LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 32B

**A GUIDE TO MOBILE DEVICE MANAGEMENT**

**TASK 32B :**

* Can you provide a detailed technical explanation of Mobile Device Management (MDM), including its core functionalities and security capabilities?

[](https://www.esper.io/mdm)

Today, as more and more employees rely heavily on mobile devices to do their work, it is becoming increasingly standard practice for organizations of all sizes and in various industries to turn to Mobile Device Management to achieve enhanced data security and improved productivity. Around [67%](https://techjury.net/blog/byod/#:~:text=In%202021%20there%20are%2014.91%20billion%20personal%20mobile,set%20to%20grow%20to%2018.22%20billion%20by%202025.) of employees use their personal devices for work and a shocking [87%](https://techjury.net/blog/byod/#:~:text=In%202021%20there%20are%2014.91%20billion%20personal%20mobile,set%20to%20grow%20to%2018.22%20billion%20by%202025.) of businesses depend on their employee’s ability to access mobile business apps from their smartphones, so there is plenty of room for vulnerabilities in this area.

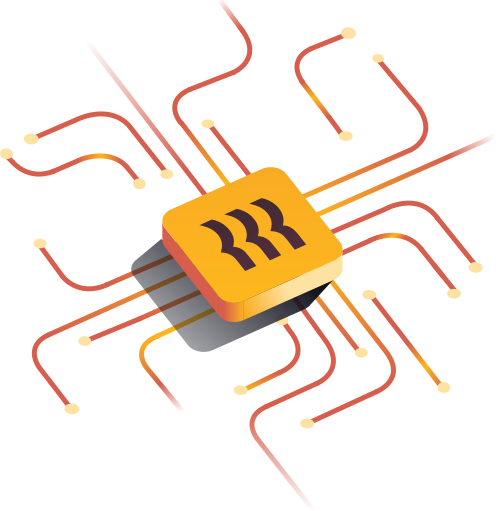
**What Is Mobile Device Management?**

Mobile Device Management (MDM) is a software tool for IT departments and administrators which is designed to support efforts to control and secure mobile devices such as laptops, smartphones, tablets and IoT devices. MDM solutions can either be hosted in the cloud or onsite, and they enable the management of all mobile endpoints, including personal and company devices. The aim of an MDM solution is to find the perfect balance between device management, user productivity and policy compliance.

Two key components of mobile device management are the MDM server (located in a data center) and an MDM agent (located on the mobile device). Whenever the IT admin wishes to configure and send out policies on any mobile device that’s on a company network, the admin must input the new policy on the MDM server’s management console. Then the server can push the change to the MDM agent, thereby implementing the command to the mobile device through the device’s own built-in APIs. This MDM server-agent connection can also be used by IT departments to deploy and control any apps on the managed devices.

There are a number of Mobile Device Management solutions on the market that provide organizations with the ability to monitor and manage mobile devices. Key features of these solutions include:

* Device tracking and inventory
* Mobile management and support
* Allow or deny applications
* Passcode enforcement
* Remote service management
* Alerts to signal users trying to use jailbreaking to bypass restrictions

[](https://www.rippling.com/blog/top-7-security-benefits-of-mobile-device-management-mdm-software)

**Advantages Of Using Mobile Device Management**

1. Security Enhancement: The same organization-wide protocols and security procedures that apply to on-premises PCs can extend to all devices, including personal smartphones.
2. Track Devices
3. Make Use of BYOD (bring your own device): With [87% of employees](https://techjury.net/blog/byod/) using their personal devices at work, a strong Bring Your Own Device (BYOD) policy is critical to maintaining security.

Using mobile devices to view business applications and platforms, join voice or video calls, and access business networks has become standard practice in recent years for many businesses.  Just one lost or stolen mobile device with access to your network could become a major security issue. Without the protection an MDM solution provides, a lost device could lead to private information (like customers’ credit card numbers or personal medical information) being compromised, potentially leading to costly fees and compliance violation-related lawsuits.