Security+ SY0-601

Module 10: Mobile

Table of Contents.

1 Mobile devices.

2 Connection methods and receivers.

3 Mobile device management.

4 Deployment models.

5 Enforcement and monitoring.

Learning objectives.

Upon completion of this module, you should be able to:

- List common mobile devices.
- Compare and contrast secure mobile network connections.
- Describe the systems for managing mobile devices and what features they offer. List and describe the security features of mobile devices.
- Define the mobile device deployment models available to an enterprise, along with their features and benefits.
- List the concerns created by introducing mobile devices on a network. Describe how these concerns can be monitored and supplemental requirements enforced.

Mobile devices.

MOBILE DEVICES.

Key concepts.

In this section, we will cover the following key concepts:

- Cell phones.
- Tablets.
- Phablets.
- Laptops.

MOBILE DEVICES.

Cell phones.

Cell phones are hand-held, portable devices using cellular data plans to connect to cell towers over the airwaves utilizing 2G, 3G, 4G, or 5G with a cellular telephone service provider. Cell phones can also connect to Wi-Fi using a local network or any wireless access point.

Apple iPhones are proprietary cell phones using the iOS operating system. Currently, iOS accounts for 54% of the North American cell phone market share.

Android is a popular Linux variation operating system that accounts for 46% of the North American cell phone market.

Globally, Android has 73% versus 27% for iOS.

MOBILE DEVICES.

Tablets.

- A tablet is a mobile device, typically larger than 7″. Tablets and cell phones share similar processor power and storage capabilities.
- Tablets typically have a smaller storage capacity than standard computers; they focus more on portability and function incorporated with a larger screen than cell phones while maximizing battery life.

MOBILE DEVICES.

Phablet.

A phablet is a combination of a cell phone and a tablet. Technically speaking, a cell phone with a screen size between 5.5″ and 7″ is considered a phablet. Phablets are typically smaller than full-size tablets but larger than a typical smartphone.

Most vendors offer cell phones with a 5.5” and 7” screen sizes. While technically labeled phablets, these large-form factor cell phones are becoming more prevalent throughout the technology world.

MOBILE DEVICES.

Laptops.

Laptops are highly portable, battery-operated small form factor computers. Laptops offer all-inclusive components such as an embedded keyboard, touchpad, function keys, and display. As computer processing power improves, laptops continue to take more powerful roles in the corporate world. Modern laptops are now capable of fully replacing common workstation desktop PCs.

It is important to remember that laptops are far more difficult to upgrade due to form factors and space limitations. There are far fewer FRUs (replaceable field units) and standardized components in laptops than desktop PCs.

MOBILE DEVICES.

Knowledge check.

Let’s apply what we have covered:

- What is the main difference between a tablet and a phablet?

Connection methods and receivers.

CONNECTION METHODS AND RECIEVERS.

Key concepts.

In this section, we will cover the following key concepts:

- Cellular.
- Wi-Fi.
- Bluetooth.
- NFC.
- Infrared / RFID.
- USB/USB On-The-Go.

CONNECTION METHODS AND RECIEVERS.

Cellular.

Cellular: Smartphones and some tablets (and phablets) can connect to the cell networks – 3G, 4G, and 5G – for phone calls and data access. Most of our connections utilize our home Wi-Fi once we are in range – if you wish to see what your cell coverage is inside of your home (3G, 4G, or 5G), simply disable the Wi-Fi option on your phone when you are home. Corporate apps and data must be secured against this cellular connection via policies and Mobile Device Management solutions.

CONNECTION METHODS AND RECIEVERS.

Wi-Fi.

- Wi-Fi: Most smartphone and some tablet (and phablet) connections are typically set up to utilize Wi-Fi connections when they are present and accessible. In the early days of cellular networks, the end users could possibly use up their allotted data plans and incur extra data use charges – these days, however, most cell plans have unlimited data usage plans, but the cell providers may throttle the connection speed if data usage is exceeded.
- IT personnel should scan for rogue hotspots that employees or unauthorized users may set up on the corporate network; these unauthorized access points could be utilized as attack vectors into your network or as an avenue for data exfiltration.

CONNECTION METHODS AND RECIEVERS.

Bluetooth.

Bluetooth: A short-range communication protocol popular for implementing personal area networks. The Bluetooth protocol operates at 2.4GHz in Wi-Fi's same unlicensed ISM frequency band. Ranges for Bluetooth are 10m - 100m.

Of interest to network administrators are the four items on the next two slides.

CONNECTION METHODS AND RECIEVERS.

Bluetooth.

- Connection – A central (master) can connect to a peripheral (slave). While the connection is active, the master and slave will communicate regularly at a determined interval.

- Bonding – Paired devices can be bonded. Bonds are created through a one-time process called pairing. When devices pair up, they share their addresses, names, and profiles and store them in memory. Bonded devices automatically establish a connection whenever they're close enough.

CONTINUED ON NEXT SLIDE >

CONNECTION METHODS AND RECIEVERS.

Bluetooth.

- Pairing – Devices that are initially connected can exchange encryption keys and encrypt the link; when they have, the link is secure, and they are paired. Pairing usually requires an authentication process where a user must validate the connection between devices. The flow of the authentication process varies and usually depends on the interface capabilities of one device or the other.
- Profiles – While Bluetooth specifications define how the technology works, profiles define how it's used. The profile(s) a Bluetooth device supports determine(s) what application it's geared towards. A hands-free Bluetooth headset, for example, would use a headset profile (HSP), while a Nintendo Wii Controller would implement the human interface device (HID) profile. For two Bluetooth devices to be compatible, they must support the same profiles.

CONNECTION METHODS AND RECIEVERS.

Near-Field Communication (NFC).

Near-field communication (NFC) is a wireless communication protocol that enables data transfer between two devices over a short distance (3-4 inches maximum).

NFC allows phones, tablets, laptops, and other devices to easily share data with other NFC-equipped devices; it evolved from radio frequency identification (RFID) technology. NFC is very much like RFID, but NFC is limited to communication within about 4 inches, so you must hold your phone close to the contactless reader if you're using payment services such as Apple Pay or Samsung Pay.

CONTINUED ON NEXT SLIDE >

CONNECTION METHODS AND RECIEVERS.

Near-Field Communication (NFC).

Most people consider NFC's small radius a major security benefit, and it's one reason why NFC has taken off as a secure alternative to credit cards. NFC can also transfer data such as videos, contact information, and photos between two NFC-enabled devices.

NFC has vulnerabilities that must be patched; if not, it can present a threat of the unauthorized transfer of data. Additionally, amplification attacks on the transaction communications are possible but difficult to achieve.

CONNECTION METHODS AND RECIEVERS.

Infrared (IR).

- Infrared (IR) is a short- and medium-range communication protocol using slightly longer electromagnetic wavelengths than red light.
- IR blasters are like remote control handsets, whereas IR sensors measure health information like heart rate and blood oxygen.
- IR sensors are used as proximity sensors – if a cell phone is held up to your ear, the cell phone that incorporates an IR sensor could temporarily disable the 'disconnect' button on your phone to keep a caller from accidentally ending the call.
- It is also used for health information – blood oxygen levels, heart rate, and perhaps even blood alcohol levels.

CONNECTION METHODS AND RECIEVERS.

Radio Frequency Identification (RFID).

- Radio Frequency Identification (RFID) is the wireless non-contact use of radiofrequency waves to transfer data.
- Tagging items with RFID tags allows users to automatically and uniquely identify and track inventory and assets.
- Administrators must be careful in the type of information they transfer using RFID, as RFID data can be intercepted by skimming. Simple asset management may not need to be encrypted, but other, more sensitive data should be.

CONNECTION METHODS AND RECIEVERS.

USB - USB OTG.

Mobile devices can be attached to a computer via the USB port (Apple devices will utilize a lightning-USB converter) and allow for those devices to access information on that computer's hard drive and also gain access to the corporate networks. This could facilitate data transfers and the sharing of videos and pictures or syncing information between devices.

USB On-The-Go (OTG) is a popular method for connecting devices in such a fashion. This type of connection could be used to infect the device they are connecting to – even the cable may be a vector for infecting another device (known as juice jacking); for that reason, you may get a prompt when you connect a device requiring you to authorize the connection prior to any data transfers taking place.

CONNECTION METHODS AND RECIEVERS.

P2P microwave.

A microwave is a wireless communication protocol used as a backhaul (or intermediate) link from a cell tower to the service provider's networks.

- Point-to-Point (P2P) microwave uses high gain (to highly directional) antennas to link two sites; this makes it difficult to eavesdrop on the signal. Point-to-point microwave wireless is the ideal alternative for business communication between two buildings or sites where a wired connection is either impossible, costly, or impractical.
- A point-to-point Ethernet bridge link facilitates a wireless data connection between two or more networks or buildings across distances up to 100 kilometers and at speeds of up to 1 Gbps.

CONNECTION METHODS AND RECIEVERS.

P2M microwave.

- Point-to-Multipoint (P2M) microwave uses smaller sectoral antennas linking multiple sites or subscriber nodes to a single hub. Each subscriber node is distinguished through the use of multiplexing.

- P2M can be used with mobile devices as well – Bluetooth may allow you to connect to multiple sources at the same time. Connecting a headset to a PC and a cell phone simultaneously would be an example of P2M.

CONNECTION METHODS AND RECIEVERS.

Global Positioning System (GPS).

- Global Positioning System (GPS): Mobile devices utilize GPS satellites orbiting the earth to triangulate your position on the ground; this enables turn-by-turn directions when you are driving, walking, or biking but also allows you to be tracked while doing so.
- GPS may also be susceptible to GPS spoofing and jamming using special equipment – this could lead to incorrect location information or be used to possibly defeat geofencing controls that you have incorporated into your network.

CONTINUED ON NEXT SLIDE >

CONNECTION METHODS AND RECIEVERS.

Global Positioning System (GPS).

- GPS can be used to find missing/lost/stolen devices, but it may also be used in geotagging, which will associate a picture with metadata information. If you do not wish such information to be tagged on your pictures, then you should ensure that you disable the GPS function on your device.

CONNECTION METHODS AND RECIEVERS.

Z-Wave.

Z-Wave is a wireless communication protocol used in IoT devices at 908.42 MHz in the US and 868.42 MHz throughout Europe. Z-Wave suffers from very little interference as the 800 to 900 band is well clear of the 2.4GHz and 5GHz used by Wi-Fi and other devices, appliances, and protocols. There is a limit of four hops between a controller device and an endpoint.

Z-Wave is a communication protocol designed for home automation and remote-control applications; it is a wireless protocol harnessing low-energy radio waves to help smart devices or appliances communicate successfully with one another.

AES 128 is mandatory for any device requesting Z-Wave certification, meaning security is ironclad, and a breach through encryption cracking is highly improbable.

Z-Wave is a wireless mesh network that can support up to 232 devices. While this is the practical limit, after 40 or 50 devices, you're likely to experience a little congestion. Communication takes place with the hub using the Z-Wave protocol.

CONNECTION METHODS AND RECIEVERS.

Zigbee.

Zigbee supports up to 65,000 nodes on a single network. However, because a company uses the protocol doesn't mean it will instantly play nice. For example, Philips Hue uses Zigbee to connect its bulbs, but that doesn't always mean you can add additional bulbs from a different manufacturer.

A typical example is when you have a Zigbee-enabled light bulb and a Zigbee-enabled light switch, and you want the light switch to control the light bulb. With Zigbee, the two devices — even if they are from different manufacturers — speak a common language, so there's no barrier to communication.

CONNECTION METHODS AND RECIEVERS.

ANT+.

ANT+ is a wireless technology created by Garmin to monitor sensor data in real-time or at intervals; it is mostly used in personal health equipment. It uses a P2P connection like Bluetooth.

One of the core differences between ANT+ and Bluetooth is that ANT+ trackers can communicate with multiple devices at once. Connecting/pairing one ANT+ device with another ANT+ tracker does not render that tracker invisible to other devices in the area.

Bike computers, otherwise known as cyclometers, cyclo computers, or cycling computers, commonly use ANT+ to transfer information.

CONNECTION METHODS AND RECIEVERS.

Knowledge check.

Let’s apply what we have covered:

- Differentiate between an IR blaster and an IR sensor.
- Describe the differences between Zigbee and Z-Wave.

Mobile device management.

MOBILE DEVICE MANAGEMENT.

Key concepts.

In this section, we will cover the following key concepts:

- MDM.
- MDM Security.
- Remote Wipe.
- Remote Lockout.
- Geofencing.
- Geolocation.
- Geotagging.
- Device Encryption.
- MAM.
- App Allow Listing (Whitelisting).
- Block Listing (Blacklisting).
- Upgrading.
- Messaging.
- EMM.
- SE Android.
- UEM.

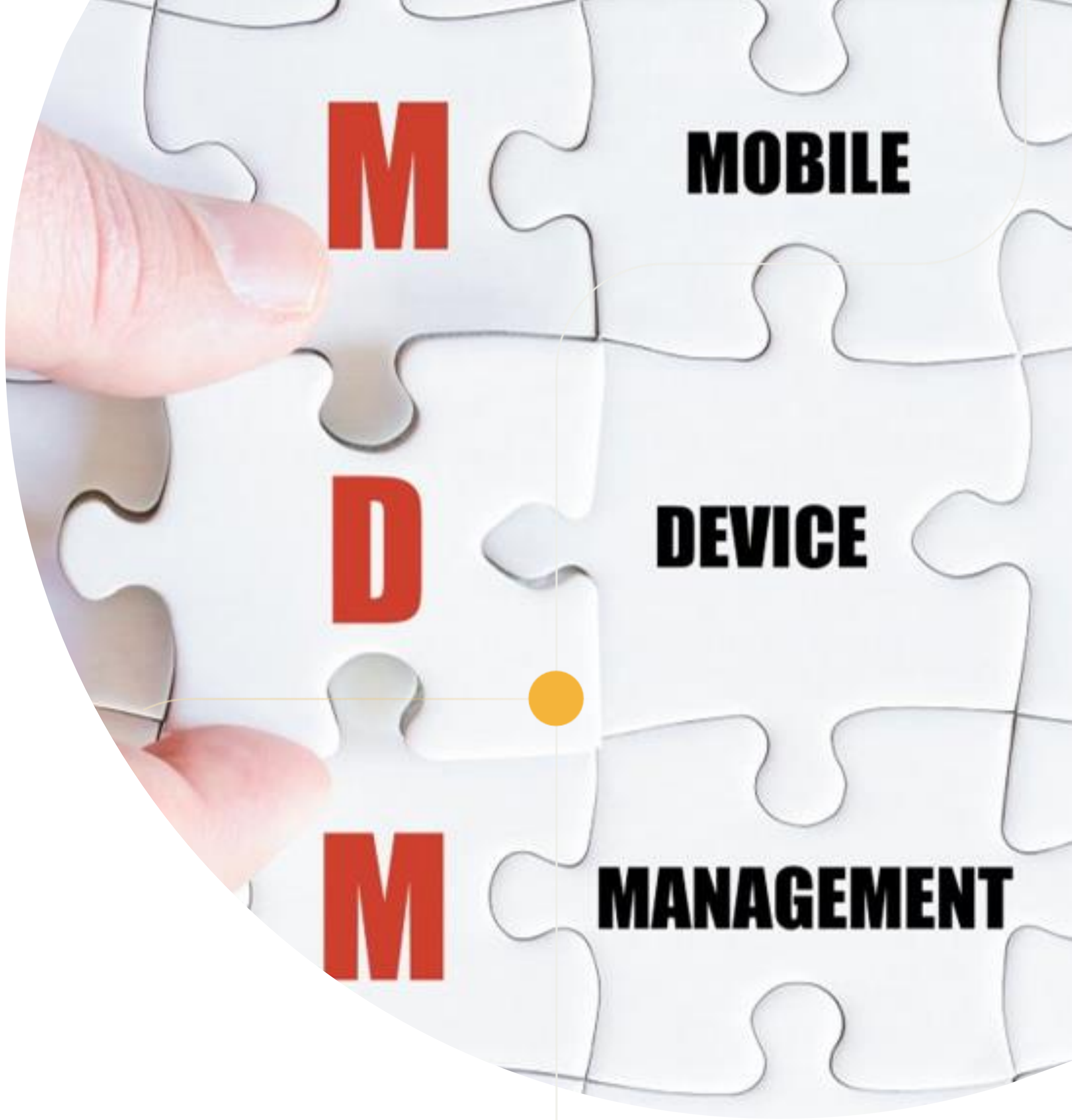
MOBILE DEVICE MANAGEMENT.

Mobile Device Management (MDM).

Mobile device management (MDM) describes the software and policies used to manage mobile devices in an enterprise environment.

Mobile devices offer a unique security challenge in an enterprise environment and must be addressed with specific mobile device policies.

IT professionals may encounter a plethora of different MDM software suites — common examples are the IBM MaaS360, Microsoft Intune, and Citrix Endpoint Management.



MOBILE DEVICE MANAGEMENT.

MDM security.

- Screen Locks – A policy that will lock a device for a period of time should a user incorrectly enter a password.

- Passwords and PINs are the basic authentication methods for logging on to a mobile device and into applications and sites accessed by the device. Password Managers can be unlocked using a password, PIN, or biometrics to facilitate an easier transfer of complex passwords into a login screen.

- Biometrics such as fingerprints and facial recognition are heavily used in authentication schemes on mobile devices. These can be used in conjunction with other authentication factors.

CONTINUED ON NEXT SLIDE >

MOBILE DEVICE MANAGEMENT.

MDM security.

- Context-aware authorization – When the device recognizes a "safe" or "trusted" location, such as the user's home or vehicle, and disables screen locks.

- Containerization and storage segmentation are methods to isolate corporate applications or data on a BYOD device from the user's personal applications/data.

- MicroSD HSM is a hardware security module placed into a MicroSD to securely store cryptographic keys. This means you can share the HSM between devices capable of using a MicroSD card.

MOBILE DEVICE MANAGEMENT.

Remote wipe.

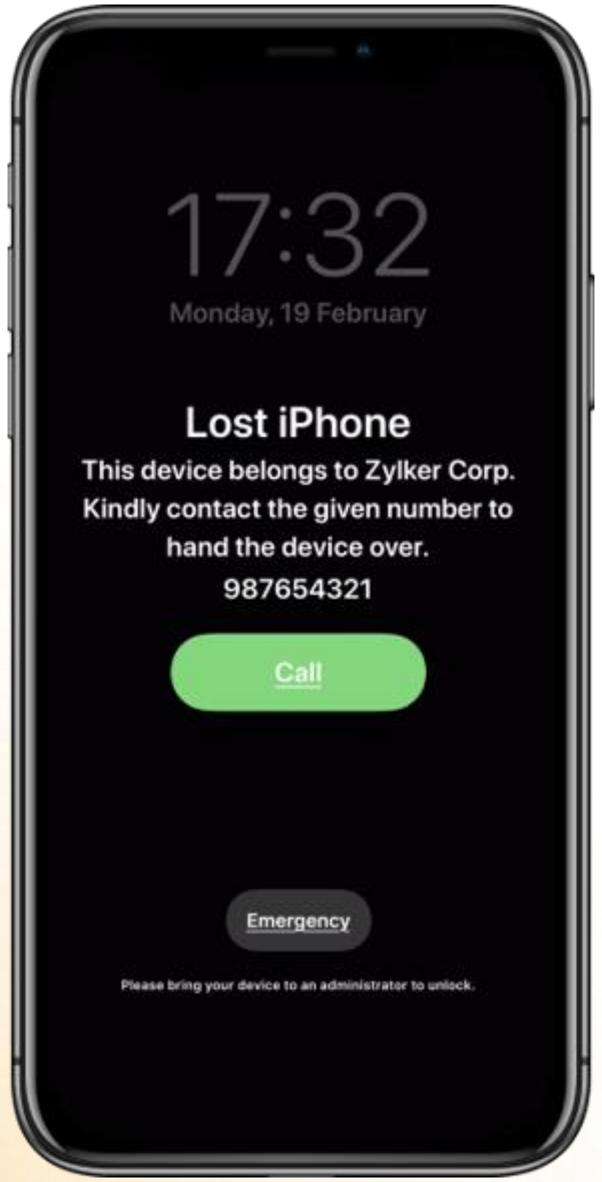
Remote wipe is a process to remove data from a compromised or lost phone, laptop, or desktop when the device is no longer in your possession. Consider remote wipe a device kill switch, erasing all data on the device.

MDM (Mobile Device Management) typically offers network policies on devices that require remote wipes to be enabled.

This includes BYOD devices. Policies involving remote wipes will be outlined in the MDM documentation.

MOBILE DEVICE MANAGEMENT.

Remote lockout.



17:32

Monday, 19 February

Lost iPhone

This device belongs to Zylker Corp. Kindly contact the given number to hand the device over.

987654321

Please bring your device to an administrator to unlock.

- If a device is lost or stolen, a remote lockout will allow someone to lock the device without having physical access to the device.
- This includes administrators and BYOD devices. Policies involving remote lockout will be outlined in the MDM documentation.

MOBILE DEVICE MANAGEMENT.

Geofencing.

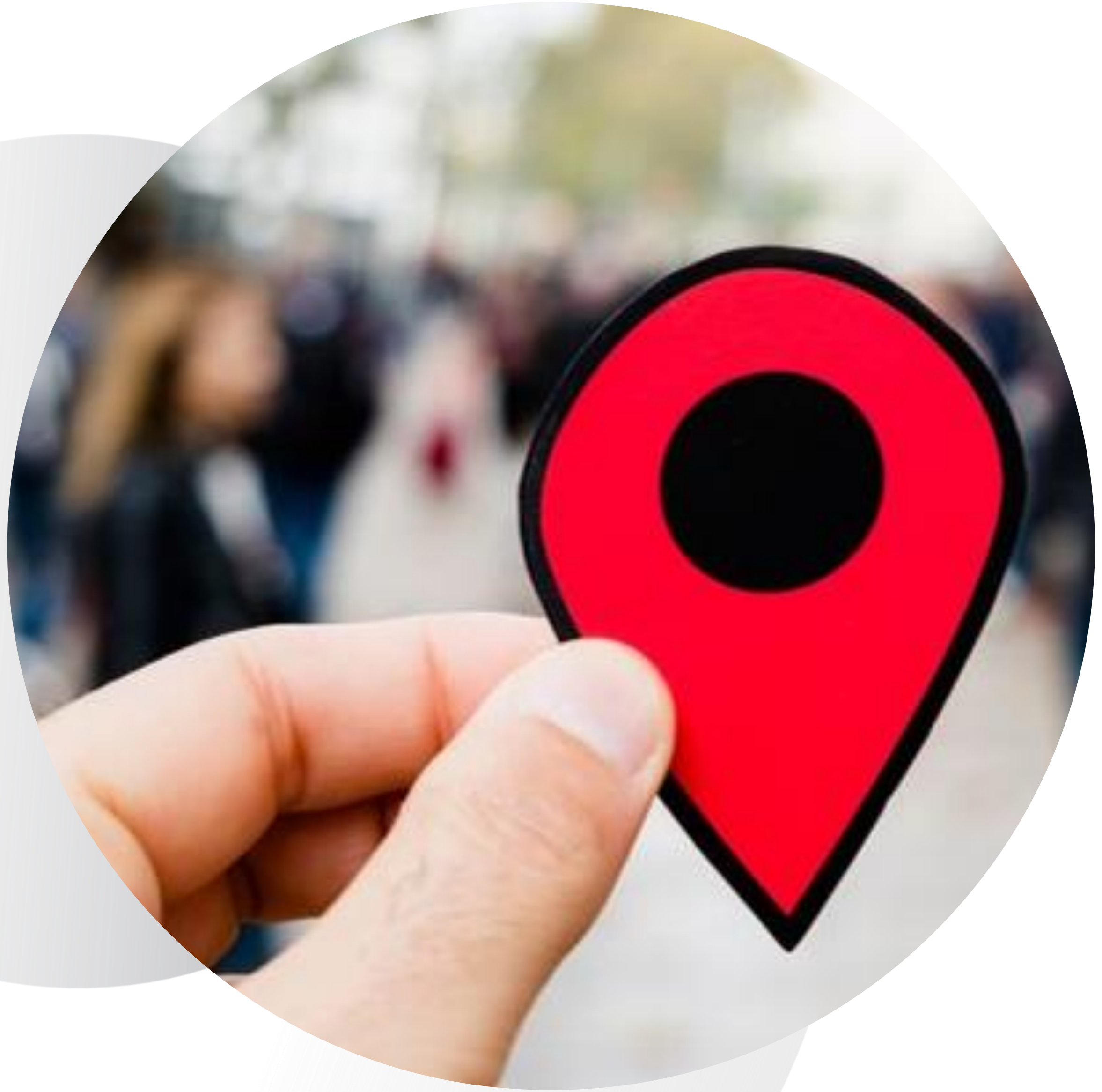
Geofencing is a method for creating a virtual fence around a physical location. Many apps and smart devices will allow the configuration of geofencing to improve functionality and, in some cases, remove functionality; it may be used to disable your portable device's camera and/or microphone.

Security is also improved – corporate data may ONLY be visible if you are inside the building or attached to the corporate network; if one is outside the boundaries of this "fence," no access is possible, further protecting the data.

Many applications and smart devices use geofencing. A very common example is geofencing with smart thermostats in homes: modern smart thermostats are controlled by an application that will use a geofence to alter temperature when the user is within a certain range of the house.

MOBILE DEVICE MANAGEMENT.

Geolocation.

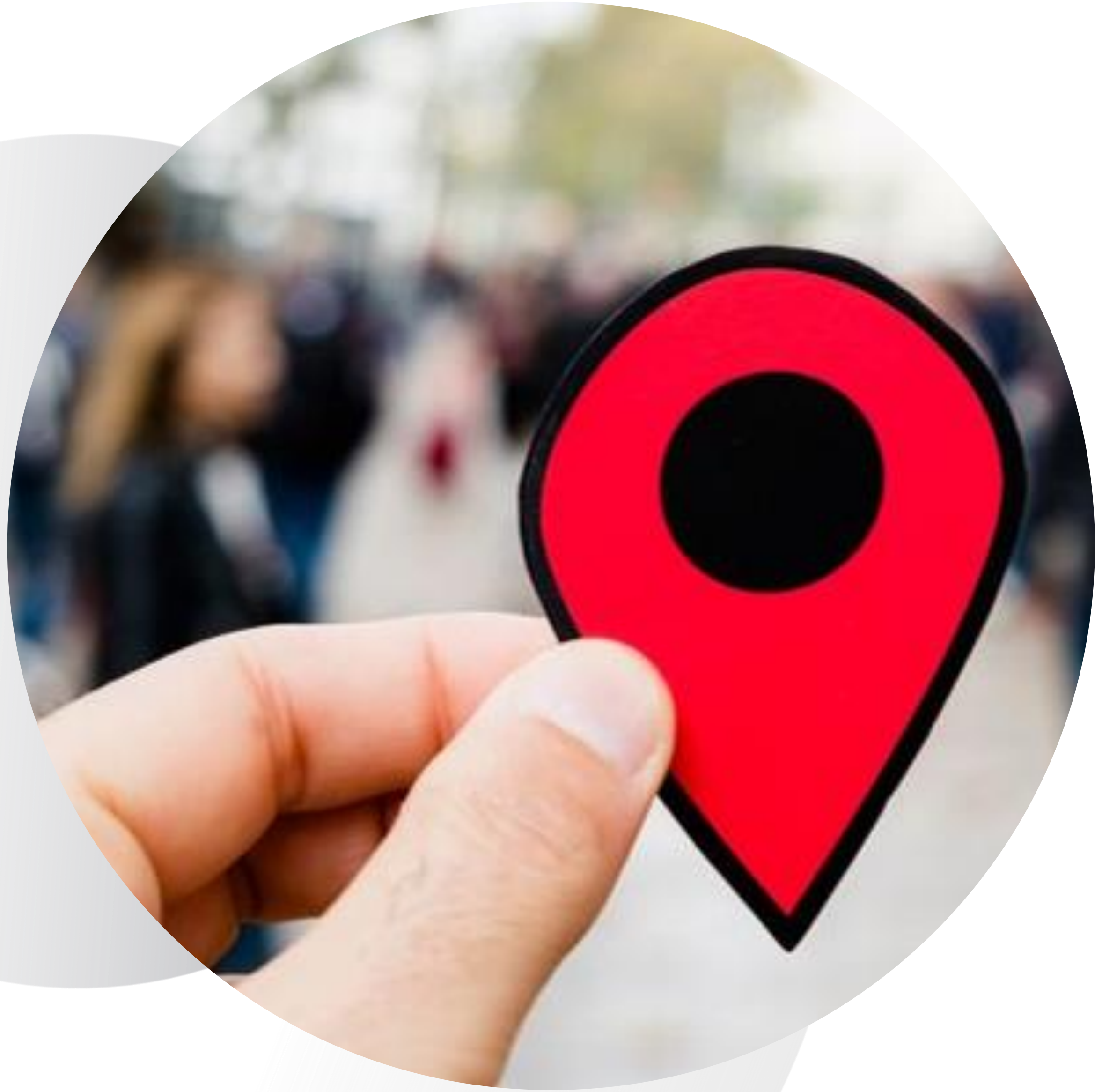


- Geolocation is a method for identifying the physical location of a device based on GPS or IPS.
- GPS (Global Positioning System) uses satellites to pinpoint your location. IPS (Indoor Positioning System) can use either wireless access points to triangulate your position or IP location services to roughly identify your position based on your IP address.

CONTINUED ON NEXT SLIDE >

MOBILE DEVICE MANAGEMENT.

Geolocation.



- Geolocation is a simple term to describe the process of using GPS to confirm a physical location. Geolocation can be tracked to determine if an impossible travel time or risky login policy violation has occurred; for example, if a user is in NYC at noon and then San Francisco at 1:00 PM.
- Geolocation may be incorporated into an authentication service to determine if the location is appropriate to allow access.

MOBILE DEVICE MANAGEMENT.

Geotagging.

Geotagging adds location metadata to files or devices. It describes location-based tagging (longitude and latitude of where and when a particular picture was taken).

Many users find this information helpful; however, it may collect more information than most users are aware of, presenting another potential security and/or privacy issue.

MOBILE DEVICE MANAGEMENT.

Device encryption.

Device encryption involves encrypting all data held on a device. Be sure not to confuse specific full-device encryption with other encryption technologies, such as EFS.

All data on a device is encrypted and protected. Full device encryption policies will be clearly defined in a documented MDM policy.

Device encryption can be helpful in wiping a device. If the decryption key is destroyed, the data is unrecoverable.

Don’t forget to encrypt external media such as MicroSD cards.

MOBILE DEVICE MANAGEMENT.

Mobile Application management (MAM).

- Mobile Application Management (MAM) is a set of application-specific policies on an enterprise network. Vulnerabilities are easier to mitigate if all applications are controlled on a network.
- There will be many layers of access control and mobile device management in secure environments.
- Mobile application management goes one step further by whitelisting acceptable, trusted applications.

MOBILE DEVICE MANAGEMENT.

Application whitelisting.

Application whitelisting is a policy that only allows approved programs to be installed.

You can only run authorized programs, applications, and processes on the "allow" list. Application whitelisting is very restrictive and is commonly implemented in very secure environments.

MOBILE DEVICE MANAGEMENT.

Application blacklisting.

Application blacklisting is a policy that blocks specific applications from being installed on a device.

You can install any programs, applications, or processes if it does not appear on the "block" list. The blacklisting of an application is a specific filter implemented to mitigate a vulnerability presented by a specific program.

MOBILE DEVICE MANAGEMENT.

Upgrading.

Firmware over-the-air (OTA) updates: Upgrades to mobile devices operating systems and applications are made wirelessly using OTA. Firmware for the radio modem, which uses its own real-time operating system (RTOS), will piggyback on top of the regular OTA upgrades.

MOBILE DEVICE MANAGEMENT.

Messaging.

- Short Message Service (SMS) and Multimedia Messaging Service (MMS) provide the transmission of text messages.
- Rich communication services (RCS) applications such as iMessage and WhatsApp are platform-independent and will allow video chats and other rich media; each of these is susceptible to various attacks and must be updated on a regular basis.

MOBILE DEVICE MANAGEMENT.

Enterprise Mobility Management (EMM).

Enterprise Mobility Management (EMM) is a comprehensive solution for securing organizational data on mobile devices. This includes:

- Mobile Email Management (MEM)
- Mobile Threat Management (MTM)
- Mobile Application Management (MAM)
- Mobile Content Management (MCM), also referred to as Mobile Information Management (MIM)
- Mobile Device Management (MDM)

MOBILE DEVICE MANAGEMENT.

SE Android.

Security-Enhanced (SE) Android is a technology built into modern Android operating systems that prevent applications from using services or functions not defined as trusted.

MOBILE DEVICE MANAGEMENT.

Unified Endpoint Management (UEM).

Unified Endpoint Management (UEM) is a method for controlling mobile devices that allows an administrator to control any device and any resource from a single console.

MOBILE DEVICE MANAGEMENT.

Knowledge check.

Let's apply what we have covered:

- Describe the different solutions that comprise EMM.
- Differentiate geofencing, geotagging, and geolocation. Provide examples of each.

Deployment models.

DEPLOYMENT MODELS.

Key concepts.

In this section, we will cover the following key concepts:

- Bring Your Own Device (BYOD).
- Company Owned Business Only (COBO).
- Corporate Owned Personally Enabled (COPE).
- Choose Your Own Device (CYOD).

DEPLOYMENT MODELS.

Bring Your Own Device (BYOD).

- Bring Your Own Device (BYOD) describes a policy allowing users to enable their personal devices on an enterprise network.
- BYOD is most popular with employees; security personnel is the least excited about this model.

DEPLOYMENT MODELS.

Corporate Owned Personally Enabled (COPE).

Corporate-Owned Personally-Enabled (COPE) is a policy that offers employees the use of a company-owned device but allows for that device to be used for personal reasons within the AUP (Acceptable Use Policy).

The corporation owns the device, but you can search the web and check your personal email using the device if you are in line with the AUP.

DEPLOYMENT MODELS.

Choose Your Own Device (CYOD).

Choose Your Own Device (CYOD) is a model that allows the employee to choose from a predetermined list of acceptable devices the company has to offer.

DEPLOYMENT MODELS.

Company Owned Business Only (COBO).

Company-Owned Business Only (COBO) is a policy that restricts the use of company-owned devices to work functions only — no personal data or functions are accepted on COBO-governed models.

The company owns the device, which may only be used for business-related activities.

MOBILE DEVICE MANAGEMENT.

Knowledge check.

Let's apply what we have covered:

- Compare and contrast BYOD, CYOD, COPE, and COBO.

Enforcement and Monitoring.

ENFORCEMENT AND MONITORING.

Key concepts.

In this section, we will cover the following key concepts:

- Third-Party App Stores.
- Rooting.
- Jailbreaking.
- Sideloading.
- Carrier Unlocking.
- Camera Use.
- Microphone Use.
- USB OTG.
- Tethering and Hotspot.
- NAC.
- VDI.

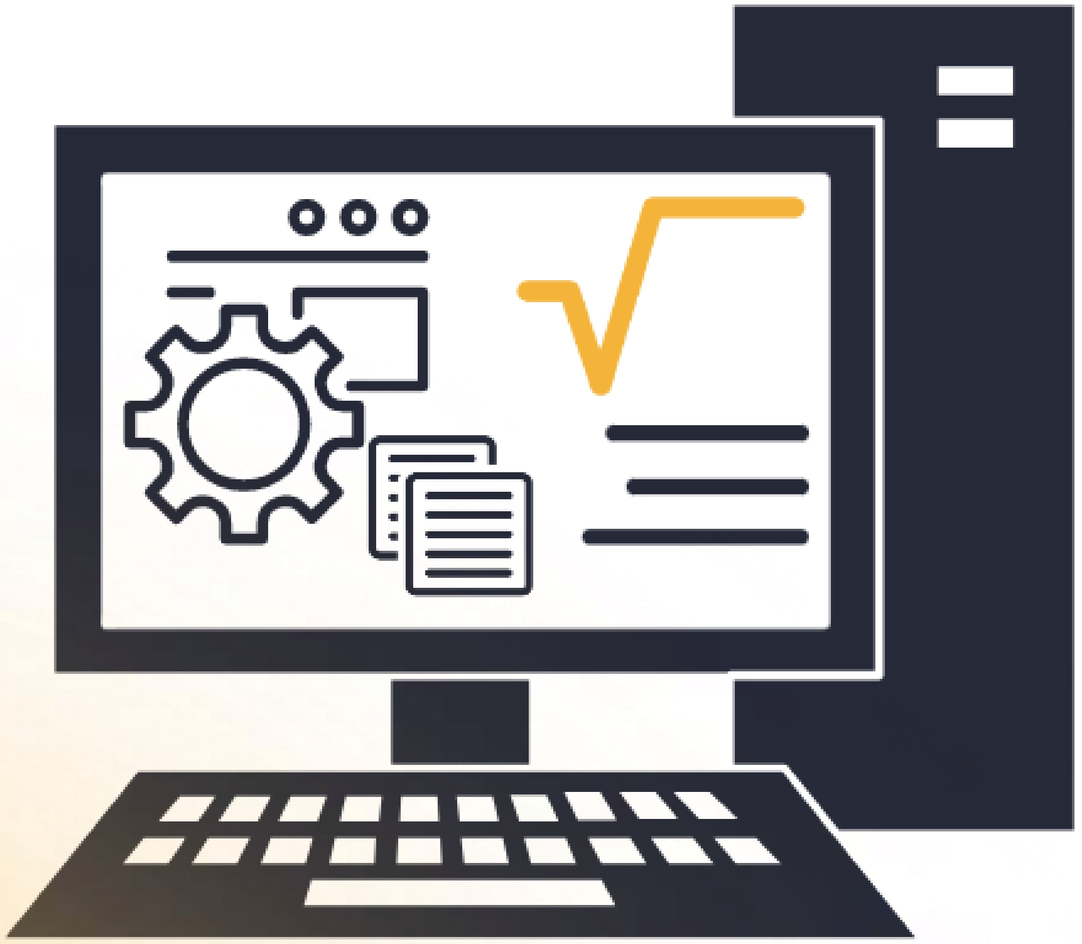
ENFORCEMENT AND MONITORING.

Third-party app store.

- Third-party app store – Inside of your corporations, you may wish to further limit what functionality is available for a mobile device. Once we allow a device onto our network, it must be contingent on what is available via those mobile connections – the App Store via Apple and the Play Store via Android.

ENFORCEMENT AND MONITORING.

Rooting.



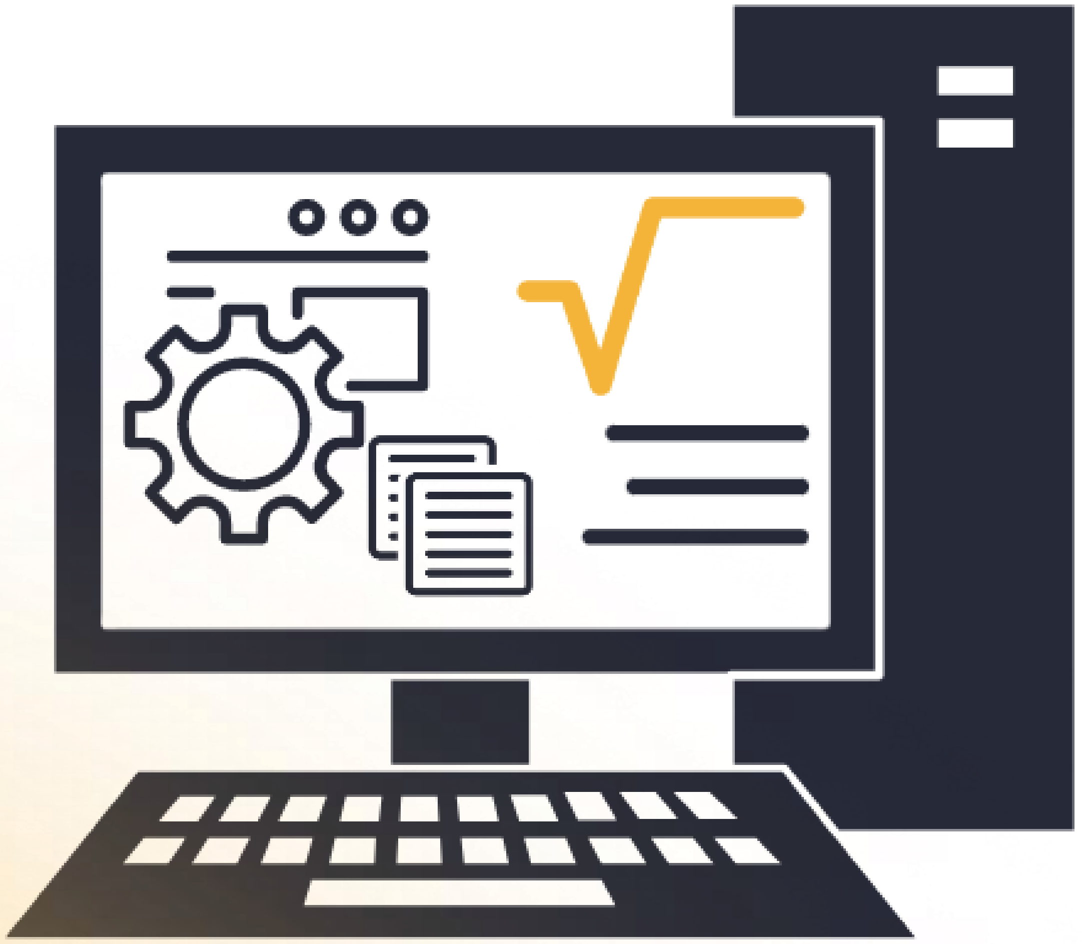
Rooting uses specialized software to force an Android device to allow for "root-level" (a Linux term for administrator) access. With a rooted Android device, limitations such as application install/uninstall, third-party app resources, and advanced settings are accessible.

Rooted devices offer users more functionality but tend to become vulnerabilities on secure networks. Rooting a device may also prevent the operating system security protocols from protecting the device in situations where malware is present.

CONTINUED ON NEXT SLIDE >

ENFORCEMENT AND MONITORING.

Rooting.



Custom firmware is a different Android OS being applied to the Android device in question.

ENFORCEMENT AND MONITORING.

Jailbreaking.

```
ness": 30,
Func": 3,
Test": true,
Write": true

"043B208C-1F83-42C6-802C-E0E35621C27C",
"MeshPhongMaterial",
```

Jailbreaking refers to manually altering the built-in restrictions of an Apple mobile device. Jailbreaking an iOS-powered device removes limitations on application sources and advanced settings but opens the device to vulnerabilities once protected by the native OS.

ENFORCEMENT AND MONITORING.

Side loading.

Side loading refers to downloading apps from locations other than the authorized App Store and Play Store — these could be from your own developers or independent developers. Lockdown what is allowed and not allowed.

ENFORCEMENT AND MONITORING.

Carrier unlocking.

Carrier unlocking involves removing the restrictions that lock your device into a single carrier/cellular vendor.

ENFORCEMENT AND MONITORING.

Camera use.

Camera use is a single aspect of the larger policy set of MDM. Depending on the organization, camera use may have specific rules when the mobile device is in a sensitive area.

AUP and EUM may dictate that your use of the camera or microphone will be disabled when on the corporate LAN or within the actual building.

The goal of each aspect of MDM is to protect data, making it an additional tool a corporation may use to protect its data.

ENFORCEMENT AND MONITORING.

Microphone use.

Microphone usage is similar to the camera policy; corporations may not allow end users access to their cameras to mitigate an end user taking screen prints of corporate data. Along those same lines, they may disable your ability to make recordings with your camera using MDM policies as well.

- AUP and EUM may dictate that your use of the camera or microphone will be disabled when on the corporate LAN or within the actual building.
- The goal of each aspect of MDM is to protect data, making it an additional tool a corporation may use to protect its data.

ENFORCEMENT AND MONITORING.

USB OTG.

Universal Serial Bus On-The-Go (USB OTG) allows a mobile device to be used as a host to utilize and access data on a USB device, such as a flash drive.

ENFORCEMENT AND MONITORING.

Tethering and hotspot.

- Tethering is the act of using a physical wire to connect a PC to a cell phone to access cellular data.
- The term hotspot describes a cell phone converting cellular data (3G, 4G, 4GLTE, 5G, etc.) into an 802.11 wireless access point.
- Tethering is typically a one-to-one setup where the connection is made over a cable. With hotspots, you could attach numerous devices to the corporate network.

CONTINUED ON NEXT SLIDE >

ENFORCEMENT AND MONITORING.

Network Access Control (NAC).

- Network Access Control (NAC) is a broad term that involves all policies and technologies that control who accesses a network. All networks will have some form of network access control.
- All the protocols, policies, and equipment authenticate and authorize network access at the device level.

ENFORCEMENT AND MONITORING.

Virtual Desktop Infrastructure (VDI).

- Virtual Desktop Infrastructure (VDI) is a way to provision a desktop OS to a mobile device.
- This is accomplished by either running a VDI client (application) on a mobile device or by connecting to an HTML5 solution — the latter is referred to as clientless.

MOBILE DEVICE MANAGEMENT.

Knowledge check.

Let's apply what we have covered:

- What are the different uses for tethering versus hotspots?
- Describe how VDI works.

End of Module.

For additional practice, please complete all associated self-study activities and labs.