, and your device policy will need to meet those requirements.

3. Assign Actions:

Third, assign the actions that you want each IT role to perform. For instance, which administrators will manage the distribution of apps, policies, and configurations based on your visibility policies?

4. Manage Distribution:

In this final step, decide which apps, policies, and configurations will be deployed, as well as who deploys them and when. Identify which IT admins will be responsible for various distribution roles, and prevent admins from performing any unauthorized actions.

Deploy

In the deployment phase of your EMM rollout, you will need to determine if your platform will be an on-premise or cloud-based solution. This decision may also be affected by various pricing models, which can include a subscription rate or perpetual licensing options.

- **On-Premise**
  An on-premise solution is packaged as an easy-to-install software appliance that plugs into the corporate network and can be up and running in less than a day. On-premise solutions can be licensed either perpetually or as a subscription agreement.
- **Cloud-Based**
  An EMM cloud deployment integrates tightly with on-premise enterprise messaging and security systems, such as corporate email and corporate directories. Cloud deployment options are offered on a subscription basis.

Rollout

Once your EMM solution is ready for rollout, you will need to make sure your help desk staff are thoroughly prepared by enabling them to:

- **Understand multi-OS management issues** by educating help desk staff about various device, server, and network issues they are likely to face. Clearly define the troubleshooting steps, escalation process, and responsibilities for resolving each type of issue.
- **Engage device experts** to provide deeper insight into all of the devices your help desk staff will encounter.
- **Access the resources they need** for the level of support they will be delivering. Ensure they have easy-to-usetroubleshooting resources, such as problem resolution scripts and an online knowledgebase.
- **Leverage ongoing education opportunities** to ensure they stay up-to-date on mobile device upgrades, infrastructure updates, and more.

What to Look for in an EMM Provider

One of the most frequently asked questions about EMM is how to find a provider that can meet all of your unique requirements. Here are a few key criteria that can help narrow and accelerate your search:

Platform neutrality

Think about what mobile devices looked like five or ten years ago. Some of those brands barely exist anymore. Chances are, mobile technology will look very different five years from now as well. Instead of trying to predict which mobile platforms will succeed in a hyper-competitive consumer market, it's much easier to choose a vendor that is designed for platform-neutral, multi-OS management. Then you don't have to worry about which devices to support, because your vendor will be able to manage them no matter what.

Purpose-built platform

Enterprise mobility is the future, and mobile IT is quickly becoming the means by which apps and data are deployed and managed. Look for a vendor whose platform was built from the ground up with this vision in mind. EMM solutions that are simply add-ons or a component of an existing infrastructure may not be comprehensive or integrated enough to deliver the scalability and reliability you need.

Extensive ecosystem

In addition to choosing a vendor with a strong vision and purpose-built EMM platform, your solution provider should also cultivate a thriving ecosystem of complementary mobile enterprise solution providers. A broad partner ecosystem ensures that your vendor can support the broadest range of mobile apps, operating systems, devices, and deployment configurations and address a broad set of customer uses cases.

Strong and growing customer base

Last but not least, look at your vendor's customer portfolio. Does the EMM provider support companies across a broad range of industries? Is their customer base expanding or do they only serve a narrow segment of the market? Researching the EMM provider's customer base will be a critical due diligence component of your vendor selection process.

Summary

Enterprise mobility is not just about buying the latest technology or putting email on an employee's phone. Mobility is about transforming your business to drive productivity in exciting new ways. Although embarking on a mobility initiative can seem like exploring unchartered territory, the right EMM solution can help you quickly move forward in your journey to becoming a Mobile First enterprise.

About MobileIron

A leader in Enterprise Mobility Management (EMM), MobileIron has been chosen by over 7,500 customers worldwide including more than 400 of the Global 2000. These companies are transforming their business through enterprise mobility and accelerating innovation. Available as an on-premise or a cloud solution, MobileIron is purpose built to secure and manage mobile apps, docs and devices for global organizations. MobileIron works with more than 130 AppConnect partners and more than 36 Technology Alliance partners who have integrated, or are in the process of integrating, with our platform. And our customers have used AppConnect to secure over 1,000 internally developed applications. Finally, our global Customer Success team has developed the depth and breadth of expertise to provide our customers with the support required on their journey to become Mobile First.

www.mobileiron.com