Enterprise security – MDM, MAM and EMM

With one in every four firms attacked by cybercrime in the recent years[1], security has never been more of an imperative for enterprises. Threats become more imminent when businesses want to gain benefits from the ongoing BYOD phenomenon. The use of privately owned mobile devices poses a fresh challenge to businesses, on how to allow employees use of their mobile devices while at work, without compromising or breaching corporate security. To ensure a high level of security, there are various mechanisms and systems available, like MDM, MAM and EMM.

1. **Mobile Device Management (MDM)** is a platform which ensures corporate security while employees and other third parties are accessing privileged information. It serves the dual purposes of ensuring employees' productivity while securing data, emails, networks, files and documents of a company. It is implemented either on-premises or on cloud.

The solution is leveraged for both, organisation-owned mobile devices or employees' personal devices under a 'bring your own device' (BYOD) program. MDM minimises supporting costs – associated with downtime and helps the business avoid risk by controlling and protecting data.

See Also: The Importance of Mobile Device Management for your Enterprise

2. **Mobile Application Management (MAM)** enables administrative control over mobile applications to manage and secure app data. It empowers a company's IT administrator to download secure applications, control access to corporate information and delete cached privileged data from mobile devices – either employees or business owned.

[1] https://www.ft.com/content/414740c4-db05-11e5-a72f-1e7744c66818

The BYOD phenomenon has also resulted in the development of Mobile Application Management (MAM). With a large number of personal and business owned devices flooding the workplace, it is important to secure the applications used in these devices.

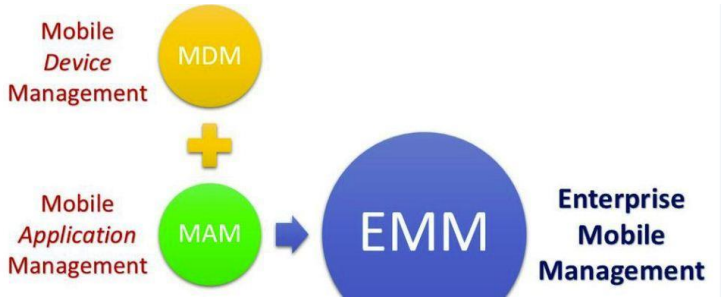
MAM's core functionality

- Downloading enterprise apps
- Updating and removing applications
- Monitoring application usage and performance
- Remotely wiping data when needed

Related Video: [Mobile Device Management (MDM) - Improve workforce productivity]

Enterprise Mobility Management (EMM) is a set of mechanisms which help protect against unauthorised access to business applications and corporate data on mobile devices. It gives comprehensive control to corporate IT administrators to enable password protection, encryption and remote deletion business data from lost or stolen devices. This is a centrally managed security feature enforced on mobile devices.

EMM is an umbrella solution used to ensure security of employees' mobile devices. Apart from securing the networks and devices, EMM also enhances employees' productivity by allotting them tools and features which enable their work on their devices.



The digital ecosystem is constantly expanding with new opportunities entering the enterprise landscape. But, the awareness of security threats and solutions to prevent such threats are at an all-time low. Security and management solutions such as MDM, MAM and EMM once deployed, can enable enterprises to capitalize on mobility and device technologies, while keeping control of device, application and information security.