



**RAMA
UNIVERSITY**

www.ramauniversity.ac.in

FACULTY OF ENGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -33

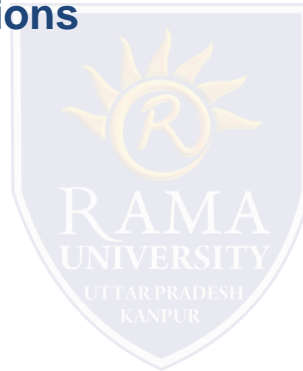
Umesh Kumar Gera

Assistant Professor

Computer Science & Engineering

OUTLINE

- **What is Mobile Device Management (MDM)?**
- **Why Mobile Device Management (MDM) is important?**
- **How mobile device management works?**
- **Advantages of using MDM solutions**
- **MCQ**
- **References**

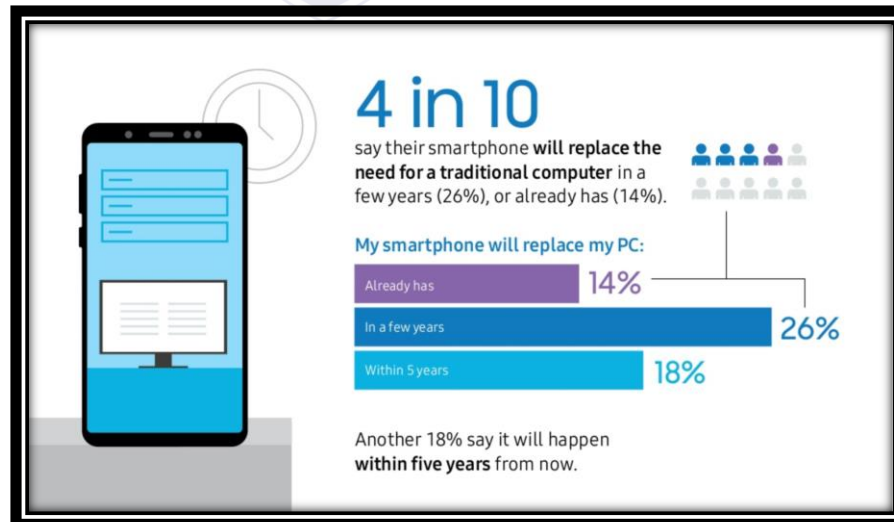


WHAT IS MOBILE DEVICE MANAGEMENT (MDM)?

What is Mobile Device Management (MDM)?

MDM or Mobile Device Management is a software application used for managing endpoints such as laptops, Smartphone's, tablets etc, in an enterprise. With more and more employees using one or all these devices, organizations across all shapes and sizes are now turning to mobile device management for enhanced data security and improved productivity.

Mobile device management (MDM), is the process of managing everything about a mobile device. MDM includes storing essential information about mobile devices, deciding which apps can be present on the devices, locating devices, and securing devices if lost or stolen. Many businesses use a third-party mobile device management software such as Mobile Device Manager Plus to manage mobile devices. Mobile Device Management has expanded its horizons to evolve into Enterprise Mobility Management (EMM).



WHAT IS MOBILE DEVICE MANAGEMENT (MDM)?

Why Mobile Device Management (MDM) is important?

Mobile Device Management (MDM) is important for an enterprises focusing on improving productivity of their employees by allowing them to access corporate data on the go using corporate or personally-owned mobile devices .

Ease of deployment

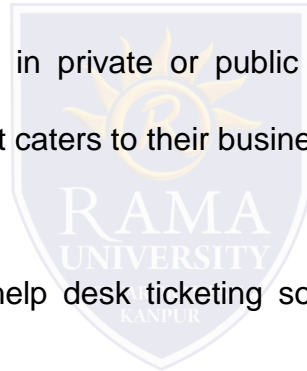
MDM solutions can be deployed on-premises or in private or public cloud environments, providing enterprises with the convenience of choosing a deployment method that caters to their business' specific needs.

Efficient Integrations

Many MDM solutions seamlessly integrate with help desk ticketing software, app development tools, and other business solutions.

Manage multiple device types

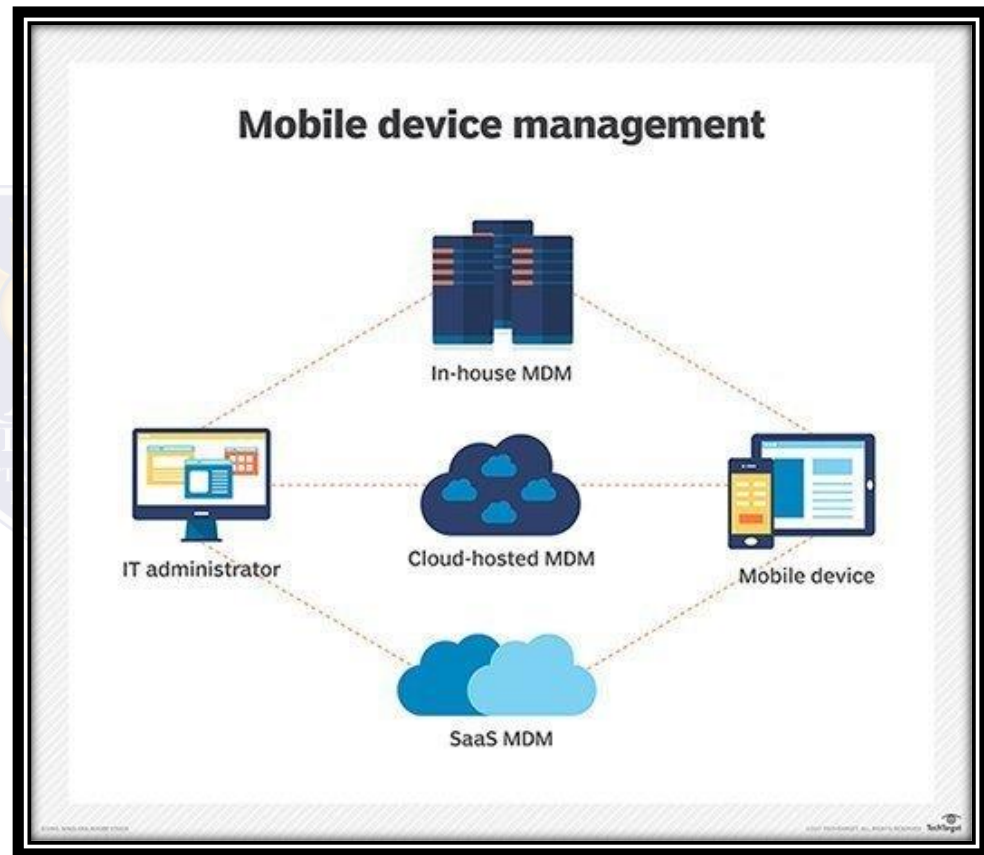
Simplified Mobile Device Management requires managing multiple OSs such as iOS, Android, Windows, macOS, tvOS, and Chrome OS, as well as multiple device types such as tablets, laptops, and smartphones.



WHAT IS MOBILE DEVICE MANAGEMENT (MDM)?

How mobile device management works?

Mobile Device Management (MDM) uses client-server architecture, with the devices acting as clients while MDM server remotely pushes configurations, apps, and policies managing the devices over-the-air (OTA). IT admins can remotely manage mobile endpoints such as laptops, tablets, and mobile phones via the MDM server. It leverages the notification services available to contact the managed devices



WHAT IS MOBILE DEVICE MANAGEMENT (MDM)?

Advantages of using MDM solutions

Organizations adopting mobility, prefer deploying MDM solutions since they simplify mobile device management and provide the following benefits:

Time-saving automations

Save time by automating repetitive tasks like configuring Wi-Fi settings on devices or asking users to install certain apps.

Improved efficiency

Configure tailor-made policies for your organization to improve workflow efficiency.

Increased productivity

Utilize a combination of policies like blacklisting non-enterprise apps during work hours to ensure employees are more productivity-focused.

Achieve compliance

Meet complex compliance standards like the GDPR, HIPAA, ISO, PCI, and CJIS in just a few clicks.

Enhanced security

Protect corporate data on mobile devices, and prevent it from being shared or saved on third-party services.

Remote management

Manage devices over-the-air (OTA) without requiring any intervention from the user and without affecting productivity.



MCQ

6. In mid-1981, the 1st virus for Apple computers with the name _____ came into existence.

- a) Apple I
- b) Apple II
- c) Apple III
- d) Apple Virus

7. The virus hides itself from getting detected by _____ different ways.

- a) 2
- b) 3
- c) 4
- d) 5

8. _____ infects the master boot record and it is challenging and a complex task to remove this virus.

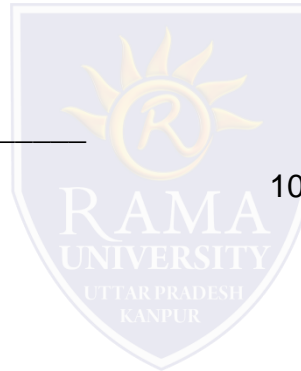
- a) Boot Sector Virus
- b) Polymorphic
- c) Multipartite
- d) Trojans

9. _____ gets installed & stays hidden in your computer's memory. It stays involved to the specific type of files which it infects.

- a) Boot Sector Virus
- b) Direct Action Virus
- c) Polymorphic Virus
- d) Multipartite Virus

10. Direct Action Virus is also known as _____

- a) Non-resident virus
- b) Boot Sector Virus
- c) Polymorphic Virus
- d) Multipartite Virus



REFERENCES

- ❑ <https://www.peerbits.com/blog/security-issues-in-developing-mobile-app.html>
- ❑ <https://www.softwaretestinghelp.com/mobile-app-security-testing-tools/>

