13.3.11 Mobile Device Management Facts

Whether brought into the workplace as company-owned or privately-owned assets, mobile devices need to be managed, especially when they access sensitive organization data.

This lesson covers the following topics:

- Mobile device management
- Bring your own device

Mobile Device Management

The term Mobile Device Management (MDM) generally describes the policies and procedures used by an organization to maintain security and permissions on mobile devices. More specifically, MDM software is used by administrators to secure mobile devices and to enforce enterprise policies on the devices. MDM software usually offers a suite of features, including policy management, security management, inventory management, telecom service management, and mobile application management.

MDM software can mitigate bring your own device (BYOD) risks while taking advantage of the benefits. MDM software is typically deployed as a combination of an on-device application or agent that communicates with a backend server. The application receives policies and settings from the server to configure and control the mobile device.

The following table lists a few MDM security features that, as an ethical hacker, you will want to check:

Security Feature	Ethical Hacker Check
A policy to require the use of a passcode to access the device	Set this policy and check that the device requires a password.
A policy to lock the device	Make sure this lockout prevents unauthorized device access.
A remote wipe policy	Check that this policy completely removes data from the mobile device.
Root or jailbreak detection	Root or jailbreak a mobile device and then check that the MDM inventory shows this vulnerability.
Policies and inventory	Create other policies and ensure they are enforced by the MDM agent as they are received. Also, check the inventory data collected by the agent.
Alerts and monitoring	Create a violation on the mobile device and check that an alert is sent. Then check that the resource monitoring data is sent by examining the server-side reports.

The following table describes three MDMs:

MDM	Description
IBM's MaaS360	IBM's MaaS360 gives visibility and control over multiple mobile operating systems including iOS, macOS, Android, and Windows. This MDM is a good choice if you need to support legacy mobile systems. There is no hardware to install, and the user enrolls from the device. It also includes protection against malware and malicious websites.
Cisco Meraki	Cisco Meraki is a suite of products. One of these products is Endpoint Management. Endpoint Management is not strictly MDM software, since it also manages traditional desktops and other devices. However, it does have a focus on mobile devices and BYOD policies. Policies can be customized for user groups, require passcodes on devices, limit jailbroken devices to a guest network, provision software, and automatically revoke privileges if a device violates security policies.
Citrix Endpoint Management	Citrix Endpoint Management (formerly XenMobile) is also a unified endpoint management system that includes MDM as a primary feature. Along with tradition MDM features including BYOD, it also provides mobile app management and secures internally developed apps.

Bring-Your-Own-Device

The policy that allows employees to use their own computers and mobile devices for work purposes is called the bring-your-own-device policy (BYOD) policy. A BYOD policy encourages company employees not only to work on the device they choose, but the device they own for personal use.

The following table list a few BYOD benefits.

BYOD Benefit	Description

Increased productivity	Personal devices are always available to the user. The user becomes an expert in its use. Also, personal devices are more likely to be upgraded to keep up with the latest productivity technologies.
Employee satisfaction	Since the user purchases the mobile device, they choose the one that best fits their preferences and budget. In addition, they're probably happy that they don't have to carry around two devices, one for work, and one for personal activities.
Work flexibility	A single device that meets both professional and personal needs can be carried anywhere in the world. The user can do work at any location; they're not tied to the office. This mobility drives technology changes from a traditional client-server model to a cloud-centric strategy.
Lower costs	Companies may help users with the cost of a mobile device or offer more compensation to cover the purchase. But generally, the employee purchases the device and any data or telecom services.

The following table lists a few BYOD risks:

BYOD Risk	Description
Data leakage	While away from the office, a user might access company data via a public network. If these connections are not encrypted, it can lead to data leakage.
Confidential data exposure	As mobile devices synchronize with an organization's email and other cloud-connected apps, they download organization and confidential information. Losing a device or having it stolen can expose this information.
Improper disposal	Improperly disposing a device can leave old information, even financial data and credit-card details, vulnerable to being used for malicious purposes.
Number of different devices	Different devices have different levels of built-in security. This creates a challenge for the IT department and may even deter them from offering BYOD.
Mixing personal and corporate data	This is both a security issue for an organization and privacy issues for users.
Bypassing security policies	Security rules that are enforced only by a policy, and not by any automated means, can be overlooked or even maliciously exploited by disgruntled employees.