



**MCMK**

# **Enterprise Mobility Management (EMM) Contributes to Sales and Revenue Growth**

---



# Table of Contents

---

Introduction	1
The Importance of Enterprise Mobility Management Technology in an Enterprise	2
1. Mobile Device Endpoint Security	3
2. Enterprise Data Loss Prevention and Mitigation	3
3. Increased Productivity	4
4. Mobile Content Management	4
What Makes Mobile Data Management Critical For Enterprises Today	5
1. Device Inventory	5
2. Restrictions and Configurations	5
3. Application and Content Management	5
4. Device Inventory	6
5. Policy Enforcement	6
6. Automation	6
7. Remote Maintenance	6
Conclusion	8





# Introduction

---

Managing mobile devices across business activities is more important than ever before for the success of the company. To deal with data security and privacy challenges, several types of mobile security technologies have emerged in recent times, including MDM (Mobile Device Management) and EMM (Enterprise Mobility Management).

MDM is all about managing devices remotely and enabling users to complete assigned tasks on their phones and tablets. Device security, device provisioning, location tracking, and enrollment are all included in MDM.

It also aids in wiping data in the event that the device is stolen or misplaced. Security policies can be enforced, inventory can be tracked, and real-time monitoring and reporting can be done with a basic MDM tool.

This is a very logical way to manage a company-owned device from a security standpoint. However, some employees are hesitant to carry two separate smartphones for work and home use. As a result, it was in the best interests of businesses to accommodate employees' requests for BYOD (Bring Your Own Device): a single device that allowed employees to easily switch from personal to work use, anywhere and at any time.

Because of the increasing proliferation of smartphones and mobile applications, as well as the requirement for data security, Mobile Application Management (MAM) solutions were developed to restrict the management and control of specific business applications.

Mobile Application Management is similar to Mobile Device Management (MDM), except it only applies to specific applications on a device rather than the entire device.

MAM is a great way for employees and employers to work together without compromising data security or invading employee privacy. However, MAM comes with its own set of challenges that make it a far cry from the perfect solution. This is where Enterprise Mobility Management (EMM) comes in.

EMM is a hybrid solution that combines MDM and MAM with a secure container to keep company data safe. App Wrapping, Mobile App Management, Containerization, and Mobile Content Management are all functions of an EMM solution in addition to MDM.

EMM is a comprehensive set of services that provides total data security for enterprises using BYOD and dedicated devices.

In this whitepaper, we discuss how, through MDM or EMM, businesses can configure robust security policies on these devices, making them fit for enterprise use. We accomplish this goal by separately discussing the role of EMM and MDM in the success of an enterprise.



# The Importance of Enterprise Mobility Management Technology in an Enterprise

---

Companies that do not have a mobile strategy are destined to fail. There are already 3.8 billion smartphone users worldwide, accounting for 60% of the global population, and this number is expected to rise to 80% by 2025<sup>1</sup>.

The figures are astonishing, and the opportunities to expand the sphere of business and customers are limitless. All things considered, a well-thought-out Enterprise Mobility Solution plan can make or ruin a company.

Enterprise Mobility Management (EMM) is the umbrella term for the solutions, technologies, and rules that govern the use of mobile devices in the workplace. EMM is a catch-all term for several mobility-related technologies, such as mobile device management (MDM) and mobile identity. To put it another way, it acts as a glue that connects your mobile devices to your IT environment.

Enterprise mobility as a service boosts productivity by delivering critical data on the go. While the emphasis is on customer service, responsiveness, and employee productivity, transitioning your organization to the next generation of technology is critical to its success.

Now, all mobile devices can interact with cloud services, enabling users to respond to any email while on the go. This enables decision-makers to convey approvals, submissions and any tasks that need to be performed in a timely manner.

Enterprise Mobility Management is important because it gives companies more confidence in reaping the benefits of BYOD policies, such as increased productivity and lower technology costs.

Companies could have a lot of trouble dealing with issues with their BYOD remote devices if they do not use enterprise mobility management.

Because of its potential benefits, EMM is critical for today's business. It can, for example, increase productivity across the firm by delivering essential information regardless of location or device.

Users can respond to emails, phone calls and organize calls on the go, which allows them to focus more on their job and servicing the customer. The following is a quick overview of EMM benefits.

1

## Mobile Device Endpoint Security

Cybersecurity is arguably the most important of all the benefits of enterprise mobility management.

Every additional connected device increases the number of nodes in a company's digital perimeter, increasing the number of attack vectors available to hackers. An enterprise can ensure a standardized level of cybersecurity across all connected devices with the right EMM solution.

2

## Enterprise Data Loss Prevention and Mitigation

Endpoint and data loss prevention and mitigation are also included in the benefits of enterprise mobility management. Threat actors utilize stolen or lost mobile devices as easy entry points into corporate networks; they can typically use the saved login information to counterfeit a company's system and steal critical data.

An organization can use enterprise mobility management to assist employees in avoiding these mobility traps. The enterprise can use it to delete data from a stolen or lost endpoint to prevent hackers from exploiting it.



## 3

### Increased Productivity

One rule of thumb in mobility is that when users have control over their devices, their productivity increases. Employees who own the device have familiarity and comfort that they would not have with a corporate-issued device; the increase in productivity is intangible but evident.

Above all, EMM allows employees to complete business operations at any time and from any location using devices they are familiar with.

## 4

### Mobile Content Management

This critical tool enables users to securely and efficiently access information on their mobile devices. Each mobile device has a secure container in which to store critical data. It also supports content push, which is a push-based document delivery system that generates notifications for new files and expiration dates.

Mobile content management also adds another layer of security to your enterprise by securing data traffic flows and documentation exchanges to and from devices.

# What Makes Mobile Data Management Critical For Enterprises Today?

---

The primary goal of enterprise MDM, also known as mobile device management, is to enable businesses to focus on increasing employee productivity by enabling them to access corporate data on the move via company or personally owned mobile devices. MDM solutions can help in achieving this in a seamless and straightforward manner.

Although features vary between different MDM solutions, some capabilities are universal. These include the following:

1

## Device Inventory

MDM software captures different hardware and software data on devices, allowing businesses to manage and track company-owned and BYOD devices.

2

## Restrictions and Configurations

The ability to set up devices remotely is one of the most important features of MDM. Companies can easily ensure data security and compliance while still providing staff with the tools they require, thanks to numerous configuration and restriction options available with MDM.

3

## Application and Content Management

The ability to set up devices remotely is one of the most important features of MDM. Companies can easily ensure data security and compliance while still providing staff with the tools they require, thanks to numerous configuration and restriction options available with MDM.

## 4

## Device and Data Security

To protect both the device and the sensitive information on it, a variety of security measures can be taken. MDM enables businesses to implement disc encryption and strong passcodes, as well as establish secure containers that separate company and personal data. If a device is misplaced, it can be tracked and erased remotely.

## 5

## Mobile Content Management

Companies can use unified device rules to unify device management, improve efficiency, and stay in compliance with regulations. Companies can pre-define which settings, restrictions, and apps should be deployed on devices using different policies and then mass-deploy these rules to a group of devices.

## 6

## Automation

When an enterprise has a lot of devices to manage, automation proves useful. Through Samsung Knox Mobile Enrollment, Android Zero-Touch Enrollment, or Apple Business Manager / Apple School Manager, most MDM systems support automatic device enrollments.

When these built-in programs are linked to mobile device management software, businesses can utilize MDM to automatically deploy all essential settings and apps to devices based on corporate policies.

## 7

## Remote Maintenance

MDM allows devices to be updated and maintained remotely, eliminating the need for employees to see the IT department in person. All software upgrades and setups, device diagnostics, and troubleshooting can be done remotely, saving time and money for enterprises.





# Conclusion

---

As more enterprises see the need to protect their networks and maintain data compliance, the transition from MDM to EMM has been quite rapid.

With the introduction of new progressive technologies into the global market, the world is transitioning towards a new set of EMM solutions such as Unified Endpoint Management (UEM), which enables enterprises to manage all endpoints such as laptops, mobile phones, tablets, PCs, printers, and wearables using a single comprehensive EMM solution.

When talking about mobile device management, all three terms, MDM, EMM, and UEM, are often used interchangeably. Considering this, you would think that it does not matter which of the three is used, but it does.

Of the three mobility management solutions, MDM is the most common among end-users. MDM tools are used by many enterprises to provide flexibility to both the IT department and end-users. MDM allows IT administrators to securely manage all devices from a single interface, while employees can use whatever devices they want.

At MCMK, we provide an MDM solution that goes beyond traditional Mobile Device Management (MDM) to a data-centric approach. Our MDM solution can help enterprises by:

**Reducing time to Triage Problems**

**Identifying Root Causes instead of band-aid fixes**

**Allowing self-remediation of deployment issues**

**Uncovering off-the-radar issues  
(Network Issues, Battery, and Physical Abuse)**

Predicting operational downtime

Ensuring compliance and best practices


Improving fleet visibility to view status in real-time

Extending life of hardware and unnecessary service center returns

You can find out more about how our solution gives enterprises the power to support front line workers and help them to streamline their operations and reduce cost by visiting our website: <https://www.mcmk.io/> or by contacting us at the following:



**Melroy Coelho**  
VP MARKETING

-  [melroy.coelho@mcmk.io](mailto:melroy.coelho@mcmk.io)
-  1-647-993-4353
-  <http://www.mcmk.io>

