

EC-Council

CCT

Certified Cybersecurity Technician

Module - 12

Mobile Device Security

This page is intentionally left blank.



Module Objectives

- 1 Understanding Various Mobile Device Connection Methods
- 2 Understanding the Concepts of Mobile Device Management
- 3 Understanding Common Mobile Usage Policies in Enterprises
- 4 Understand the Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
- 5 Understanding Enterprise-level Mobile Security Management Solutions
- 6 Understanding General Security Guidelines and Best Practices for Mobile Platforms

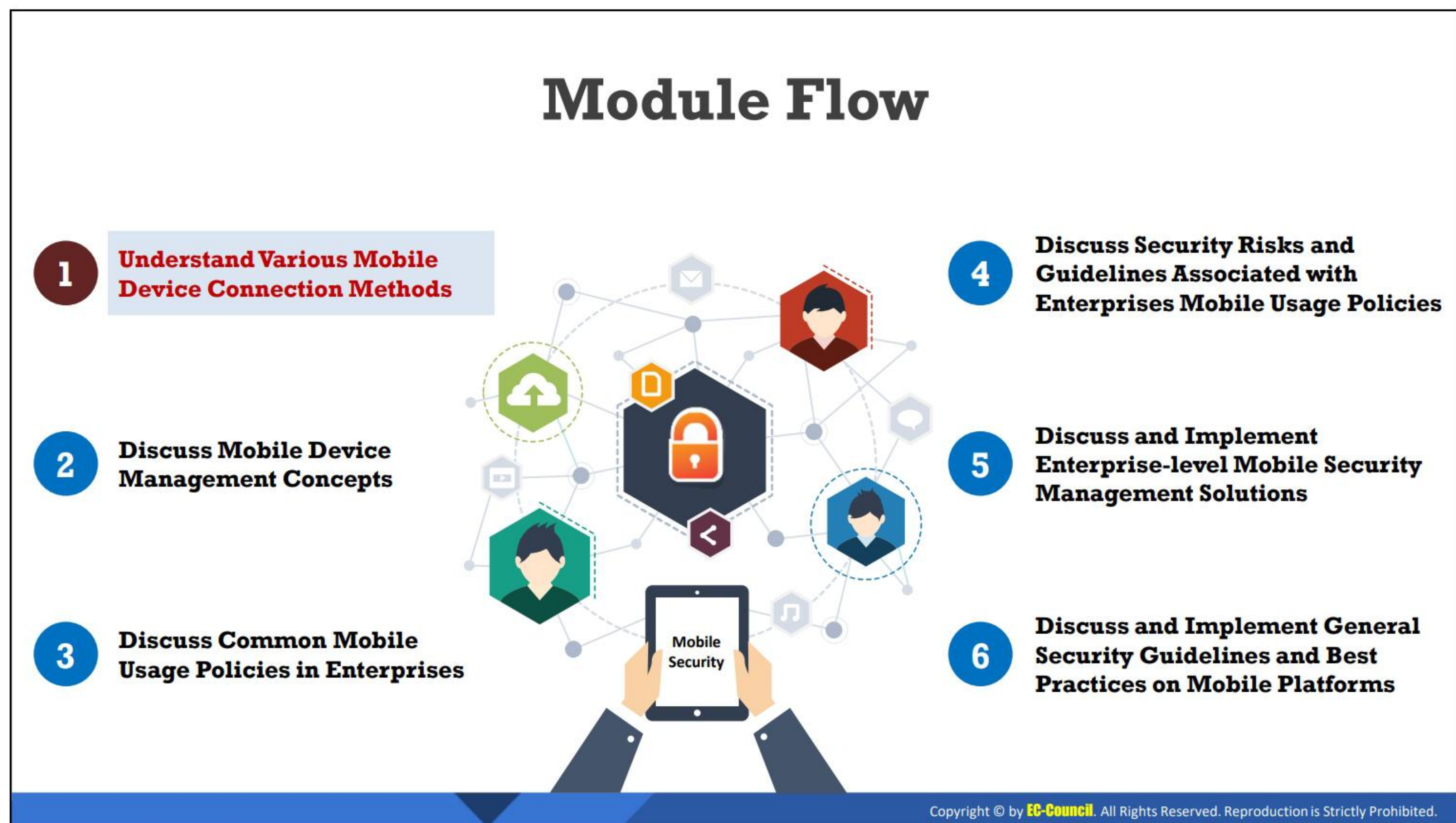
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

With the introduction of mobile phones in enterprises, enterprise security has become more complex. Enterprise mobile security has become a major challenge for organizations. Therefore, it is important for organizations to address these security concerns to effectively manage the security of mobile devices.

At the end of this module, you will be able to do the following:

- Understand various mobile device connection methods
- Understand the concepts of mobile device management
- Understand common mobile usage policies in enterprises
- Understand the security risks and guidelines associated with enterprise mobile usage policies
- Understand enterprise-level mobile security management solutions
- Explain general security guidelines and best practices for mobile platforms



Understand Various Mobile Device Connection Methods

To secure mobile devices from various cyber-attacks, security professionals should be aware of different connection methods involved in mobile communications. They should also understand how devices gain access to the network and share their resources with other devices. There are many ways in which mobile networks can be connected; therefore, it is important for security professionals to be aware of the security concerns associated with each connection method and how to protect mobile networks from malicious intents. This section discusses various mobile device connection methods.

Mobile Device Connection Methods



Near-field Communication (NFC)

- It employs **electromagnetic induction** to enable communication between the devices connected within a range of 10 cm

Satellite Communication (Satcom)

- It is an **artificial geostationary satellite** that provides services across the globe, but it is much slower and more expensive than other technologies

Cellular Communication

- It is based on a **single network tower** that serves devices located within a specific radius

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Connection Methods (Cont'd)



ANT

It is a **wireless sensor protocol** that enables communication between sensors and their controllers



Universal Serial Bus (USB)

It enables **wired communication** for devices. It can be used for power supply and serial data transmission between devices



Global Positioning System (GPS)

It is a **radio navigation** and **positioning system** based on satellite communication. It provides information related to geolocation and timing irrespective of weather conditions on the Earth



Infrared (IR)

It is a wireless technology for transferring data between two devices in the digital form within a **short range** of up to 5 m



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Connection Methods (Cont'd)



Wi-Fi

It is a common **wireless technology** used in homes and office buildings to connect local devices



Bluetooth

It is a **short-range, high-speed, and low-power** wireless technology that enables communication between devices connected within the Bluetooth range



5G Cellular (Mobile) Communication

It is a **broadband cellular network** that operates at high bandwidth with low latency and provides high-speed data downloads

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Connection Methods (Cont'd)

Point-to-point (P2P) Connection



- It enables **secure communication** between two mobile devices without data encryption because they are connected through fixed paths without the interference of other devices

Point-to-multipoint Connection



- It allows **one-to-many connections** by providing multiple paths from a single location to several other locations

Radio-frequency Identification (RFID)



- It works on the basis of **radio-frequency technology**, which identifies a person or object using their tags (unique labels)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Connection Methods

The following are some commonly used mobile connection methods.

- **Near-field communication (NFC):** NFC covers very short distances using RFID technology. It employs electromagnetic induction to enable communication between devices connected within a range of 10 cm. The NFC chip embedded within a mobile device can read RFID tags and also be used to establish Bluetooth connections with

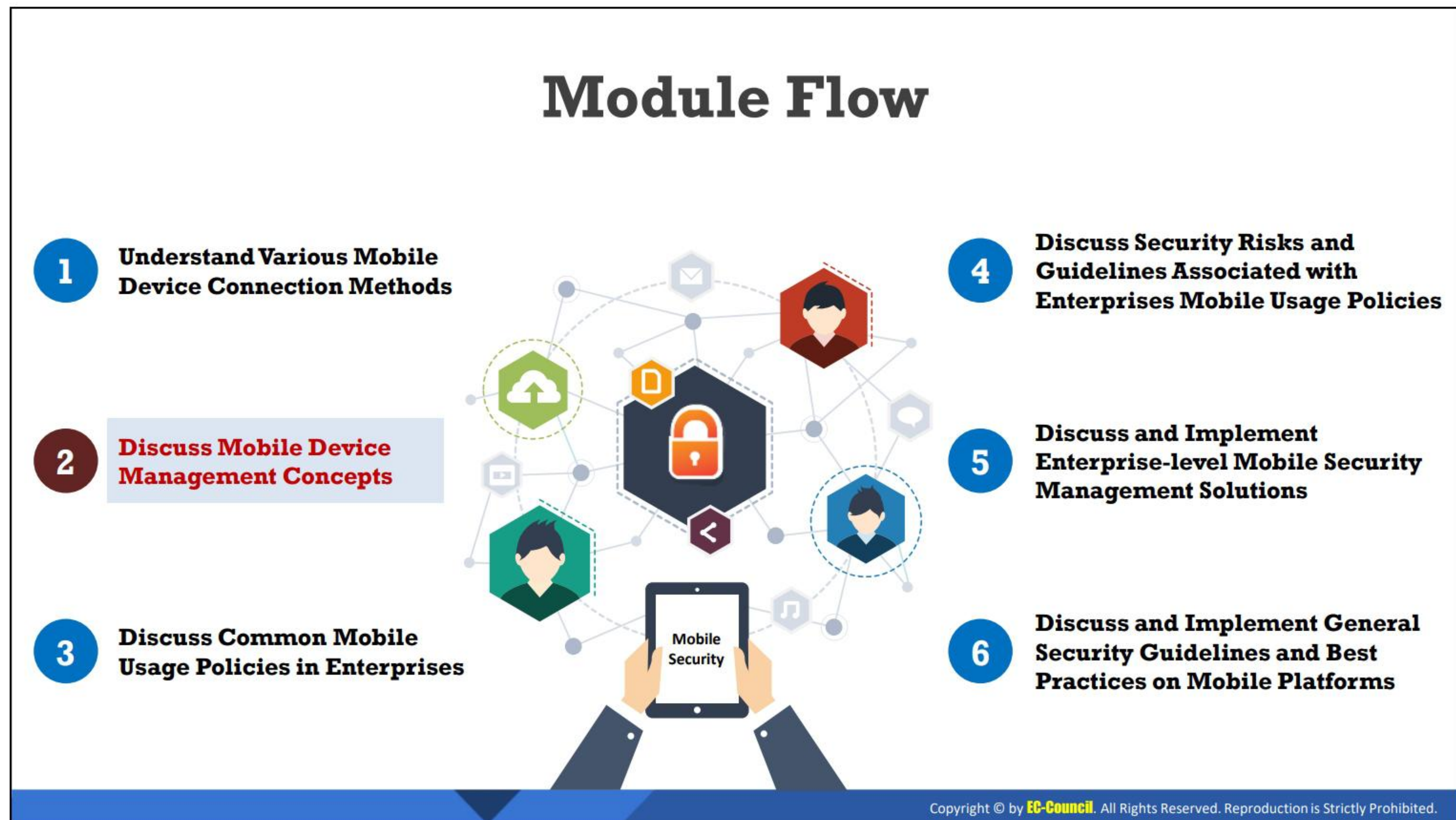
nearby devices to exchange information such as images and contact lists. Although it allows a very narrow communication range, an attacker with a specialized antenna can intercept and capture the data by jamming the traffic. This security issue may result from the improper configuration of NFC and non-encrypted data transmission. An attacker may craft and send malicious RFID tags, forcing the mobile user to visit a fake website in the browser. Furthermore, an attacker may perform a DoS attack by creating enormous RF signals to corrupt the NFC data being transmitted in that area.

- **Satellite communication (Satcom):** Satcom is an artificial geostationary satellite that provides services across the globe, but it is much slower and more expensive than other technologies. There are many technologies that utilize satellite technology; some employ a connection to geostationary satellites, while others connect to satellites that revolve around the Earth in a low orbit, through which voice and data can be transmitted. The technology also has security concerns such as remote code execution and OS vulnerabilities.
- **Cellular communication:** Cellular communication is based on a single network tower that serves devices located within a specific radius. They are installed in urban, suburban, and rural areas and cover a large distance. Mobile devices contain built-in antennas, which enable the device to communicate via a cellular network. Security concerns with cellular networks include location tracking, exploiting SS7 vulnerability, traffic monitoring, denial-of-service (DoS) attacks, channel jamming attacks, and illegitimate access.
- **ANT:** ANT is a wireless sensor protocol that enables communication between sensors and their controllers. This technology is used in Internet of Things (IoT) devices such as heart-rate or fitness monitoring equipment. It is not a Bluetooth or 802.11 wireless technology and has its own set of protocols developed for low-powered devices. It is susceptible to DoS or jamming attacks, and attackers can capture data in transit.
- **Universal Serial Bus (USB):** USB enables wired communication for devices. It can be used for power supply and serial data transmission between devices. It is also designed to enable hot-swapping and improve plug-and-play features. USB ports are commonly used in mobile devices for both data transmission and power supply. It is relatively more secure than other connection methods, but disgruntled employees can use a USB device to exfiltrate data from the organization's local network.
- **Global Positioning System (GPS):** GPS is a radio navigation and positioning system based on satellite communication. It provides information related to geolocation and timing irrespective of weather conditions on the Earth. Devices do not need to pass any data to satellites to establish a GPS connection; they only need to receive the signals from four or more satellites out of 28 to estimate their location. As the initial position fixing is slow with GPS, smart devices use assisted GPS (A-GPS), which uses external data sources for improved position fixing and faster location tracing. Security concerns with this technology include the fact that GPS signals can be intercepted and tampered with using specially designed GPS jammers.

- **Infrared (IR):** IR is a wireless technology for transferring data between two devices in the digital form within a short range of up to 5 m. It works only when there is no physical blockage or obstacle between the two devices. It is a type of networking feature integrated within devices such as tablets and smartphones that allows them to manage IR devices. It can also be used to transfer files between devices. Any device with IR accessibility can be managed using the IR feature of a mobile device. Furthermore, IR is used in modern wearable technology to enable devices to emulate the features of a remote control to operate devices such as smart TVs and detect health information such as oxygen levels. IR can also be used to perform IR therapy for treating chronic and acute pains.
- **Wi-Fi:** A Wi-Fi network connects devices within a limited (Wi-Fi enabled) area with high bandwidth. It covers a shorter distance than a cellular network and is a common wireless technology used in homes and office buildings to connect local devices. Furthermore, a mobile device can share its Internet service with other devices by using the hotspot tethering feature based on Wi-Fi technology. If clients do not use an encrypted channel or the channel does not use an appropriate protocol, then the clients can be targeted by man-in-the-middle (MITM) attacks, through which attackers can sniff the traffic between two communicating devices. As the technology uses a set of 5 or 2.5 GHz frequencies, it can also be vulnerable to DoS attacks and frequency interferences. Wi-Fi Direct is another Wi-Fi feature that enables peer-to-peer communication without any mediator such as router, but one of the connected devices in Wi-Fi Direct communication serves as a soft access point.
- **Bluetooth:** Bluetooth technology covers a longer distance than NFC. It is a short-range, high-speed, and low-power wireless technology that enables communication between devices connected within the Bluetooth range. When a device enables a Bluetooth connection, it sends “pairing” requests to a certain number of devices located within range, following which the corresponding device pairs with it using the device name and ID. It is mostly used in personal area networks (PANs). Conventional Bluetooth has a low data transfer rate. Therefore, with modern Wi-Fi technology, Wi-Fi connections are preferred for faster data transmission. Security concerns with Bluetooth technology include interception, eavesdropping, DoS attacks, transmission of viruses or worms, Bluesnarfing, and Bluejacking.
- **5G cellular (mobile) communication:** 5G or fifth-generation communication technology is a broadband cellular network that operates at high bandwidth with low latency and provides high-speed data downloads. Some of the applications of 5G include the automobile industry, public safety, and fixed wireless access. The technology is designed to support IoT devices. Security concerns with this technology are associated with its management complexity. Attackers may attempt to take advantage of the increased number of devices connected to a 5G network to compromise and use them as botnets to paralyze the network through DDoS attacks.
- **Point-to-point (P2P) connection:** A P2P connection enables secure communication between two mobile devices without data encryption because they are connected

through fixed paths without the interference of other devices. For example, in a scenario of mobile communication between two people, only the concerned device can hear the voice from the dialed device. Routing devices can also use this method to connect with each other by adopting the over-the-air encryption technique, which reduces the risk of eavesdropping.

- **Point-to-multipoint connection:** A point-to-multipoint (P2MP, PTMP, and PMP) connection allows one-to-many connections by providing multiple paths from a single location to several other locations. In this connection method, a central antenna broadcasts signals to multiple receiving antennas and devices through either time-division multiplexing (TDM) or frequency-division multiplexing (FDM) for bidirectional data transmission. One technology that uses PMP connections is Bluetooth, which can use the PMP method to connect one device with multiple devices such as headphones and media players. This type of connection does not provide high security or privacy, because the communication channel is broadcasted and shared.
- **Radio-frequency identification (RFID):** RFID works on the basis of radio-frequency technology, which identifies a person or object using their tags (unique labels). The tagging range can vary from a few centimeters to meters. RFID operates in the low-frequency (LF), high-frequency (HF), and ultra-high-frequency (UHF) bands. HF-RFID with a mobile device operates via servers by providing data history, data persistence, and data management. If the reader is located within the range of the tag, it generates an electromagnetic wave that activates the tag, thereby allowing the reader to gather information. RFID systems can be susceptible to attacks such as power analysis, reverse engineering, replay attacks, spoofing, sniffing, DoS, and cloning.



Discuss Mobile Device Management Concepts

This section discusses various mobile device management concepts.

Mobile Device Management (MDM)



MDM provides platforms for **over-the-air** or **wired distribution of applications, data** and **configuration settings** for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.



Mobile Application Management

- ❑ A software that is mostly used by IT admins to **control** and **secure organizational data**. It offers features such as the remote activation or deactivation of devices, remote wiping in case of theft or loss, etc.



Mobile Content Management

- ❑ A software that offers solutions to **safeguard the content** or data on the mobile devices. It provides features to store and deliver data, offer the required services, and permit employees to access the organizational data remotely



Context-aware Authentication

- ❑ It uses the contextual information of a user such as **geolocation**, **identity**, and **behavior** for enhancing data security decisions

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM) (Cont'd)

Mobile Email Management

It offers **secure access** to organizational email infrastructure and data on an employee's mobile devices

Enterprise Mobility Management

It consists of **tools** and **technologies** used in an organization to secure the data in employees' personal (BYOD) and organizational devices



Mobile Security Management

It involves **actions** and **precautionary steps** for securing the organizational data and mobile devices used by employees

Remote Wipe

It is a technique used for securing and protecting data from miscreants if a mobile device used by an employee was lost. This feature allows the administrator to send a command that can **erase all the device data**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.






Mobile Device Management (MDM) (Cont'd)



Screen Lock		It is a feature in mobile devices that is used to secure data and prevent illegal access by perpetrators
Passwords and PINs		It protects private data of the employee and confidential information of the organization stored on a mobile device
Biometrics		It is an advanced and unique security technology that utilizes an individual's physical attributes such as fingerprint, iris, face, voice , and behavior for verifying their identity
Push Notification Services		It is a messaging feature that originates from a server and enables the delivery of data or messages from an application to a mobile device without any explicit request from the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM) (Cont'd)

Geolocation <ul style="list-style-type: none">It is a technology that can identify the real-world geographical location of users or devices when connected to the Internet 	 Geofencing <ul style="list-style-type: none">A geofence is a virtual fence positioned at a specific location that interacts with mobile users whenever they cross the fenceIt helps marketers gather sensitive data and information about users' offline activities from the location data	Full Device Encryption <ul style="list-style-type: none">It is a security feature that can be used to encrypt all the information stored on any storage medium within a mobile device 	 Containerization <ul style="list-style-type: none">It is a technique in which all personal and organizational data are segregated on an employee's mobile device. It helps in improving the security of organizational data	OTA Updates <ul style="list-style-type: none">It is a new method of delivering updates for applications, firmware, and time-zone rules, as well as any other essential data, to a mobile device 
--	--	--	---	---

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM)

MDM provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on. It helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure,

monitor, manage, and support these devices. It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise.

Discussed below are various concepts related to mobile device management:

- **Mobile application management**

Mobile application management (MAM) is software that is mostly used by IT admins to control and secure organizational data. MAM offers features such as the remote activation or deactivation of devices, device registration in the organization, and remote wiping in case of theft or loss. These features are suitable for mobile devices that are used only for organizational purposes by the employees. For mobile devices that are used for both work and personal use, IT admins can implement and apply privacy policies on mobile applications by limiting organizational data sharing. They can also enable the partitioning of the applications used in the organization and personal data on the same mobile devices. MAM features also include software or application distribution to employees, license management, data encryption, configuration, and inventory management.

- **Mobile content management**

Mobile content management (MCM) is software that forms a part of mobile device management (MDM). MCM offers solutions to safeguard the content or data on the mobile devices used in an organization. It provides features to store and deliver data, offer the required services, and permit employees to access the organizational data remotely and at any time necessary. MCM ensures that unauthorized data access is restricted or blocked, thereby protecting the confidential data of the organization. It oversees critical data management, access to work documents, email management, and digital asset management. It can also encrypt confidential data and use any strong password technique for data transmission and data storage.

- **Context-aware authentication**

Context-aware authentication is a type of enhanced security technique that uses the contextual information of a user such as geolocation, identity, and behavior for enhancing data security decisions. It also uses the data about the user, requests made, connection, and location. All this data help in preventing malicious users from accessing the organizational data. This technique also allows employees to access the organizational network within the office perimeter and denies access when a device is connected to a public Wi-Fi network.

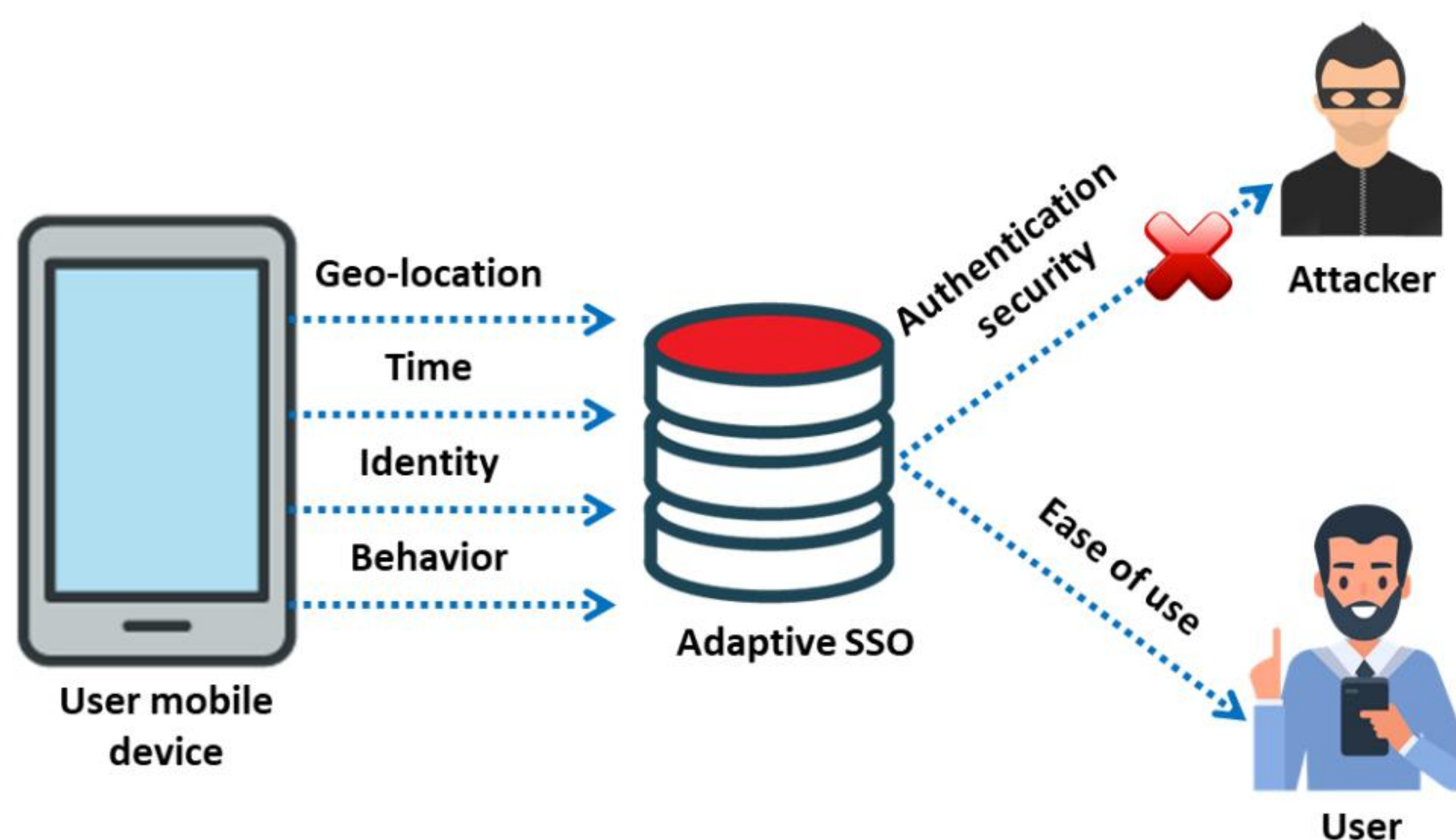


Figure 12.1: Context-aware authentication

- **Mobile email management**

Mobile email management (MEM) offers secure access to organizational email infrastructure and data on an employee's mobile devices. It helps in the remote pre-configuration and pre-set up of organizational email accounts for employees. MEM can enforce compliance and thwart unauthorized access by allowing only approved and authorized devices and applications to access the email.

- **Enterprise mobility management**

Enterprise mobility management (EMM) consists of tools and technologies used in an organization to secure the data in employees' personal (BYOD) and organizational devices. EMM acts as a comprehensive solution responsible for MDM, MAM, MTM, MCM, and MEM. It safeguards the enterprise data accessed and used by employee mobile devices. EMM can increase employee productivity as the IT admin can configure applications remotely and provide data access to employees.

- **Mobile security management**

Mobile security management involves actions and precautionary steps for securing the organizational data and mobile devices used by employees. It can protect the organization's network access, helps in device and application security, and enables secure access to the organization's emails.

The following are some of the features of mobile security management:

- Generates separate logical containers on mobile devices to prevent private apps from accessing the organization's data
- Employs strong passcode techniques to restrict third-party access
- Automates updates of the devices and OS with the latest security patches
- Blacklists malicious applications
- Executes commands on lost mobile devices remotely
- Configures a VPN specifically for the organization's data, resources, and applications

- **Remote wipe**

Remote wipe is a technique used for securing and protecting data from miscreants if a mobile device used by an employee was stolen or lost. This feature allows the device owner or the organization's administrator to send a command that can delete or erase all the device data. This helps prevent perpetrators from compromising sensitive personal data or confidential organizational assets.

- **Screen lock**

Screen lock is a feature in mobile devices that is used to secure data and prevent illegal access by perpetrators. Enabling screen lock in a mobile device can prevent access to private data in the mobile device even if it was lost or stolen. Screen lock can be set in a mobile device by using protection techniques such as a password, face lock, fingerprint lock, pattern, or PIN. Unlocking the screen involves a set of actions that needs to be performed correctly, failing which the device can lock out after a certain number of unsuccessful attempts.

- **Passwords and PINs**

Passwords and PINs are basic security features used in all mobile devices. Using a secure PIN and complex password can protect private data of the employee and confidential information of the organization stored on a mobile device. A password or PIN acts as a simple but effective defense to safeguard the data from being accessed by any malicious user. A PIN consists of a sequence of numbers, without any letters or special characters. In contrast, a password comprises uppercase and lowercase letters, numerals, and special characters and are usually lengthier than a PIN.

- **Biometrics**

Biometrics is an advanced and unique security technology that utilizes an individual's physical attributes such as fingerprint, iris, face, voice, and behavior for verifying their identity. These data are stored in a database, and whenever the mobile device needs to be accessed, the user-provided data are compared with the stored data; access is allowed only if there is a match. Biometrics can be used to authenticate a user very easily, quickly, and securely. It also prevents the need for remembering complex passwords.

- **Push notification services**

A push-notification service is a messaging feature that originates from a server and enables the delivery of data or messages from an application to a mobile device without any explicit request from the user. It is a great marketing tool for maintaining contact with users. This service does not require any application to be opened for receiving the notification, and the text message in the notification will be displayed on the mobile device, even if the application is closed or the screen is locked. The mobile user has the option of enabling or disabling push notifications. It is important for the developers of mobile applications to apply appropriate security controls for apps or services that

receive push notifications. Otherwise, attackers may be able to send fraudulent push notifications to hack mobile devices.

- **Geolocation**

Geolocation is a technology that can identify the real-world geographical location of users or devices when connected to the Internet. It works on mobile devices through the GPS system and is accurate to the level of approximately one foot. Deploying geolocation in applications helps marketers in implementing their business and marketing techniques easily. Geolocation is also famous for offering a rich user experience for navigation through maps and for tracking people, devices, or vehicles having the GPS feature. Geolocation is also used in weather forecasting.

- **Geofencing**

Geofencing is a technique through which mobile-application marketers utilize the location of the user to gather information. This technique can determine how close the user's mobile device is to an exact location by using the GPS feature. A geofence is a virtual fence that is positioned at a static location and interacts with mobile users that cross the fence. Geofencing helps marketers gather sensitive data and information about users' offline activities from the location data. Geofencing uses cellular triangulation for locating a user's device with an accuracy level of 50–50,000 m.

The following are the main advantages of geofencing for marketing:

- Sends promotions directly to clients
- Improves sales locally
- Reduces cost on paid advertising
- Obtains data on user experience for further improvement

Organizations can employ geofencing to control the usage of unnecessary features such as camera and video within their premises. Geofencing allows organizations to create a virtual boundary around their office premises and implement security controls when a mobile device either enters or leaves the virtual boundary.

- **Full Device Encryption**

Full disk encryption is a security feature that can encrypt all the information stored on any storage medium within a mobile device. This technique encodes the user's information stored on the mobile device by using an encryption key. It is useful for automatically encrypting data, which can be decrypted using the key. It employs encryption algorithms such as the 128-bit Advanced Encryption Standard (AES) with cipher-block chaining (CBC).

Mobile devices also support data encryption at different levels. One encryption technique is to encrypt all user-related data with a key that is stored on the device. This technique is useful at the time of data wiping. The mobile device deletes the key permanently and makes the data inaccessible to a third person. Furthermore, mobile

devices support multiple levels of encryption for email messages using the data protection option.

- **Containerization**

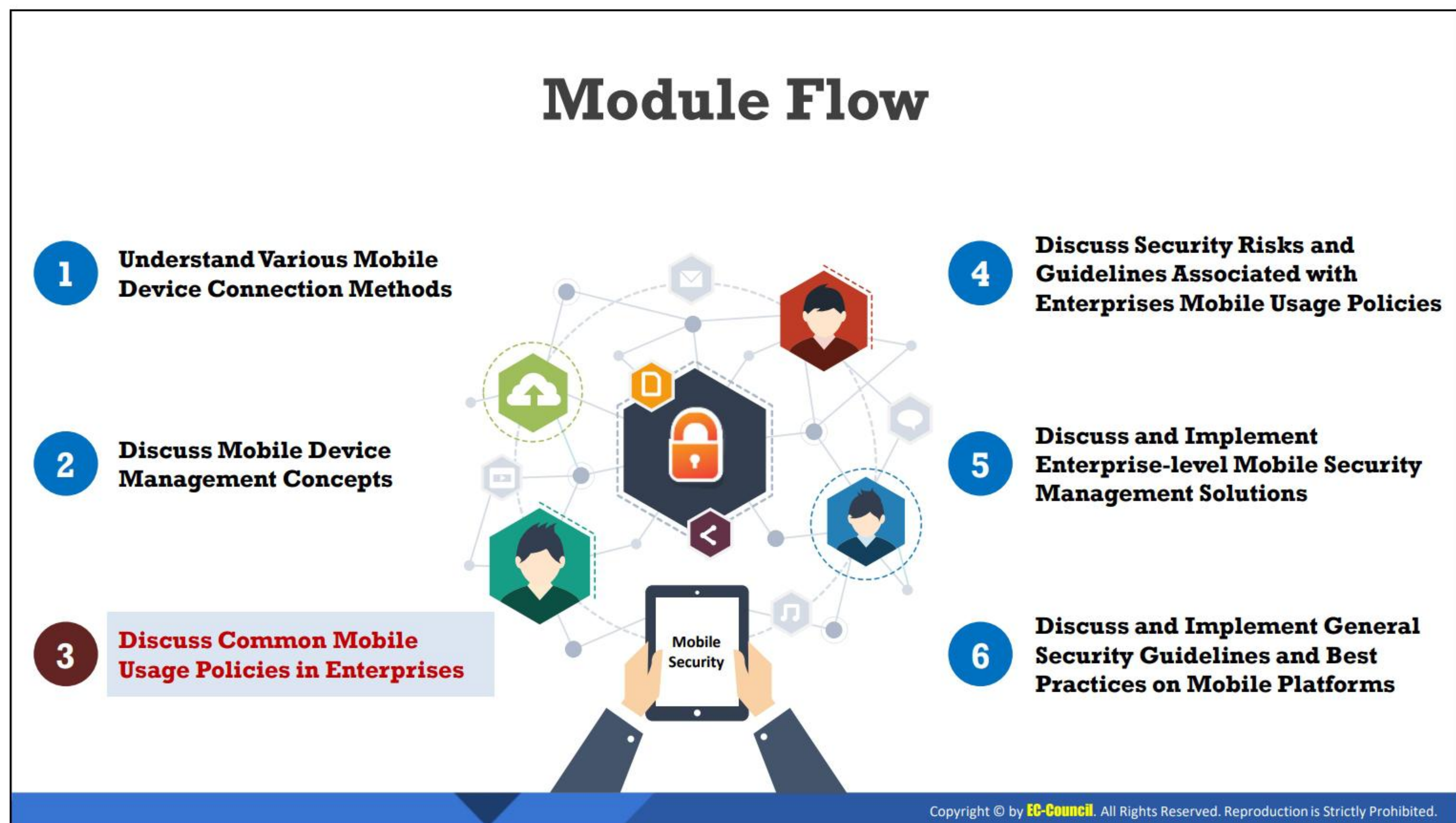
Containerization is a technique in which all personal and organizational data are segregated on an employee's mobile device. With the increasing adoption of BYOD policies, using this technique substantially helps in improving the security of organizational data. It also improves productivity and enables the easy use of company resources and applications. These applications do not have any control of or communication with the private applications or data of the employees as they exist outside the container.

The following are the benefits of containerization:

- By default, containers are encrypted to secure corporate data.
- Data cannot enter or exit the container.
- Data are shared only between the apps within the container.
- Containerization provides complete control over the container's workspace.
- Containerization provides privacy to the user's data on the mobile device.

- **Over-the-air (OTA) Updates**

Over-the-air (OTA) updating is a new method of delivering updates for applications, firmware, and time-zone rules, as well as any other essential data, to a mobile device. This method is used in many tasks such as configuring IoT devices, updating SIM cards, and updating software in electric cars. The manufacturers of mobile devices are introducing OTA technology to update the operating system (OS) and default apps in the device without interfering with the applications downloaded from Google Play Store or any other app store. For iOS devices, the OTA feature was introduced in the iOS 5.0.1 update. Previously, all updates to iPhones were performed by connecting to a computer and updating through iTunes. The main feature of OTA updates is that one updated device can send updates to all other devices in the network. However, OTA technology has vulnerabilities that may allow attackers to place an evil base station in a particular area and perform various attacks such as MITM and exploit device firmware.



Discuss Common Mobile Usage Policies in Enterprises

An organization that enables its employees to work remotely using a smartphone or tablet must design a policy to secure these devices and protect the company data. This section introduces the various mobile usage policies that can be implemented by an organization based on its requirements.



Mobile Use Approaches in Enterprise

An organization can implement any of the following policies based on their requirements as well as the role and responsibilities of its employees to enable them to use mobile devices for business purposes.

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

The following questions can help an organization to determine which approach to follow:

- **Device Specific**
 - Device type (which device to use (smartphone/phablet/laptop)?)
 - Selection of device (who uses which devices?)
 - Who pays for the device?
 - Service providers for cellular connectivity and monthly plans
- **Management and Support**
 - Who manages the device?
 - Who is responsible for support?
- **Describe Integration and Application**
 - Describe how closely the device is integrated and important for everyday workflow?
 - Describe the installed/running applications
 - Should personal applications be restricted?

Bring Your Own Device (BYOD)

- ❑ Bring your own device (BYOD) refers to a policy that allows employees to bring their **personal devices** such as laptops, smartphones, and tablets to the **workplace** and use them for accessing the organizational resources based on their access privileges
- ❑ The BYOD policy allows employees to use the devices that they are comfortable with and best fits their preferences and work purposes

BYOD Benefits

- 1 Increased productivity
- 2 Employee satisfaction
- 3 Work flexibility
- 4 Lower costs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD)/Bring Your Own Technology (BYOT)/Bring Your Own Phone (BYOP)/Bring Your Own PC (BYOPC) refers to a policy that allows employees to bring their devices such as laptops, smartphones, and tablets to the workplace and use them for accessing the organizational resources based on their access privileges.

The BYOD policy allows employees to use the devices they are comfortable with that best fit their preferences and work purposes. With the “work anywhere, anytime” strategy, the BYOD trend encounters challenges in securing the company data and satisfy compliance requirements.

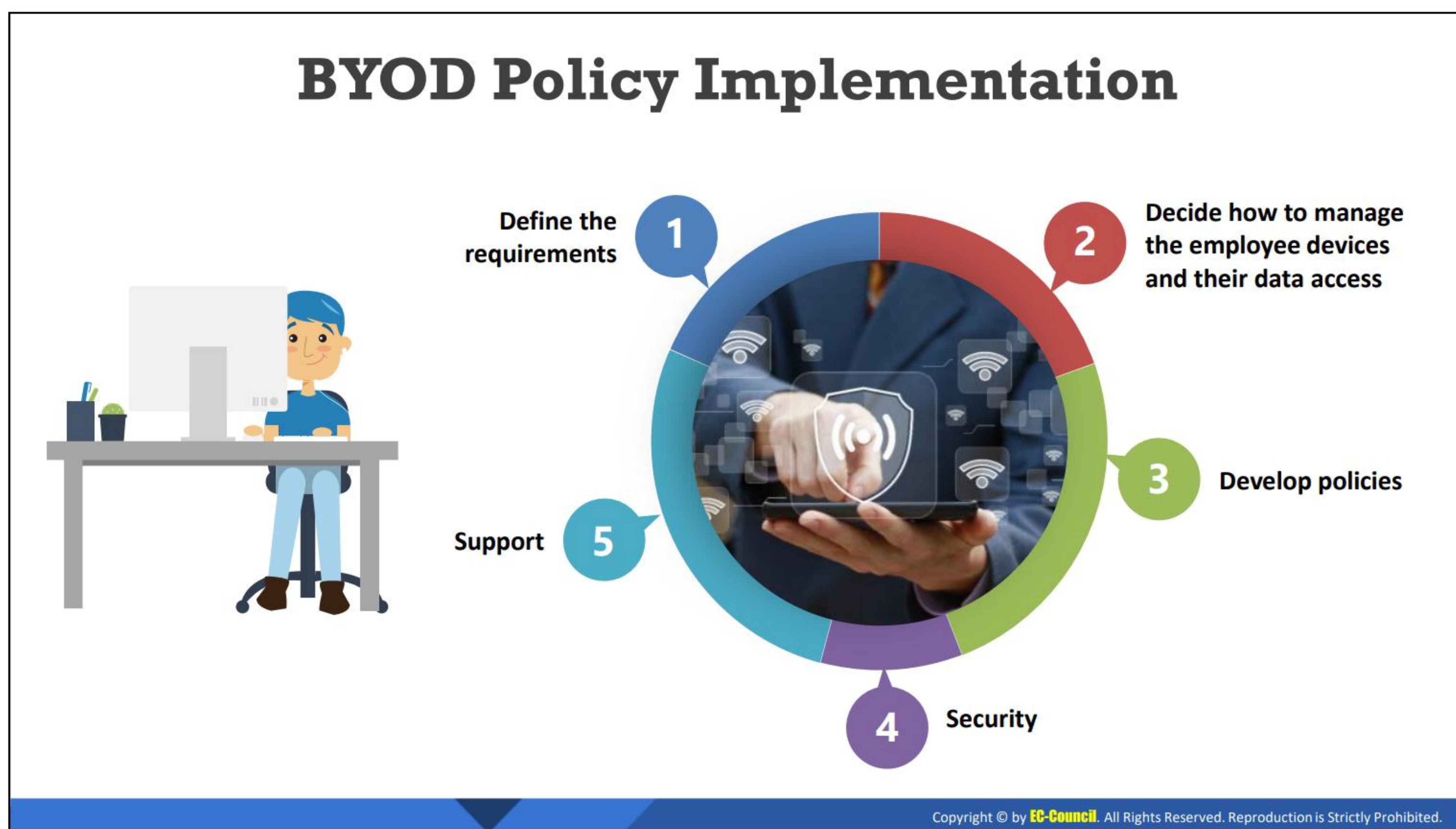
BYOD Advantages

The adoption of BYOD is advantageous to the company as well as its employees. Its advantages include:

- Increased productivity and employee satisfaction
- Enhances work flexibility
- Lower IT Costs
- Increased availability of resources

BYOD Disadvantages

- Difficult to maintain security access in organizational networks
- Increased compatibility issues
- Reduced Scalability



BYOD Policy Implementation

For the implementation of the BYOD policy, the employee devices must be introduced to the corporate environment to minimize the risks associated with data security and privacy.

- **Define the requirements**

Not all user requirements are similar. Thus, the employees must be grouped into segments considering the job criticality, time sensitivity, value derived from mobility, data access, and system access. Further, end user segments should be defined based on the location/type of worker (e.g., an employee working from home, full-time remote, day extender, part-time remote), and a technology portfolio should be assigned for each segment based on user needs.

Privacy impact assessment (PIA) should also be performed at the beginning of each BYOD project in the presence of all relevant teams after assigning the responsibilities and collecting the requirements. It provides an organized procedure to document the facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project lifecycle. It should be a central activity performed by the mobile governance committee (end users from each segment/line of business and IT management).

- **Decide how to manage the employee devices and their data access**

Apart from the mobile device management (MDM) system that provides a minimum level of control, other options such as virtual desktops or on-device software can be used to improve the security and data privacy. Additionally, it should be ensuring that the corporate environment supports WLAN device connectivity and management.

- **Develop policies**

- A delegation of company resources should develop the policies, instead of just IT. It should include key participants such as the HR, legal, security, and privacy.
- Each device (smartphone, PC, laptop, tablet, or even smartwatch) and OS in the BYOD policy of a company should be listed; devices with a poor security record should not be permitted. This involves only permitting devices with specific OSes or manufacturers.
- Establish a policy to determine a reasonable, binding policy regarding BYOD to secure businesses and employees.
- The IT staff of an organization should be trained about the various platforms, devices, and OSes to familiarize them with the risks associated with wrong device handling or to avoid the security threats imposed by a BYOD work environment.
- The BYOD policy should also ensure that the devices are appropriately backed up to prevent the loss of critical data under unforeseen circumstances.

- **Security**


The mobile management technology is effective only when suitable policies are established, implemented, and supported. The organizations must ensure sufficient security in the mobile ecosystem to make the BYOD programs work. This requires a thorough assessment of the operating environment and the development of a solution that provides the following.

- Asset and identity management
- Local storage controls
- Removable media controls
- Network access levels
- Network application controls
- Corporate versus personal app controls
- Web and messaging security
- Device health management
- Data loss prevention


- **Support**

The inconsistent nature of BYOD users will increase the frequency of support calls. Therefore, organizations should establish suitable processes and capabilities in the early stages to ensure success. Mobile committees should frequently reassess the support levels and ensure the productivity of their mobile employees.

Choose Your Own Device (CYOD)



Choose Your Own Device (CYOD) refers to a policy that allows employees to **select** devices such as laptops, smartphones, and tablets from the list of devices approved by the company. The company purchases the selected device, and the employees use it for accessing the organizational resources **according to their access privileges**



CYOD Benefits

1

Streamline device options

2

Employee satisfaction with company's control

3

Devices compatible with the company security policy

4

Lower cost compared to COPE

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Choose Your Own Device (CYOD)

Choose Your Own Device (CYOD) refers to a policy in the employees select their device of choice from a preapproved set of devices (laptops, smartphones, and tablets) to access company data according to the access privileges of an organization. For example, allowing employees to select an Apple device instead of Android devices. CYOD has recently garnered more attention than BYOD in the business world because securing BYOD systems can be difficult considering the various devices available in the market, and employees store personal and professional data irrespective of whether a device is personal or belongs to the employer.

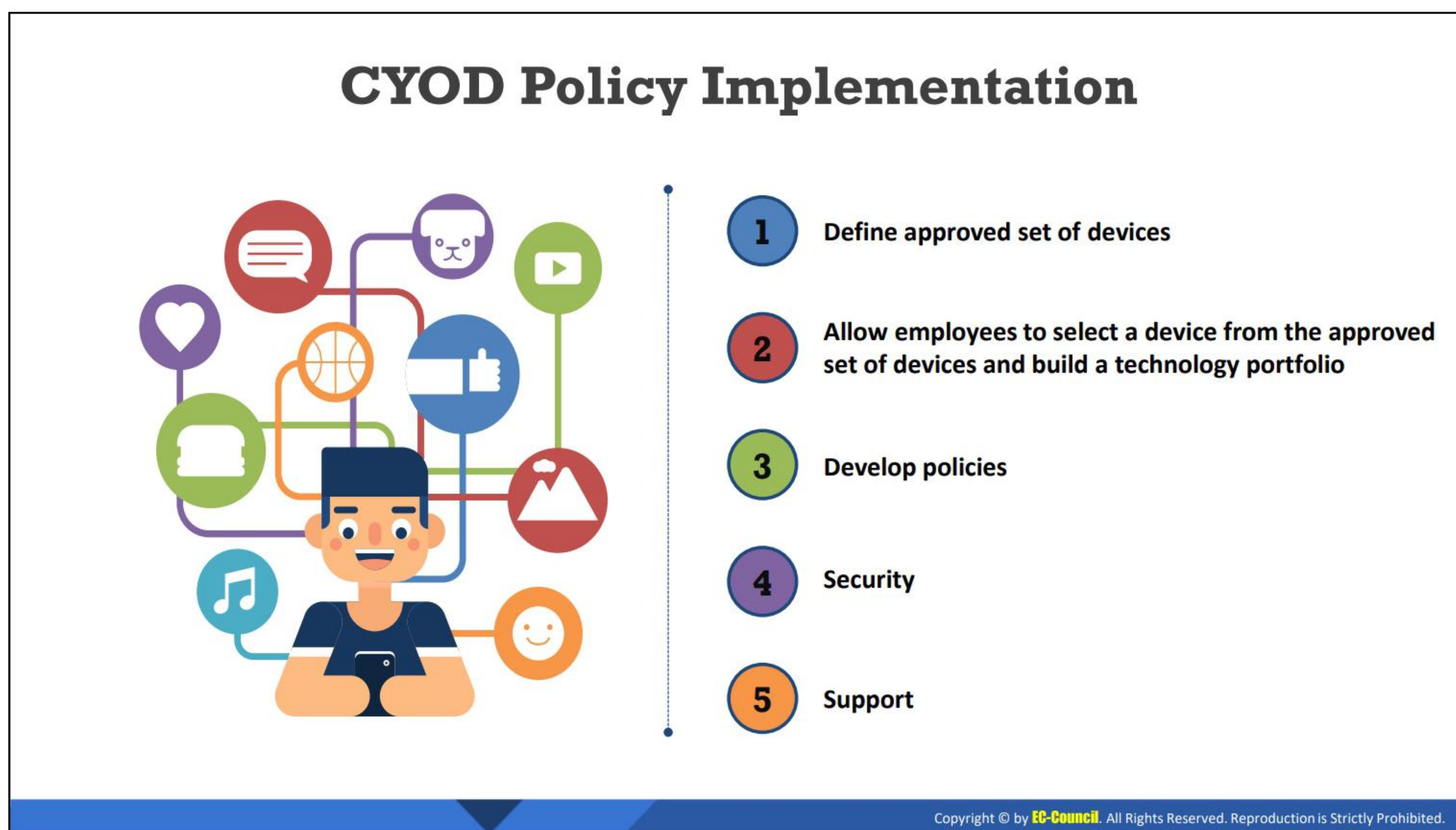
CYOD Advantages

- Users are allowed to carry only one smartphone and one tablet.
- It reduces hardware costs compared to COPE.
- End users are still in control of their own technology.
- Procurement standards are stricter than those of BYOD.
- Its support standards are streamlined.
- Each security device is preinstalled with a security solution and predefined firewall and network settings of a dedicated administrator.
- Administration of a small number of different specifications makes record-keeping easy.
- Employees comply with data and information management requirements.

CYOD Disadvantages

- Some IT staff may not be happy with the choices.

- It involves a more complex procurement process than BYOD or COPE.
- End users face replacement and repair problems.
- It needs to be updated with the mobile technology / apps used by the organizations.
- It comprises a slower deployment timeframe.



CYOD Policy Implementation

The key considerations before implementing a CYOD policy are

- **Define an approved set of devices:** Organizations must formulate a list of corporate-sanctioned devices and plans for their employees to access company data according to their access privileges.
- **Allow employees to work with company-owned devices (including personal work) and build a technology portfolio:** Allow employees to select devices (laptops, smartphones, and tablets) and plans from role-based corporate catalogs. Before delivery, set up the devices with apps, software, and settings required by each employee, thereby enabling them to operate the apps immediately. For example, set up devices with Outlook with the employee credentials.
- **Develop policies and device security:** Establish policies to ensure that the employees understand the responsibilities accompanying network access. The more granular the organizational policies are in terms of device types, different versions of OSes, and device model number, the more resources will need to be tested to support such devices. For example, allowing only a specific Android mobile model or a specific version of a mobile OS.

Implement the following:

- Virus protection
- Encryption
- Network access controls and authentication
- Data wipes and remote locks in case devices are lost or stolen

- Train the employees to inform them about their mobile responsibilities, including how data are accessed, used, and stored, and how to use apps and services.
- **Support:** Deploy expertise solutions (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
 - Device troubleshooting
 - Service troubleshooting
 - Activating devices
 - Deactivating devices
 - Managing service requests



Corporate Owned, Personally Enabled (COPE)

Corporate Owned, Personally Enabled (COPE) refers to a policy that allows employees to use and manage the devices purchased by the organizations. The devices include laptops, notebooks, smartphones, tablets, and/or software services. Larger enterprises are more likely to employ the COPE model.

COPE is a lesser expensive option than BYOD because the companies buy devices at a lower cost than the retail price. COPE reduces the risks associated with BYOD by implementing stringent policies and protecting devices.

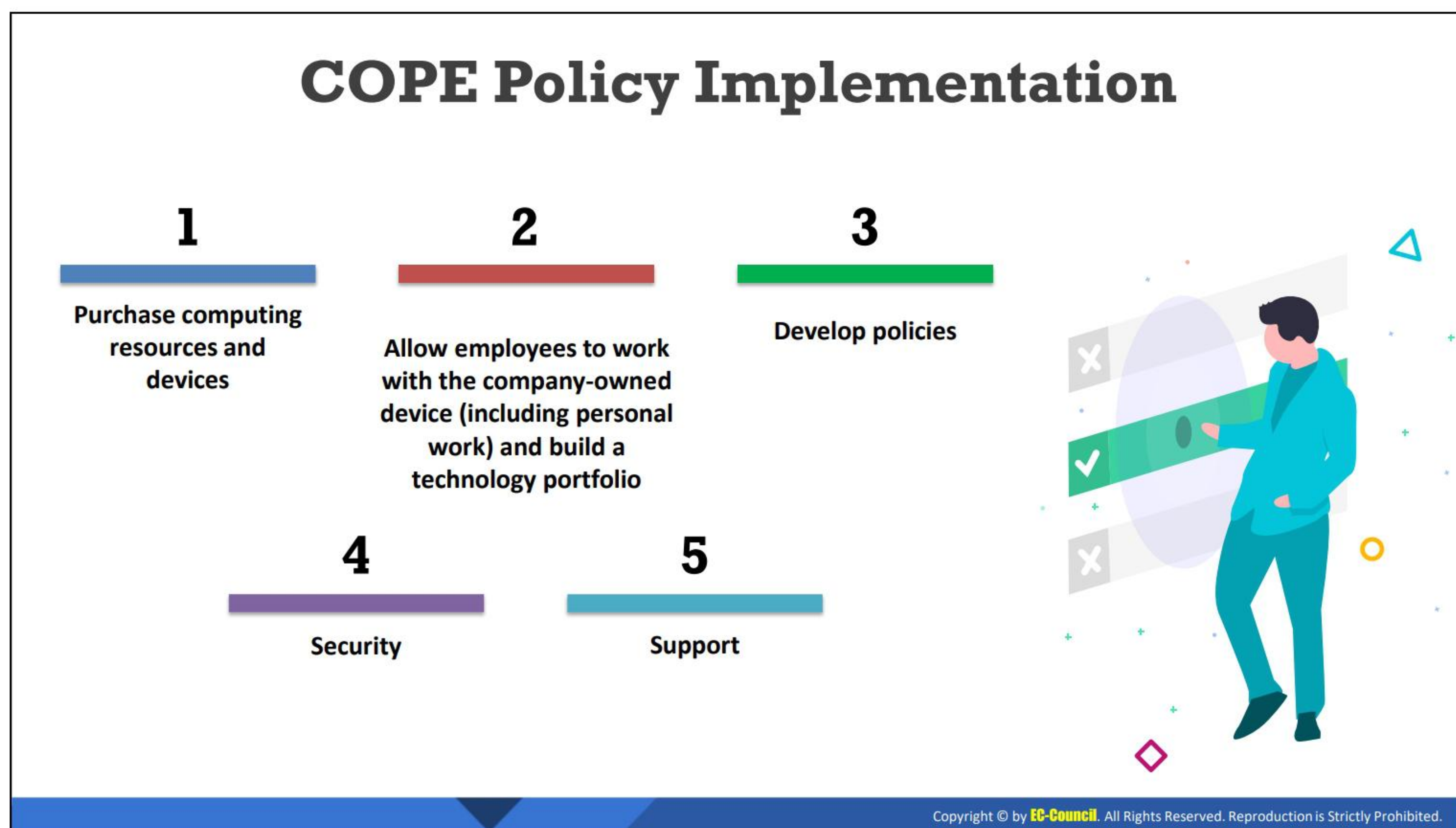
COPE Advantages

- Work or life balance on a single device
- Fewer security concerns than BYOD and CYOD
- Personal apps
- Enhanced control and authority over devices
- Prevents employees from carrying two phones
- Retains ownership of devices
- Less expensive than BOYD
- Enables organizations to freely install management software and/or integrate devices in MDM systems
- Helps in solving regulatory and legal issues associated with deleting data on lost/stolen mobile devices

- Economizes the resources (save and time) of the IT department because the employees are responsible for the condition of their devices.

COPE Disadvantages

- Need to purchase devices
- Monitoring policies must be established
- Business is completely responsible for keeping up with the latest technologies
- Potential for productivity issues owing to less user freedom
- Slowest deployment timeframe



COPE Policy Implementation

The considerations for the implementation of a COPE strategy include:

- **Purchase computing resources and devices:** The organization purchases preapproved devices from vendors based on their centrally designed plan.
- **Allow employees to work with company-owned devices and build a technology portfolio:** These organization-owned devices allow employees to have COBO's conservatism and BYOD's freedom. The devices are designed for both office and personal works.
- **Develop policies**
 - Ensure that the **employees completely understand and sign-off on the policy** related to them leaving the company.
 - Decide whether the employees will be **allowed to procure or retain the device** after leaving the company and create a procedure for removing all corporate data and assets from the device.
- **Security:** To ensure device security, organizations apply security controls, restrict certain features to secure from malware and data leaks, and monitor devices for data breaches or jailbreaking.
- **Support:** Deploy expertise solutions (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
 - Device troubleshooting
 - Service troubleshooting
 - Activating devices
 - Deactivating devices
 - Managing service requests



Company Owned, Business Only (COBO)

Company Owned, Business Only (COBO) refers to a policy that allows employees to use and manage the devices purchased by the organization but restrict the use of the device for business use only. COBO is used to describe a device that runs a single application. For example,

- An inventory system with an embedded barcode scanner.
- Blackberry is the best example of devices used in a COBO environment.

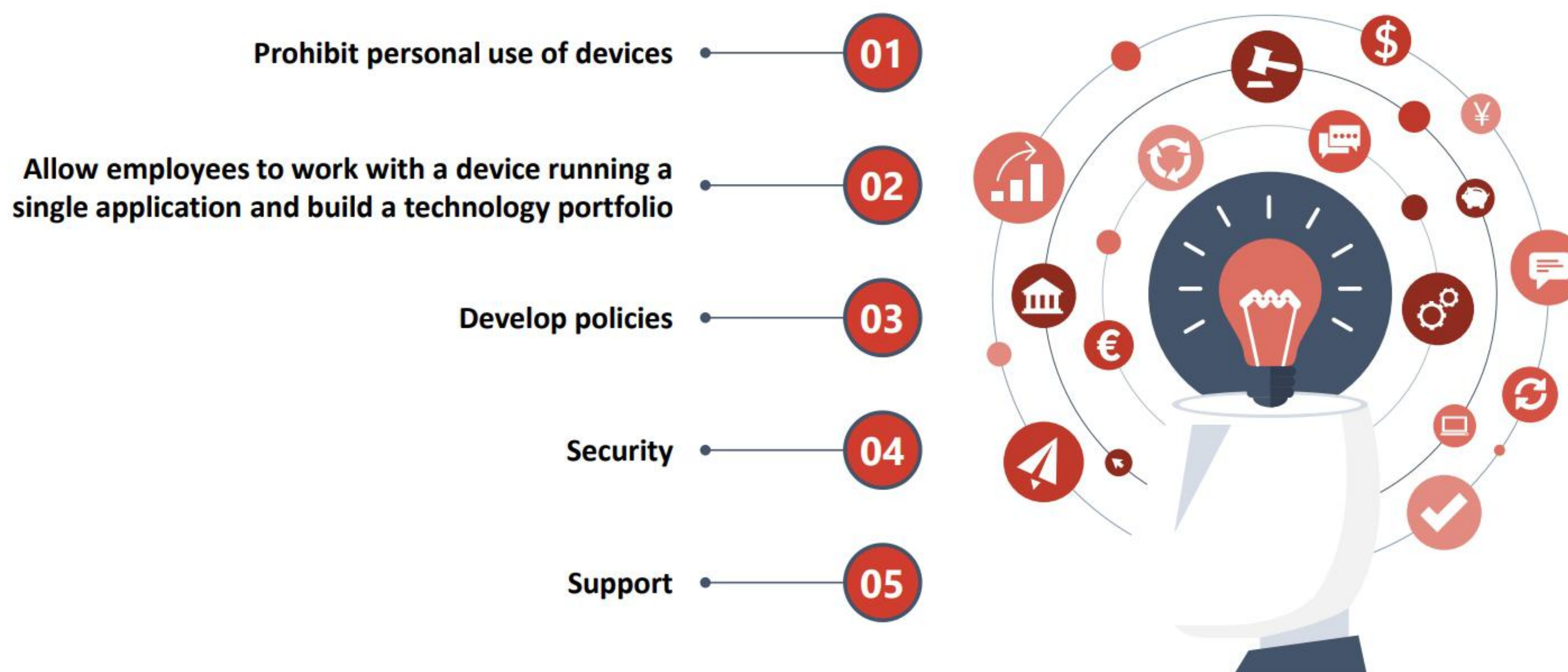
COBO Advantages

- The company retains full control over all apps on the device and its data.
- A uniform system landscape is adhered to because the organization purchases the device.
- Prevents data leakage.

COBO Disadvantages

- High purchase cost for devices.
- Employees do not really enjoy working with at least two devices in their pockets.

COBO Policy Implementation



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

COBO Policy Implementation

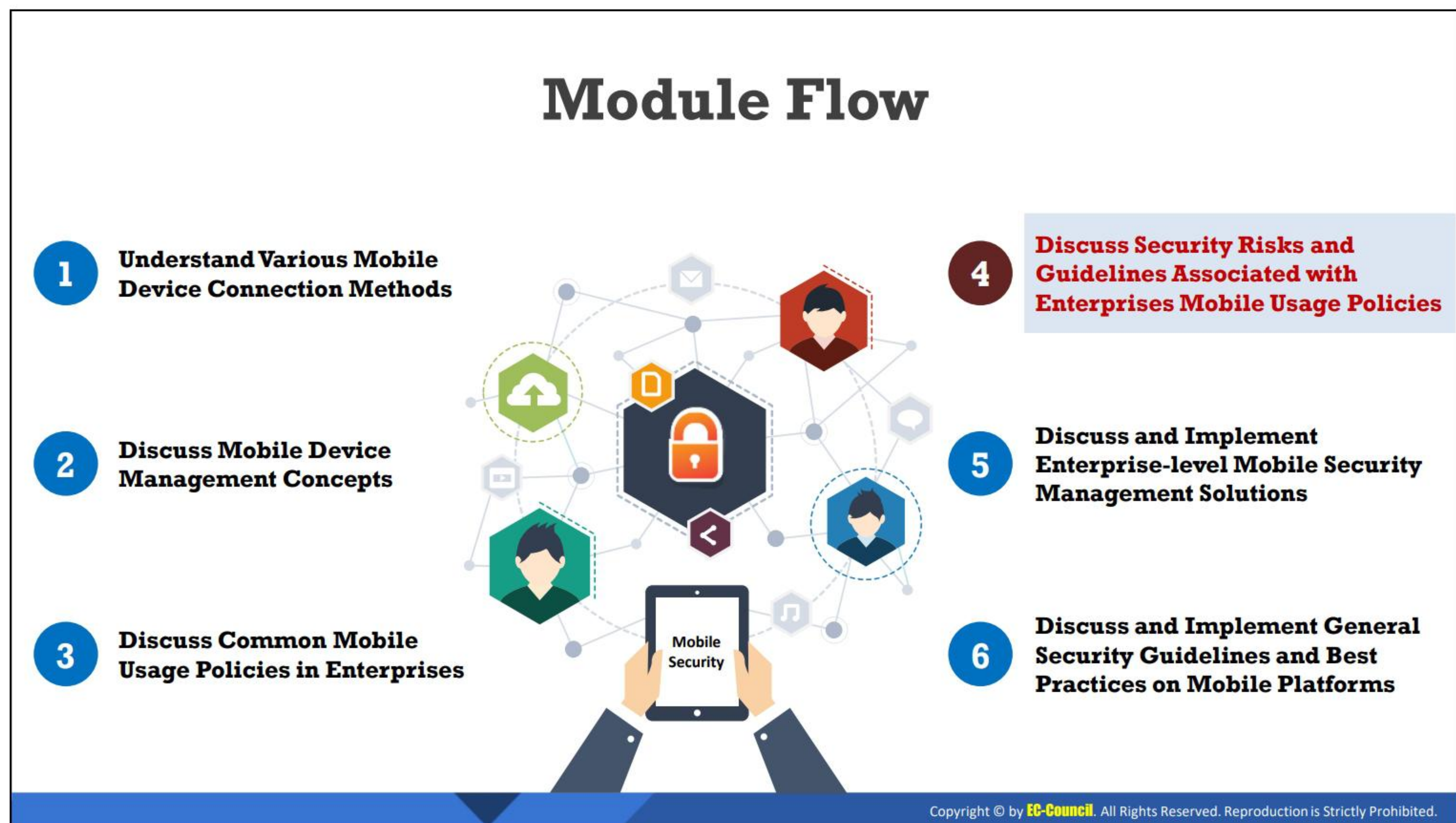
The considerations for the implementation of a COBO strategy are

- **Prohibit personal use of devices:** Enterprises prohibit the use of mobile devices as a part of their designing policy based on the COBO approach.
- **Allow employees to work with devices running single application and build a technology portfolio:** Enterprises allow employees to work with a device that runs a single application; for example, an inventory system with an embedded barcode scanner. Otherwise, they can allow the use of smartphones with prohibited personal use. Additionally, they should implement highly granular devices as well as app and data management to enable compliance.
- **Develop policies:** Ensure that the mobile device management (**MDM**) and mobile application management (**MAM**) solutions fully meet the requirements of the company's concept.
- **Security**
 - Ensure fully locked down devices to maintain control over granular policies and control the device usage
 - Prevent app downloads
- **Support**

Deploy expertise systems (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address

 - Device troubleshooting

- Service troubleshooting
- Activating devices
- Deactivating devices
- Managing service requests



Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies

Creating a mobile usage policy that will enable smooth functioning and ensure security of the corporate assets is a major challenge. The objective of this section is to explain the security risks and challenges associated with the enterprise mobile usage policies. It describes the risks associated with the BYOD, CYOD, COPE, and COBO policies in detail along with the security guidelines to be implemented for them.

Enterprise Mobile Device Security Risks and Challenges



Security Risks

- ✓ The use of mobile devices in a work environment has changed the approach of organizational security. Mobile usage in enterprises has created a new set of security risks and challenges
- ✓ Hence, enterprise mobile device security encounters additional security challenges besides the **mobile device-level security risks** that include weak security systems and insufficient configuration of mobile devices and platforms
- ✓ Mobile devices are moving **targets** that can be used outside an organization and its security system, thereby defeating the purpose of preventing security attacks when organizations allow mobile devices at the workplace



Security Challenges

- ✓ Mobile devices are **harder** to track and secure
- ✓ Mobile devices are **portable** enough that they can be easily lost or stolen
- ✓ It is difficult to ensure that mobile **software patches** and **security settings** are updated



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enterprise Mobile Device Security Risks and Challenges

The use of mobile devices in work environments has changed the security approach of organizations. It has given rise to a new set of security risks and challenges in organizational security. In addition to the mobile device security risks that include weak security systems and insufficient configuration of mobile devices and platforms, enterprise mobile device security faces additional security challenges. Mobile devices are moving targets that can be used outside an organization and its security system, thereby defeating the purpose of preventing security attacks when organizations allow mobile devices at the workplace.

These challenges can be divided into the following categories:

■ Physical Risks and Challenges

This includes the loss or theft of a mobile device owing to their portability and lightweight. Attackers can perform malicious actions if they get physical access to a device such as flashing the device with a malicious system image that is connected to a computer to install a malicious application or conduct data extraction.

Therefore, the devices should not be left unattended. Security measures such as device authentication and encryption must be enforced. Instead of using a simple password, enforce multiple forms of authentication to prevent unauthorized access to mobile devices.

■ Network-based Risks and Challenges

Mobile devices that use common wireless network interfaces (Wi-Fi, Bluetooth) for connectivity are vulnerable to wireless eavesdropping attempts.

Therefore, employees should connect to trusted networks using WPA21 or use secured network protocols (IPsec, SSL, SSH, HTTPS, Kerberos, etc.) to prevent mobile devices from network-based threats. Moreover, they can use special gateways with customized firewalls and security controls to direct the mobile traffic. For example, content filtering and data loss prevention tools.

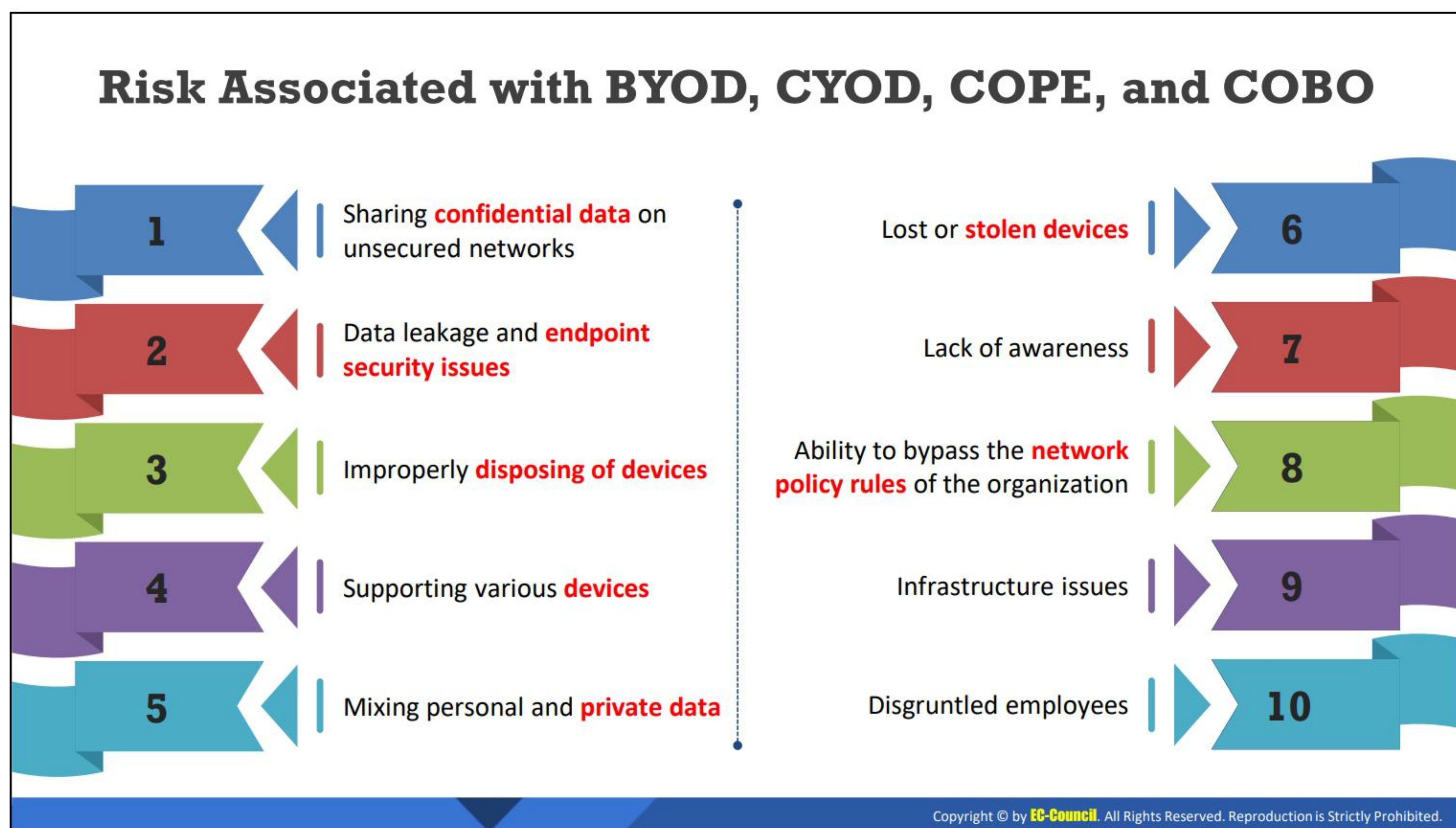
- **System-based Risks and Challenges**

Manufacturers may unintentionally introduce vulnerabilities in devices; for example, vulnerabilities in SwiftKey keyboards or mobile OSes. Therefore, the devices should be regularly updated to reduce threats.

- **Application-based Risks and Challenges**

Vendors may not release timely app updates and support for older OS versions or users may not update their apps regularly. Attackers can exploit the vulnerabilities in applications and attempt to steal data, download other malware, or control the device remotely, thereby resulting in financial loss and risk the reputation of an organization.

Thus, strict controls must be enforced regarding downloading and installing applications on a device and using mobile anti-virus. Additionally, strong policies must be established to limit or block the use of third-party applications on devices.





Risk Associated with BYOD, CYOD, COPE, and COBO

Employees connecting to a corporate network or accessing corporate data using their own mobile devices pose security risks to an organization. Following are some security risks associated with the BYOD, CYOD, COPE, and COBO policies:

- **Sharing confidential data on an unsecured network:** Employees might access corporate data via a public network. These connections may not be encrypted and sharing confidential data via an unsecured network may lead to data leakage.
- **Data leakage and endpoint security issues:** In this cloud-computing era, mobile devices are insecure endpoints with cloud connectivity. By synchronizing with organizational email or other apps, these mobile devices carry confidential information. If a device is lost, it could potentially expose all corporate data.
- **Improperly disposing of devices:** An improperly disposed of device could contain a wealth of information such as financial information, credit card details, contact numbers, and corporate data. Therefore, it is important to ensure that devices do not contain any data before they are disposed or passed on to others.
- **Support of many different devices:** Organizations allow employees to access their resources from anywhere in the world, thereby enhancing productivity and driving employee satisfaction. Support for different devices and processes can increase the cost. Employee-owned devices have limited security that operate on different platforms. This deters the capabilities of the IT department to manage and control devices in a company.

- **Mixing personal and private data:** Control over isolating business use from personal use is difficult. For example, managing employees that shop on compromised websites, use public Wi-Fi connections, or given their device to others.
- **Lost or stolen devices:** Owing to their small size, mobile devices are often lost or stolen. When an employee loses their mobile device that is used for both personal and official purposes, the organization might face a security risk because the corporate data on the lost device may be compromised.
- **Lack of awareness:** Failing to educate employees regarding these policy and security issues may compromise the corporate data stored in mobile devices.
- **Ability to bypass organizational network policy rules:** According to requirements, the policies imposed may differ for wired and wireless networks. The devices connected to wireless networks can bypass the network policies enforced only on wired LANs.
- **Infrastructure issues:** These policies involve dealing with various platforms and technologies. Not all employees carry the same device. Different devices, each running different OSes and programs, have security loopholes. This can be problematic for an IT department to set up and maintain an infrastructure that supports the requirements of different devices such as managing data, security, back up, and compatibility among devices.
- **Disgruntled employees:** Disgruntled employees in an organization can misuse the corporate data stored on their mobile devices. They may also leak sensitive information to competitors.

Security Guidelines for BYOD, CYOD, COPE, and COBO

 For Security Professional	 For Employee
<ul style="list-style-type: none">❖ Secure organizational data centers with multi-layered protection systems❖ Educate employees about the COPE policy❖ Clarify who owns which apps and data❖ Use encrypted channels for data transfer❖ Clarify which apps are allowed or banned❖ Control access on a need-to-know basis❖ Ensure that the employees completely understand and sign-off on the policies	<ul style="list-style-type: none">❖ Use the encryption mechanism to store data❖ Maintain a clear separation between business and personal data❖ Register devices with a remote locate and wipe facility if the company policy permits❖ Regularly update the device with the latest OS and patches❖ Use anti-virus and data loss prevention (DLP) solutions❖ Set a strong passcode for the device and change it often❖ Set passwords for apps to restrict others from accessing them

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Guidelines for BYOD, CYOD, COPE, and COBO

The following are some of the security guidelines to be followed by network defender and employees when the BYOD, CYOD, COPE, and COBO policies are implemented.

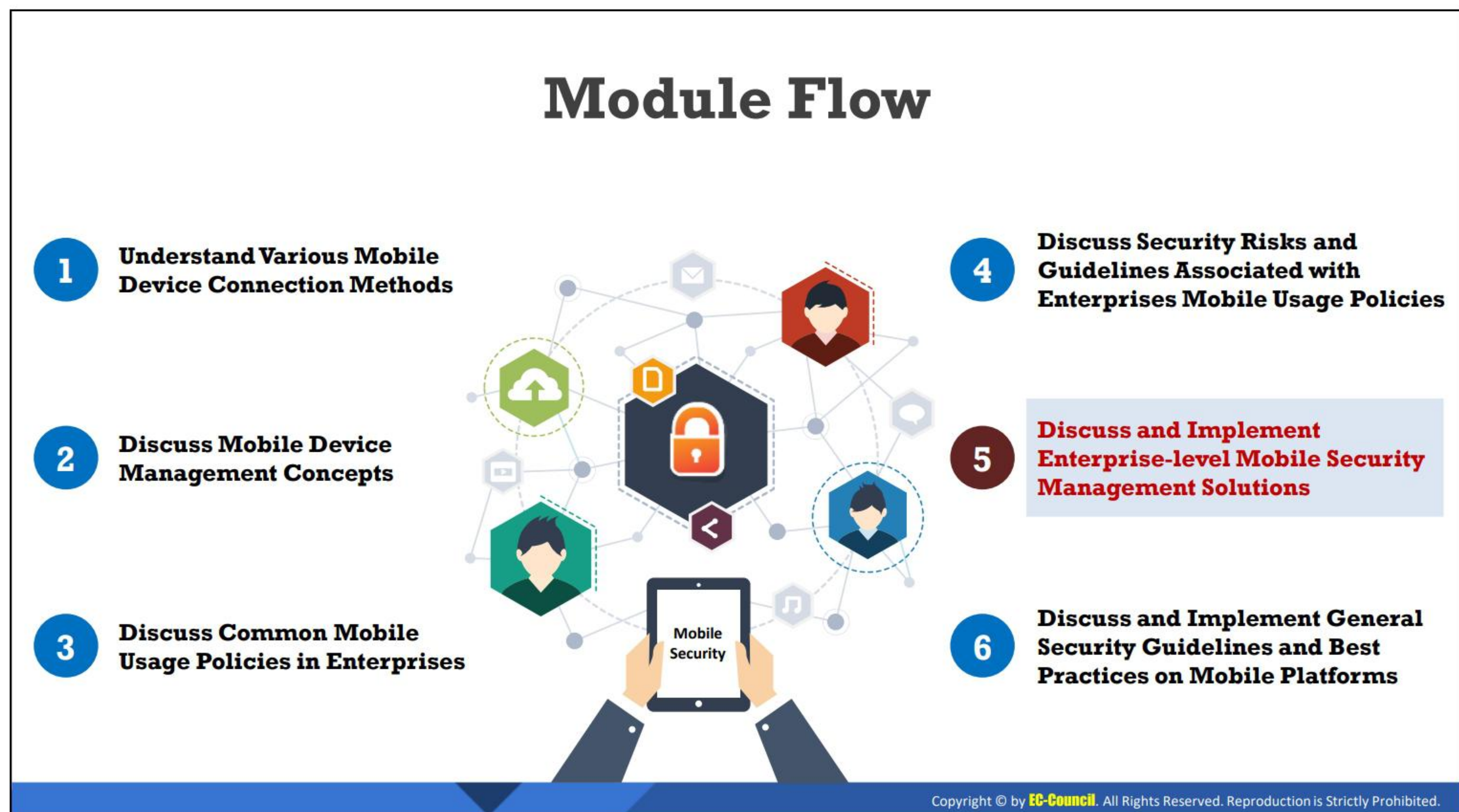
▪ For Security Professional

With the increased use of tablets, smartphones, and other devices at work, mobile security has become a great concern. Listed below are the security guidelines that should be implemented to ensure the security of the network and data of an organization.

- Secure the data centers in organizations with multi-layered protection systems.
- Educate employees about these policies.
- Clarify who owns which apps and data.
- Use an encrypted channel for data transfer.
- Clarify which apps are allowed or banned.
- Control access on a need-to-know basis.
- Do not allow jailbroken and rooted devices.
- Apply session authentication and timeout policy on access gateways.
- Ensure that the employees completely understand and sign-off on the policies.
- Create a procedure for removing all corporate data and assets from the device if an employee leaves the company.
- Ensure that the MDM and MAM solutions of company correspond its requirements.

▪ **For Employees**

- Impose company WLAN access when on-site.
- Ensure the use of complex passcodes and change them frequently.
- Ensure that mobile devices are registered and authenticated before allowing access to the organizational network.
- Consider multi-factor authentication methods to enhance the security while remotely accessing the organization's information systems.
- Make users agree and sign the policies before they can access the organization's information system.
- When an employee leaves the organization, state whether total device wipe or selective wipe of certain apps and data is required and ensure that the organization and personal data are maintained separately.
- Implement strong algorithms to encrypt the organization data stored in the devices; also use an encrypted channel for data transfer.
- If a device is lost or stolen, remotely reset or wipe the device passwords to prevent unauthorized access to the sensitive data of an organization.
- Implement an SSL-based VPN, which provides secure remote access.
- Ensure that user devices are regularly updated with the latest OSes and other software, which could avoid and sometimes even fix any security vulnerabilities.
- Do not provide offline access to the sensitive information of an organization, which should be accessible only via the company network.
- Use anti-virus and data loss prevention (DLP) solutions.
- Set passwords for apps to restrict others from accessing them.



Discuss and Implement Enterprise-level Mobile Security Management Solutions

To handle the mobile security challenges in enterprises, organizations are implementing various mobile security management solutions. Mobile management solutions help an organization to manage mobile devices across the organization from a central location. The objective of this section is to explain the benefits of such mobile management tools and solutions. It describes mobile devices management tools such as MDM solutions, MAM solutions, mobile content management (MCM) solutions, mobile threat defense (MTD) solutions, mobile email management (MEM) solutions, enterprise mobility management (EMM) solutions, and unified endpoint management (UEM) solutions.

Mobile Device Management Solutions

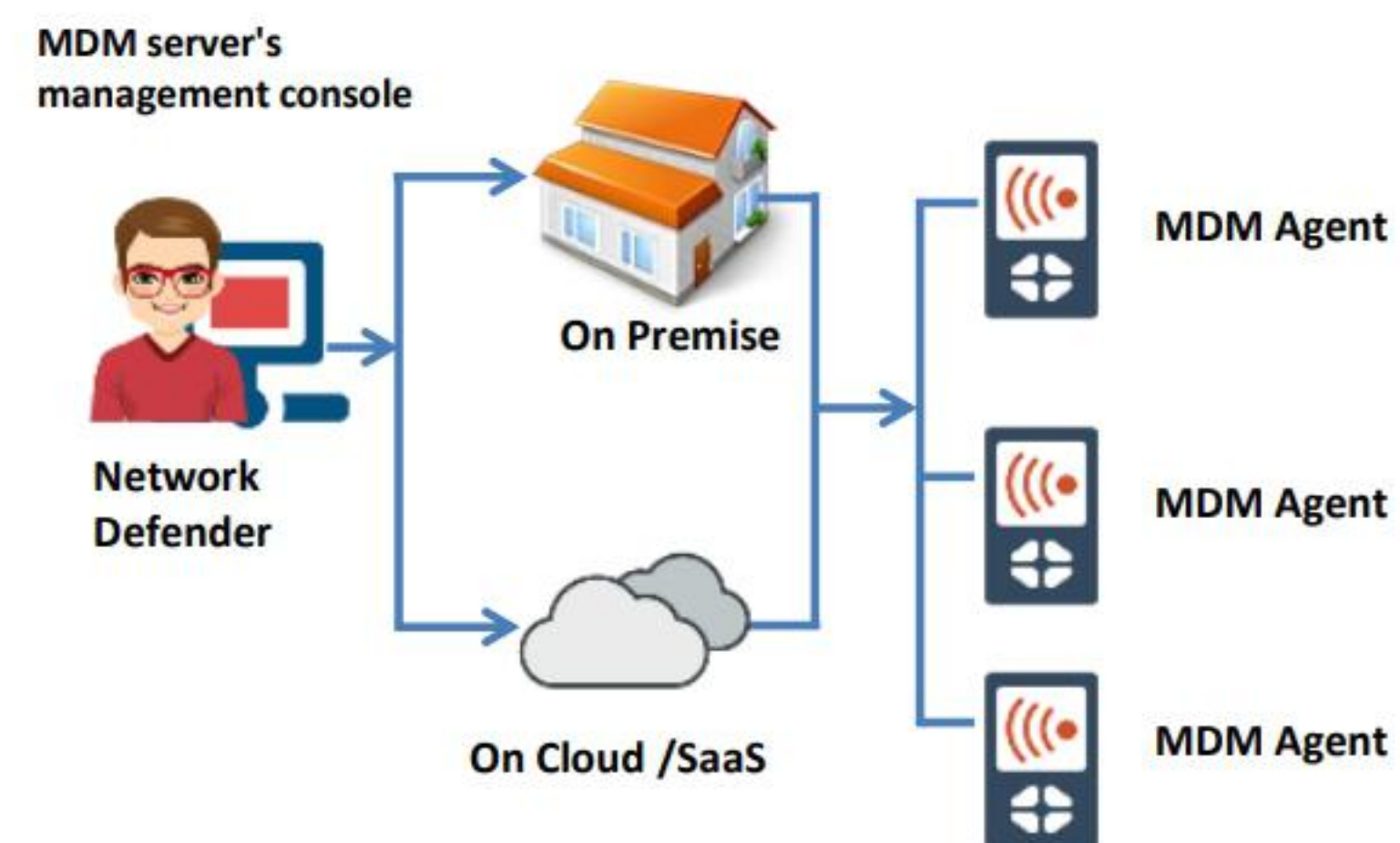


Mobile device management (MDM) solutions are used to **deploy**, **secure**, **monitor**, and **manage** company and employee-owned devices



Security professionals use the MDM server management console to remotely configure **the MDM agents** installed on the devices

MDM Solution Deployment

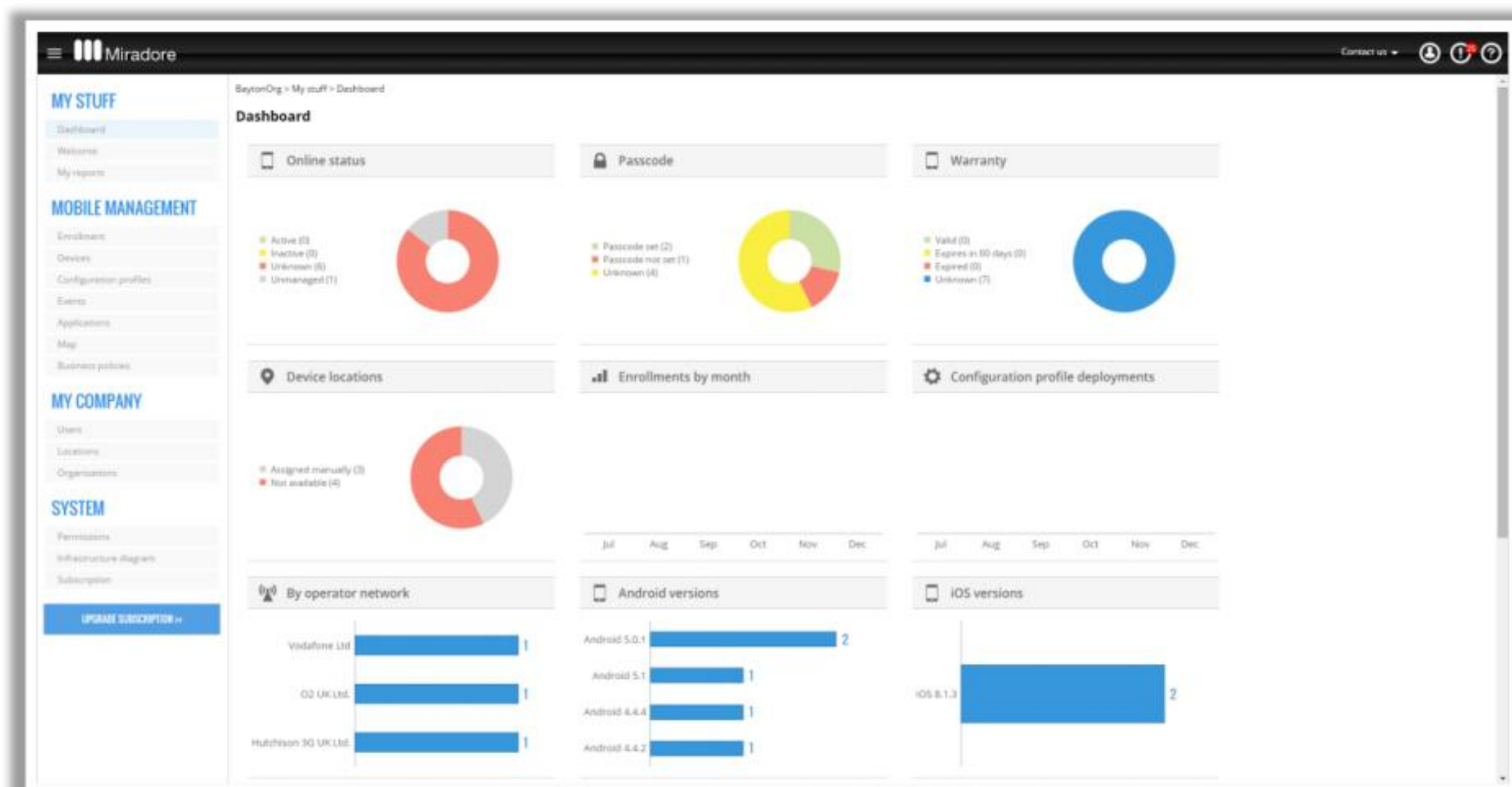


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management Solutions (Cont'd)

Miradore

Miradore helps ensure device and **data security** as well as **data compliance** across an organization



<https://www.miradore.com>



AirWatch
<https://www.vmware.com>



Microsoft Intune
<https://www.microsoft.com>



IBM MaaS360
<https://www.ibm.com>



XenMobile
<https://www.citrix.com>



Absolute Manage MDM
<http://www.absolute.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management Solutions

Mobile device management (MDM) is gaining significant importance with the adoption of policies such as BYOD across organizations. The increase in different types of mobile devices such as smartphones, laptops, and tablets has made it difficult for enterprises to make policies and manage the devices securely. MDM is a policy that helps in managing devices carefully while reducing support costs, mitigating security risks, and reducing business discontinuity.

Mobile device management (MDM) solutions are used to deploy, secure, monitor, and manage company and employee-owned devices. Network defenders use the MDM server management console to remotely configure the MDM agents installed on the devices.

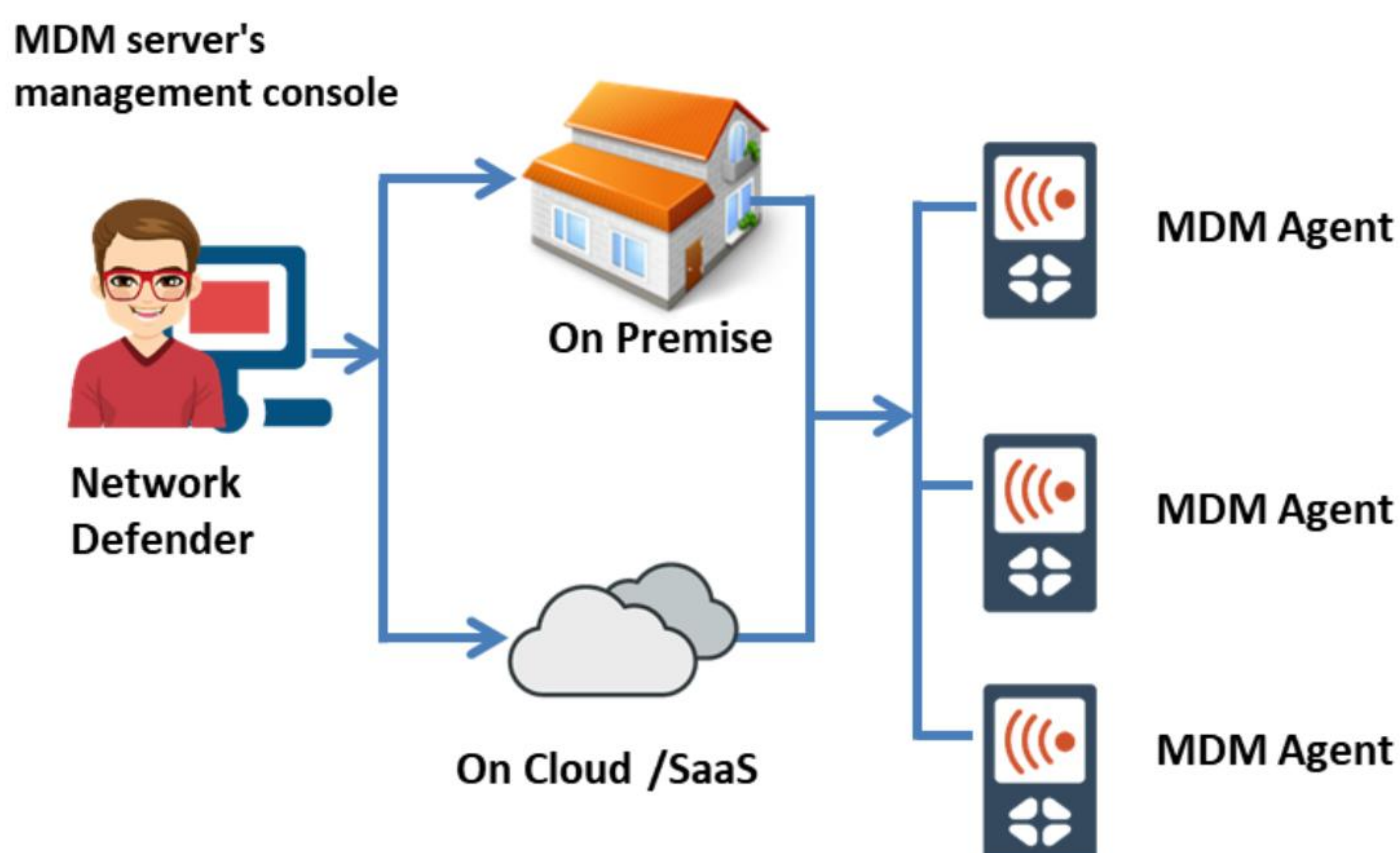


Figure 12.2: MDM solution deployment

Features of MDM Solutions

- Security Management
- Device Configuration Management
- Device Inventory and Tracking
- Over-the-Air Application Distribution
- Enterprise Policy Management
 - Password Enforcement
 - Data Encryption Enforcement
- Enterprise Network Integration
- Remote Data Wipe
- Blacklisting/Whitelisting Apps and Devices

Mobile Device Management (MDM) Solutions

- **Miradore**

Source: <https://www.miradore.com>

Miradore helps ensure device and data security as well as data compliance across an organization. It can easily encrypt all confidential data, separate business and personal use, enforce safe passcodes and screen locks, and prevent the use of unwanted applications.

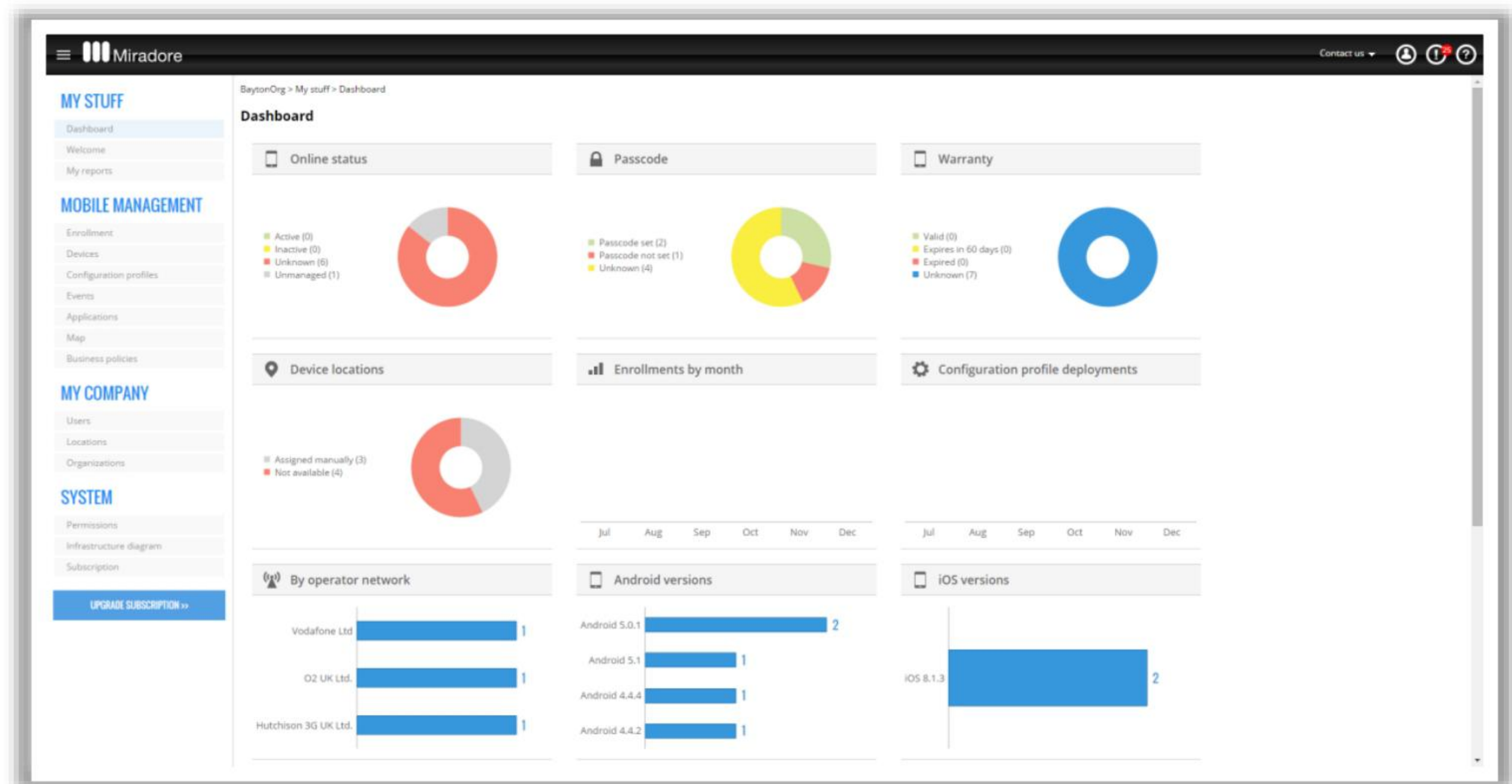


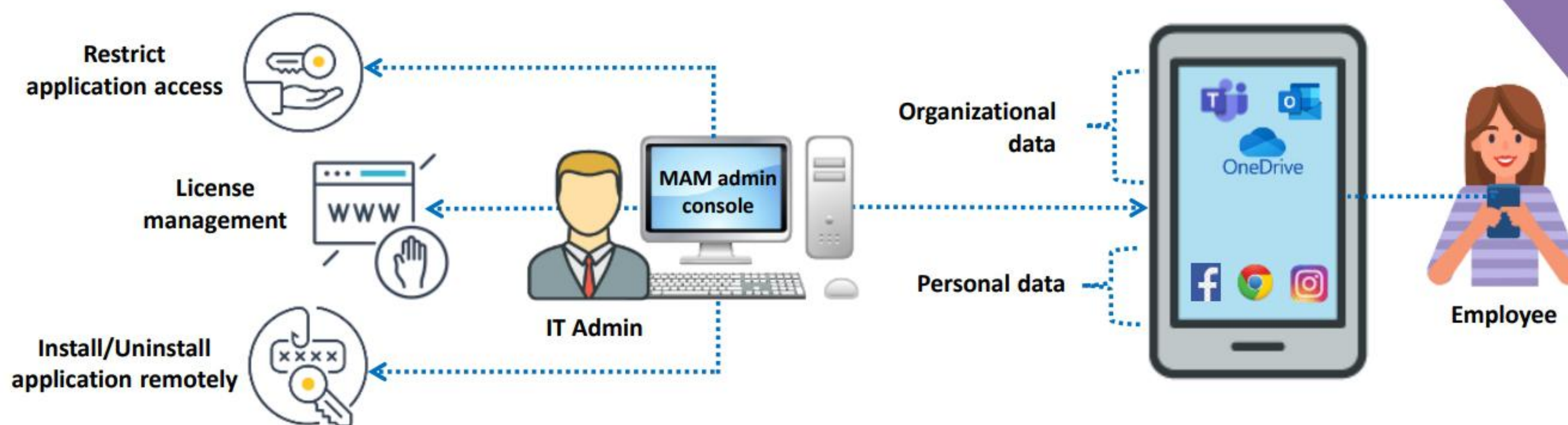
Figure 12.3: Screenshot of Miradore

Following are some examples of additional MDM solutions:

- AirWatch (<https://www.vmware.com>)
- Microsoft Intune (<https://www.microsoft.com>)
- IBM MaaS360 (<https://www.ibm.com>)
- XenMobile (<https://www.citrix.com>)
- Absolute Manage MDM (<http://www.absolute.com>)

Mobile Application Management Solutions

➡ Mobile application management (MAM) is a software or service that enables network defenders to **secure**, **manage**, and **distribute** enterprise applications on employee mobile devices

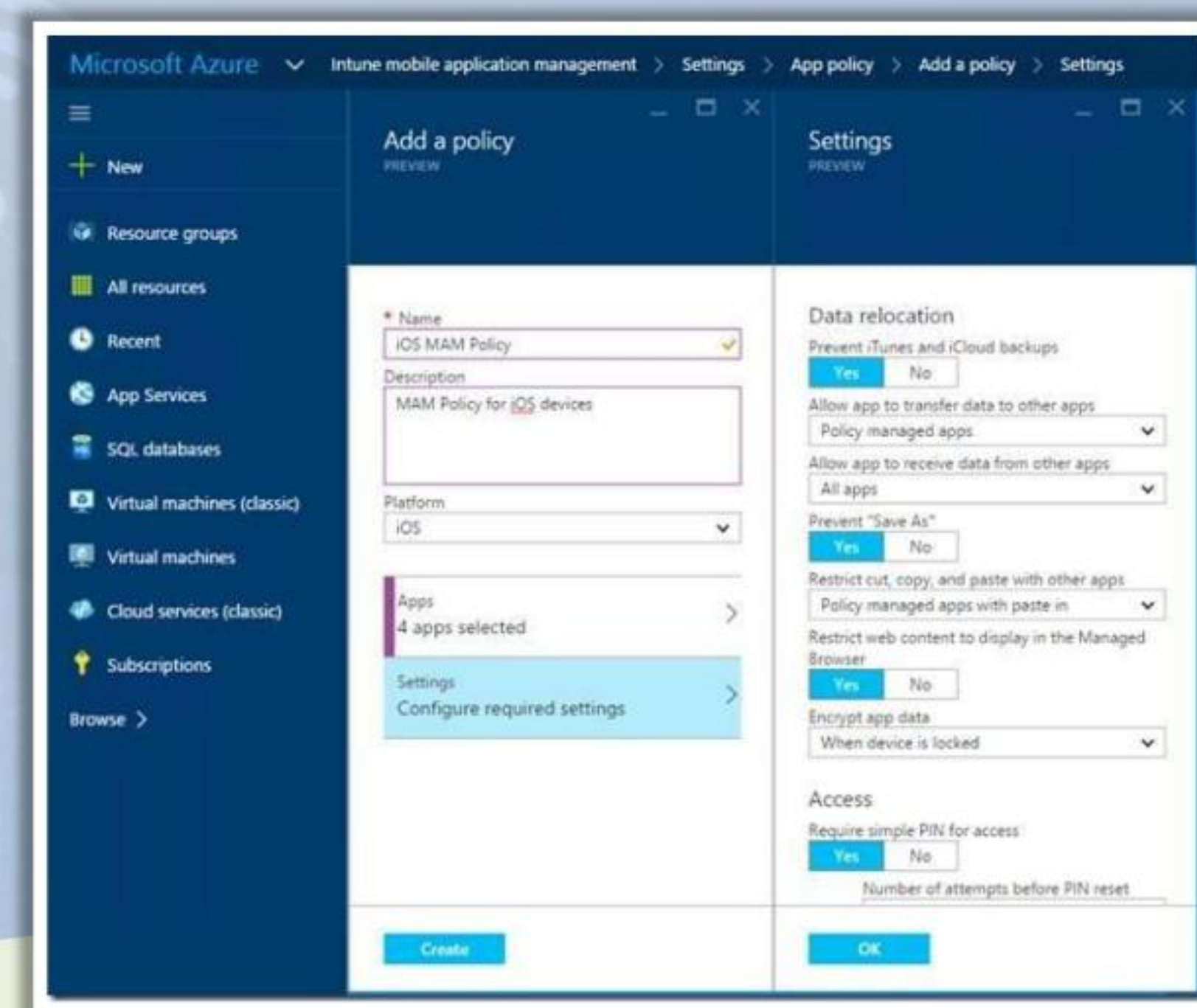


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Application Management Solutions (Cont'd)

Microsoft Intune

Intune MAM is a suite of Intune management features that lets users **publish**, **push**, **configure**, **secure**, **monitor**, and **update** mobile apps



<https://www.microsoft.com>

✓ AppStation's MAM
<https://www.mobileiron.com>

✓ Scalefusion Application Management
<https://scalefusion.com>

✓ ManageEngine Mobile Device Manager Plus
<https://www.manageengine.com>

✓ Apriorit Enterprise Mobile Device and Application Management
<https://www.apriorit.com>

✓ Appaloosa
<https://www.appaloosa.io>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Application Management Solutions

Mobile application management (MAM) software and services enable an organization to secure, manage, and distribute enterprise applications on user mobile devices, without interfering with personal apps and data. Enterprise Application Management allows removing the access to a particular application for employees who left the organization. MAM can be applied to company-owned mobile devices and BYOD. It also enables the separation of enterprise apps and data from personal content on the same device.

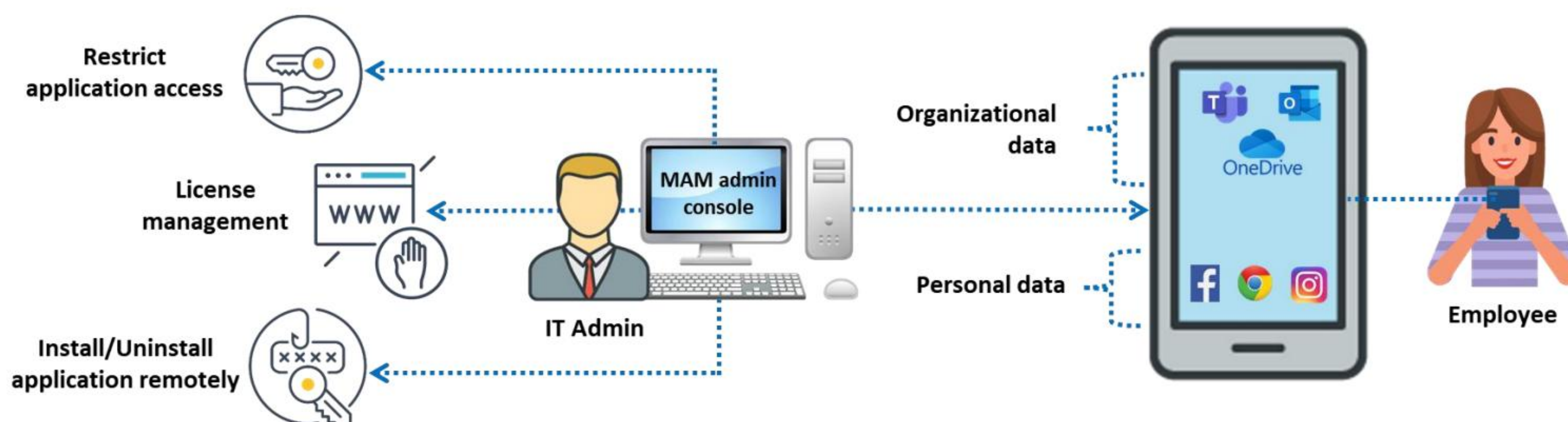


Figure 12.4: Mobile application management

Common features provided by MAM solutions:

- Device activation
- Enrollment and provisioning capabilities
- Remote wipe and other device-level functionalities
- Remote management does not require possession of the device
- Need minimal admin intervention and zero user action.

Services provided by Enterprise Application Management (MAM):

- Application delivery (enterprise app store)
- Software Licensing
- Application configuration
- Application authorization
- Application usage tracking
- Application lifecycle management
- Application updating
- Application performance monitoring
- User authentication
- Crash log reporting
- User and group access control
- App version management
- Push services
- Reporting and tracking
- Usage analytics
- Event management
- App wrapping

Examples of Mobile Application Management (MAM)

- **Microsoft Intune**

Source: <https://www.microsoft.com>

Intune MAM is a suite of Intune management features that lets organizations publish, push, configure, secure, monitor, and update mobile apps for users.

Intune MAM supports two configurations:

- **Intune MDM + MAM:** Apps are managed using MAM and app protection policies on devices that are enrolled with Intune MDM.

- **MAM without device enrollment (MAM-WE):** Apps are managed using MAM and app protection policies on devices that are not enrolled with Intune MDM.

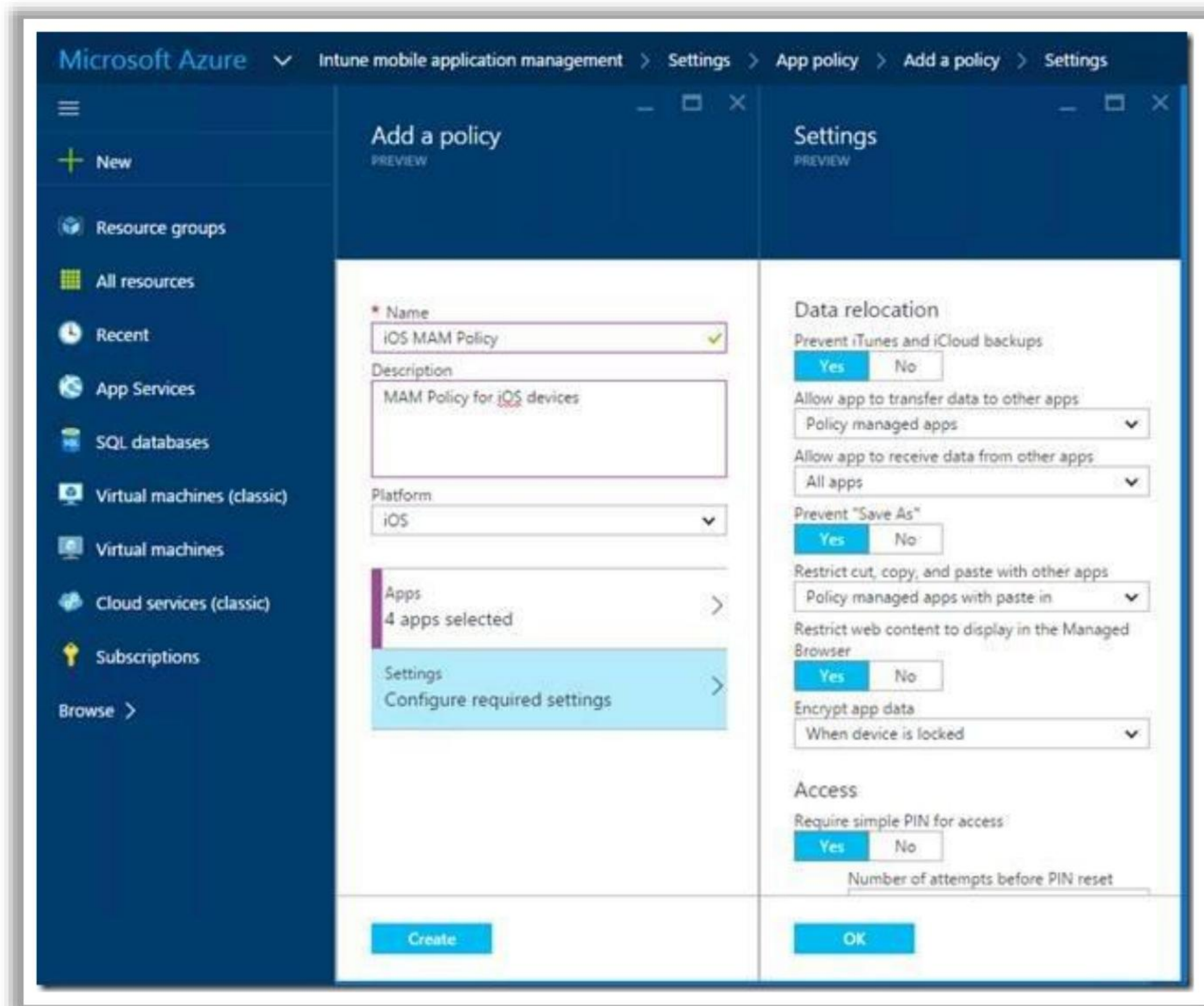
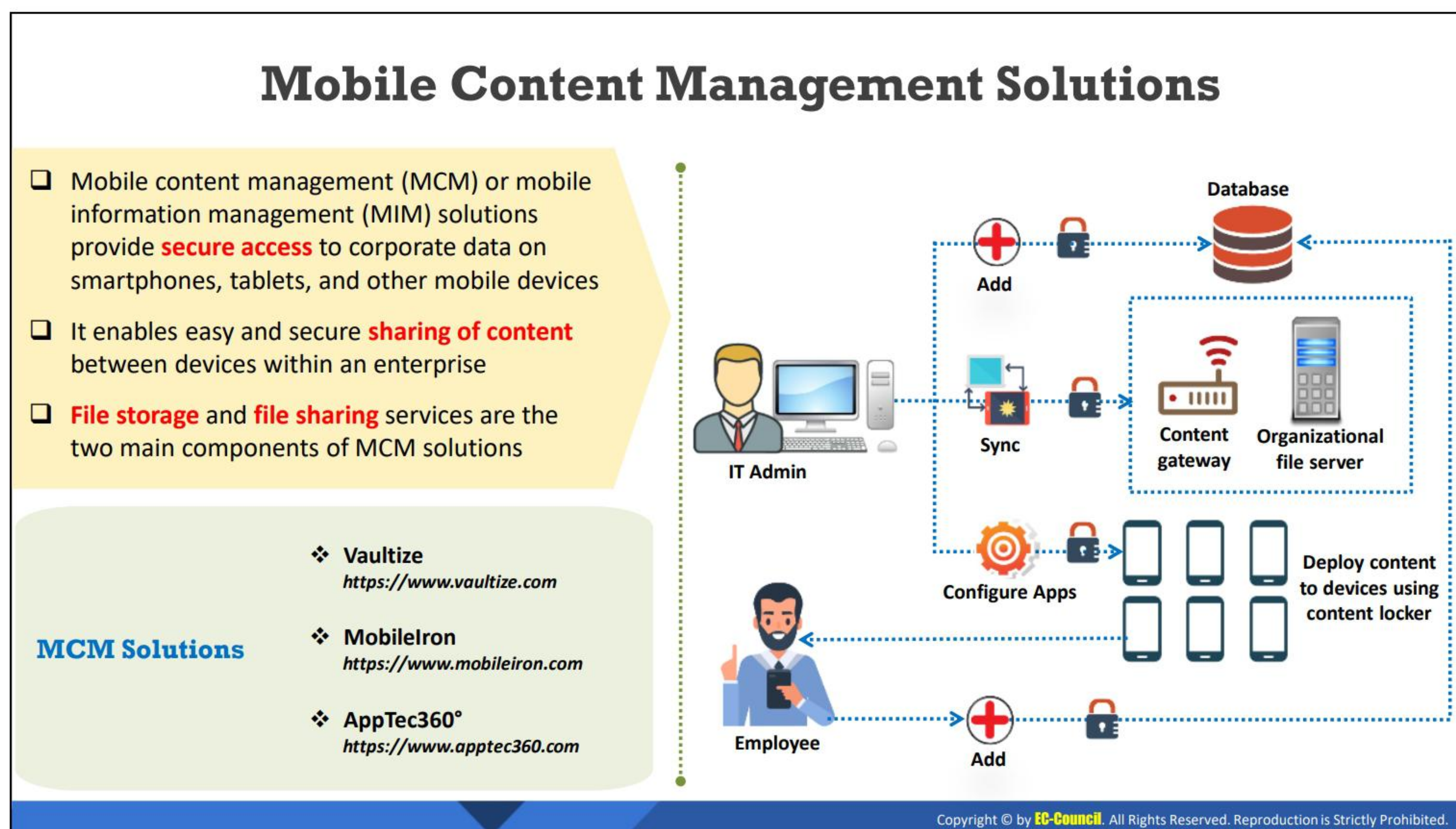


Figure 12.5: Microsoft Intune MAM

- AppStation's MAM (<https://www.mobileiron.com>)
- Scalefusion Application Management (<https://scalefusion.com>)
- ManageEngine Mobile Device Manager Plus (<https://www.manageengine.com>)
- Apriorit Enterprise Mobile Device and Application Management (<https://www.apriorit.com>)
- Appaloosa (<https://www.appaloosa.io>)



Mobile Content Management Solutions

Mobile content management (MCM) or mobile information management (MIM) solutions provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across the organizational networks without compromising with the speed. They enable easy and secure sharing of content between devices within an enterprise. File storage and file sharing services are the two main components of MCM solutions. MCM involves encrypting important information and allowing accessing, transmitting, or storing important information on only authorized apps using strong password protection policies.

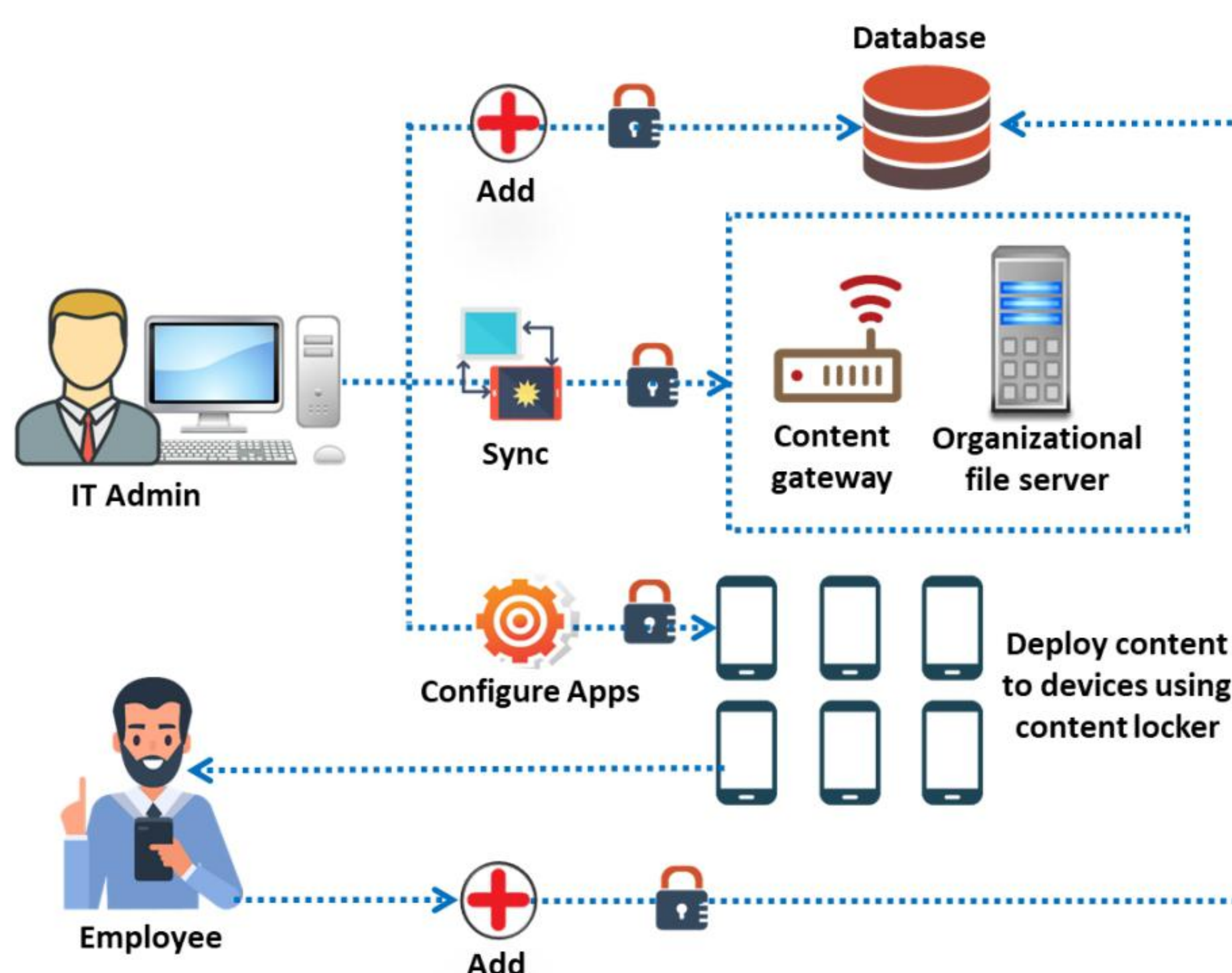


Figure 12.6: Mobile content management

MCM enables:

- **Multi-channel content delivery capabilities** that feature the management of a central content repository while delivering the content to devices simultaneously.
- **Content access control:** Access control to content includes
 - Authorization
 - Authentication
 - Access approval to content
 - Download control
 - Wipe-out for specific users
 - Time-specific access
- **Specialized templating system:** There are two approaches for adapting to mobile CMS templates.
 - **Multi-client approach** allows to view different versions of a site on the same domain and presents suitable templates based on the devices used by clients for viewing the website.
 - **Multi-site approach** displays mobile sites on a targeted sub-domain.
- **Location-based content delivery** provides content to mobile devices based on their current physical location.

Examples of MCM Solutions:

- Vaultize (<https://www.vaultize.com>)
- MobileIron (<https://www.mobileiron.com>)
- AppTec360° (<https://www.apptec360.com>)



Mobile Threat Defense Solutions

Mobile threat defense (MTD)/mobile threat management (MTM)/mobile threat prevention (MTP) protects organizations and their employees from threats on iOS and Android mobiles using different security technologies. The agents installed on the devices scan them for various mobile attacks using advanced threat intelligence. It uses machine learning and real-time analysis to protect mobile endpoints. MTD generate alerts for the enterprise mobility management (EMM) solutions to perform appropriate actions (switching mobiles into the quarantine state).

The MDM and MAM management tools only allow to set baseline management profiles for mobile devices and applications used within organizations. These two management tools lack insights related to app characteristics, protection against threats and user behaviors, reacting to threats dynamically, and providing continuous visibility of device health and trust. MTD extends EMM/MDM with additional security capabilities because it works with devices and secures them against the following attacks.

- It secures against device/physical threats by adding active threat detection and risk-based mobile management for more educated policy enforcement.
- It secures against malware.
- It secures against phishing.
- It secures against network attacks.

Factors to Consider Before Selecting an MTD solution:

The best suited MTD solution for an organization depends on

- The OS employed by the organization

- Mobile approach (BYOD or COPE)
- Type of access given to employees on their devices
- The EMM employed by the organization

Examples of MTD:

- MobileIron Threat Defense (MTD) (<https://www.mobileiron.com>)
- Pradeo Security Mobile Threat Defense (<https://www.pradeo.com>)
- Zimperium Mobile Threat Defense (MTD) (<https://www.zimperium.com>)
- Wandera Mobile Threat Defense (<https://www.wandera.com>)
- Lookout MTD (<https://www.lookout.com>)

The infographic is titled "Mobile Email Management Solutions". It features a blue header with a white icon of a computer monitor with a wrench and screwdriver. Below the header, a grey box contains the text: "Mobile email management (MEM) solutions ensures the security of the **corporate email infrastructure** and **data**". The main content is divided into two columns. The left column, titled "Features of MEM solutions", lists four features with checkmarks: "Pre-configures emails on devices remotely", "Ensures that only approved apps and devices can access the emails", "Prevents unauthorized access of email attachments", and "Pre-installs the email client to be used for e-mail access". The right column, titled "MEM Solutions", lists three solutions with icons: "42Gears MEM" with a gear icon and URL <https://www.42gears.com>, "Hexnode Mobile Email Management" with a clock icon and URL <https://www.hexnode.com>, and "Mimecast Mobile Email Management" with a share icon and URL <https://www.mimecast.com>. A footer at the bottom right states: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."




Mobile Email Management Solutions

Mobile email management (MEM) solutions ensures the security of the **corporate email infrastructure** and **data**

Features of MEM solutions

- ✓ Pre-configures emails on devices remotely
- ✓ Ensures that only approved apps and devices can access the emails
- ✓ Prevents unauthorized access of email attachments
- ✓ Pre-installs the email client to be used for e-mail access

MEM Solutions

-  **42Gears MEM**
<https://www.42gears.com>
-  **Hexnode Mobile Email Management**
<https://www.hexnode.com>
-  **Mimecast Mobile Email Management**
<https://www.mimecast.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Email Management Solutions

Mobile email management (MEM) solutions ensure the security of the corporate email infrastructure and data on mobile devices. MEM allows

- Controlling mobile devices that access emails
- Prevention of data loss
- Enforcing strict compliance policies
- Encrypting sensitive corporate data

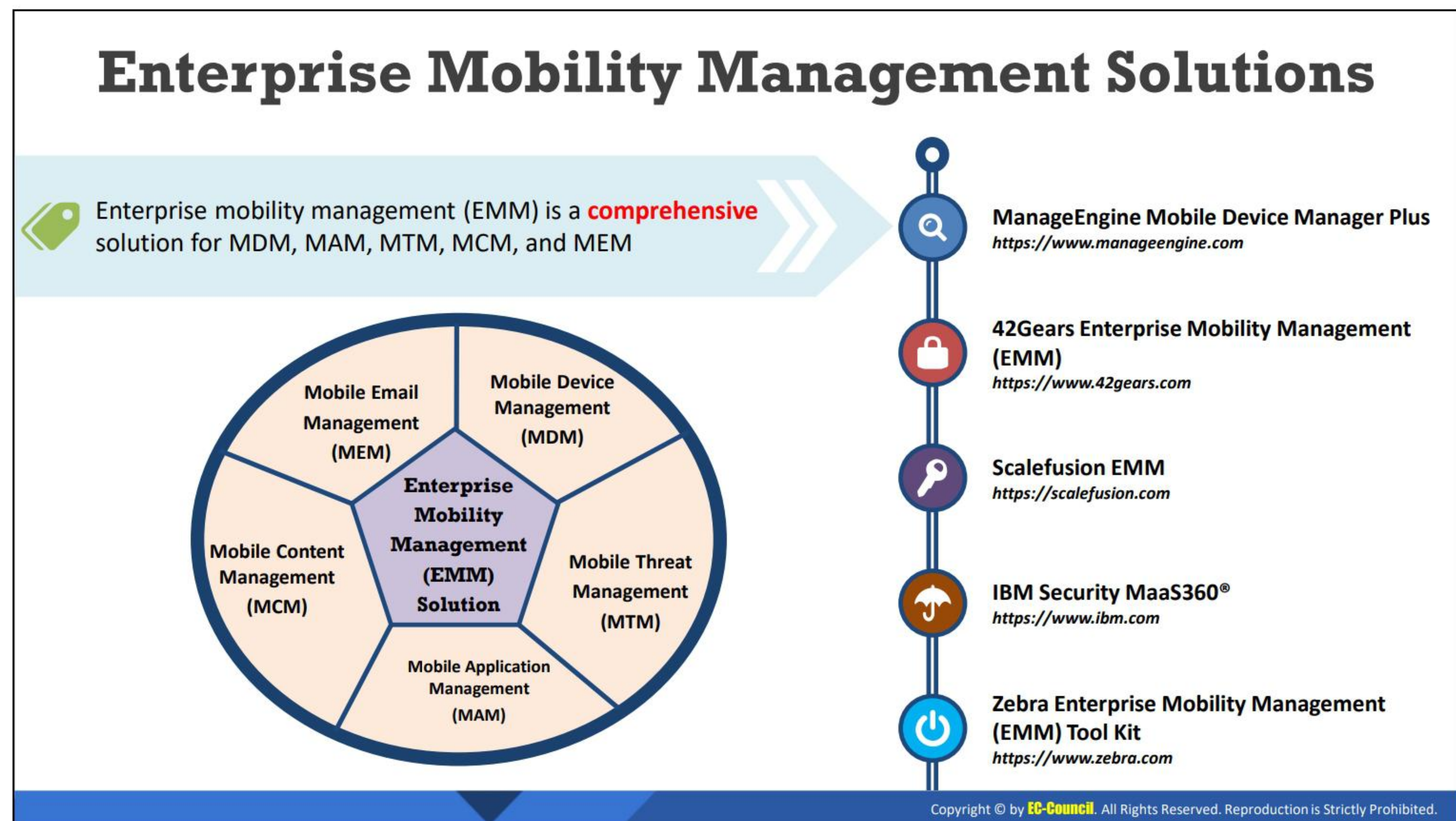
Common MEM Key Features:

- **Preconfiguring email on devices remotely:** Using MDM, MEM allows
 - Creating email accounts by associating an email policy with employee devices.
 - Configuring the email signature and setting up a default email account for users.
- **Ensure only approved apps and devices can access e-mail:** Using MDM, MEM provides
 - An additional layer of encryption through S/MIMEMDM.
 - Configuring Simple Certificate Enrollment Protocol (SCEP) for iOS and Windows devices to secure emails using certificates.
- **Prevent unauthorized access of email attachments:** Using MDM, MEM assures
 - Securing email attachments during transit and after downloading.
 - Ensuring secure viewing and storage of key attachments using the built-in document viewer of MEM, and MDM apps.

- Restricting document sharing to other devices or cloud services to prevent security breaches.
- **Pre-installing the email client to be used for email access:** The managed app configurations of MDM allow
 - Customizing the managed email app functionalities to suit the organizational requirements.
 - Distributing the app to devices.
 - Preconfiguring parameters (account type, domain name, and email signature) to make the app ready for corporate usage after installation.
 - Preconfiguring the app permissions.

Examples of MEM Solutions:

- 42Gears MEM (<https://www.42gears.com>)
- Hexnode Mobile Email Management (<https://www.hexnode.com>)
- Mimecast Mobile Email Management (<https://www.mimecast.com>)



Enterprise Mobility Management Solutions

Enterprise mobility management (EMM) is a comprehensive solution responsible for MDM, MAM, MTM, MCM, and MEM. It safeguards the enterprise data accessed and used by employee mobile devices.

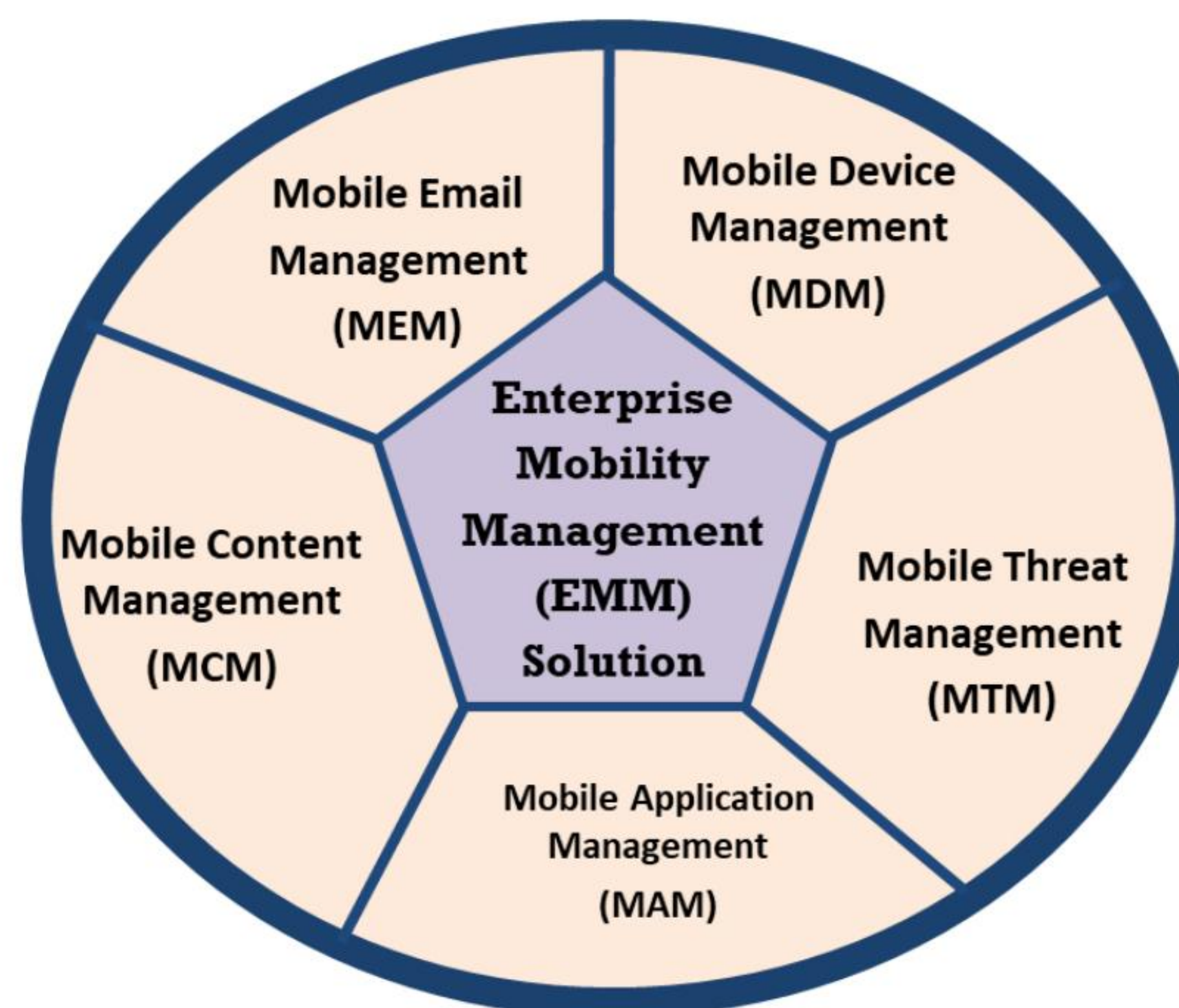


Figure 12.7: Enterprise Mobility Management Solution

Specifically, EMM is responsible for:

- Device management to provide the foundation for EMM solutions by
 - Enabling automatic device configuration
 - Allowing employees to be productive on the mobile devices they like to use

- Wiping enterprise data from mobile devices selectively without interfering with personal data
- Securing and managing mobile devices across multiple OSes (Android, iOS, macOS, and Windows 10)
- Content management
 - Encrypt email attachments
 - Establish DLP controls to secure corporate content
 - Secure corporate data distribution to mobile devices by applying content level policies (e.g., device-independent encryption keys, authentication, and file sharing)
- Application management
 - Protect applications on any device
 - Create and manage an enterprise app store
 - Provide authentication for end users on the device
 - Separate business and personal apps on mobile devices
 - User and identity management
- Mobile threat management
 - Protect organizations and their employees from threats on iOS and Android mobiles using different security technologies
- MEM
 - Provide security to the corporate email infrastructure and data on mobile devices

Examples of EMM Solutions:


- ManageEngine Mobile Device Manager Plus (<https://www.manageengine.com>)
- 42Gears Enterprise Mobility Management (EMM) (<https://www.42gears.com>)
- Scalefusion EMM (<https://scalefusion.com>)
- IBM Security MaaS360® (<https://www.ibm.com>)
- Zebra Enterprise Mobility Management (EMM) Tool Kit (<https://www.zebra.com>)


Unified Endpoint Management Solutions


Unified endpoint management (UEM) solutions ensure **remote provisioning, managing, controlling, and securing** Internet-enabled devices from a single interface


Features of UEM


- Remote, manual, or automatic pushing of updates
- Configuration for on-device security policies
- Supporting employee-owned devices
- Erasing the data of lost or stolen devices remotely
- Tracking device usage
- Threat detection and mitigation
- API framework for custom applications

**MobileIron UEM**
<https://www.mobileiron.com>

**Ivanti Unified Endpoint Manager**
<https://www.ivanti.com>

**Workspace ONE**
<https://www.vmware.com>

**ManageEngine Desktop Central**
<https://www.manageengine.com>

**42Gears UEM**
<https://www.42gears.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Unified Endpoint Management Solutions

Unified endpoint management (UEM) solutions help in managing and controlling Internet-enabled mobile devices, desktops, applications, and content across the organization from a single interface. It provides security, management, and provisioning of mobile devices. UEM solutions address the problems of IT managers by extending MDM and EMM solutions.

Features and Capabilities of UEM

UEM solutions handle the unique security requirements in mobile enterprises by providing:

- App containerization
- Multi-OS environment
- Closed-loop automation features
- Certificate-based identity management
- Security for enterprise email, apps, and content
- Self-service features to simplify IT management
- DLP features to define open-in and copy/paste functions
- Help users maintain compliance with the corporate policies
- Secure multi-user profiles to securely allow users to share a single device
- Highly effective security measures that are invisible to the end users
- Per-app VPN technology that provides corporate network access to authorized apps only

- Allow users to find and install critical enterprise apps (corporate email, calendar, etc.)
- Separate and manage highly sensitive personal and corporate data on mobile devices.
- Remote, manual, or automatic pushing of updates
- Configuration for on-device security policies
- Supporting employee-owned devices
- Erasing the data of lost or stolen devices remotely
- Tracking device usage
- Threat detection and mitigation
- API framework for custom applications

UEM Components

The key components that define the attributes of UEM solutions are:

- **CMT**
CMT provides IT infrastructure to ensure the efficient working of mobile enterprises while enhancing the service to end users.
- **MDM**
MDM provides a foundation for UEM solutions by allowing the IT team to
 - Secure corporate email
 - Certificate-based security
 - Automatic device configuration
 - Allow employees to be productive on the mobile devices they like to use
 - Wipe enterprise data from mobile devices selectively without interfering with personal data
 - Secure and manage mobile devices across multiple OSes (Android, iOS, macOS, and Windows 10)
- **MAM**
MAM provides IT infrastructure to
 - Protect applications on any device
 - Create and manage an enterprise app store
 - Provide authentication for end users on a device
 - Separate business and personal apps on mobile devices

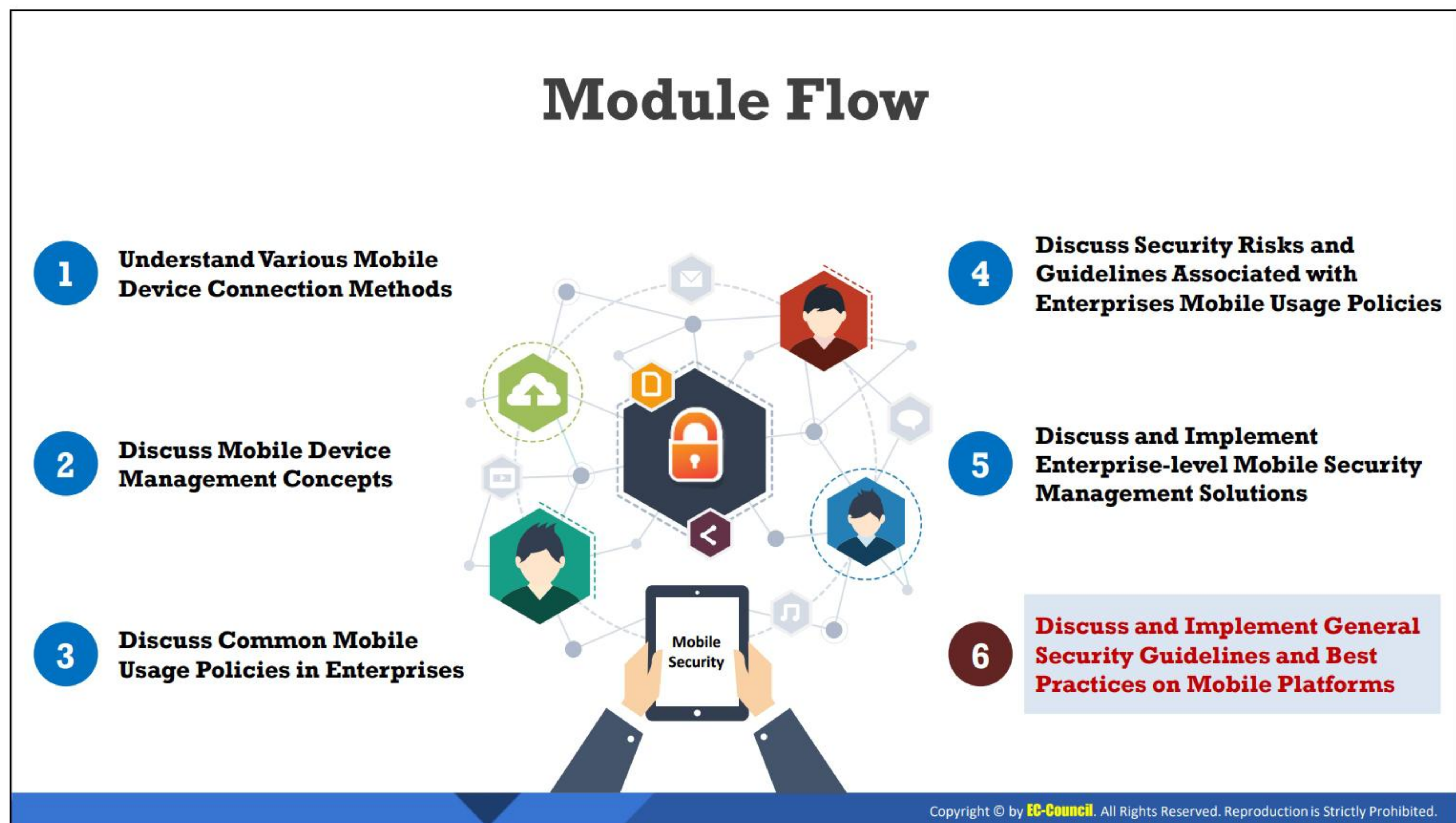
- **MCM**

MCM provides IT infrastructure to

- Encrypt email attachments
- Establish DLP controls to secure corporate content
- Secure corporate data distribution to mobile devices by applying content level policies (device-independent encryption keys, authentication, and file sharing)

Examples of UEM Solutions for Mobile Engagement:









- Mobileiron UEM (<https://www.mobileiron.com>)
- Ivanti Unified Endpoint Manager (<https://www.ivanti.com>)
- Workspace ONE UEM (<https://www.vmware.com>)
- ManageEngine Desktop Central (<https://www.manageengine.com>)
- 42Gears UEM (<https://www.42gears.com>)



Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms

Enterprise-level mobile security management solutions can only deliver their promised benefits if they are backed by strong mobile device security practices. The objective of this section is to explain the general security guidelines and best practices to be implemented for securing mobile platforms.

Mobile Application Security Best Practices

-  Ensure that the apps do not **save** passwords
-  Avoid the use of **query string** while handling sensitive data
-  Use **code obfuscation** and encryption to secure the application source code
-  Implement **two-factor authentication**
-  Use **SSL/TLS** to send data over secure channels
-  Avoid **caching** app data
-  Perform **validation checks** on input data
-  Implement **secure** session management



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Application Security Best Practices

Security best practices that protect mobile applications:

- Ensure that the apps do not save passwords
- Avoid using query string while handling sensitive data
- Use code obfuscation and encryption to secure the application source code
- Implement two-factor authentication
- Use SSL/TLS to send data over a secure channel
- Avoid caching app data
- Perform validation checks on input data
- Implement secure session management
- Protect application setting
- Use server-side authentication
- Use cryptographic algorithms and key management
- Build threat models to defend data
- Ensure that employees download trusted apps from enterprise app stores
- Use containerization for critical corporate data
- Perform regular mobile security audits
- Regular software updates
- Implement jailbreak protection



Mobile Data Security Best Practices

Security best practices that protect mobile data:

- Secure mobile infrastructure and strengthen the endpoints
- Encrypt the data stored on devices
- Enable over-the-air encryption using SSL, TLS, VPN, and WPA2
- Backup mobile data periodically
- Do not store extremely sensitive information on mobile devices
- Do not store passwords or PINs as contacts on your phone
- Use private data centers to store data and implement device authentication
- Maintain access control for devices and data
- Avoid public Wi-Fi networks
- Set automatic device locks when devices are not in use
- Ensure that users can access the corporate data from a secure central location
- Complete software updates and patches in a timely manner
- Educate employees to recognize suspicious emails
- Keep the antivirus and anti-malware software updated
- Train employees to encrypt hard drives and USBs before storing any work-related data on them



Mobile Network Security Guidelines

- 1 Disable **interfaces** such as Bluetooth, infrared, and Wi-Fi when not in use
- 2 Set **Bluetooth-enabled** devices to non-discoverable mode
- 3 Avoid connecting to **unknown Wi-Fi** networks and using public Wi-Fi hotspots
- 4 Connect your device to **encrypted** Wi-Fi networks only
- 5 Configure web accounts to use **secure** connections

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Network Security Guidelines

Security best practices that protect mobile networks:

- Disable interfaces such as Bluetooth, infrared, and Wi-Fi when not in use
- Set Bluetooth-enabled devices to non-discoverable mode
- Avoid connecting to unknown Wi-Fi networks and using public Wi-Fi hotspots
- Connect the mobile devices to encrypted Wi-Fi networks only
- Configure web accounts to use secure connections
- Isolate a group of users using different SSIDs and segment the traffic for these groups to different VLANs
- Apply different firewall rules and filters to different combinations of user groups or devices
- Configure web accounts to use secure connections

General Guidelines for Mobile Platform Security



General Guidelines for Mobile Platform Security

Given below are various guidelines that can help users to protect their mobile devices.

- Do not install too many applications and avoid auto-uploading photos to social networks
- Perform security assessment for the application architecture
- Maintain configuration control and management
- Install applications from trusted app stores
- Securely wipe or delete the data while disposing of devices
- Do not share any information within GPS-enabled apps unless required
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Disable wireless access such as Wi-Fi and Bluetooth if not in use
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Configure a strong passcode with the maximum possible length
- Update the OS and apps to keep them secure
- Enable Remote Management
- Do Not Allow Rooting or Jailbreaking
- Use remote wipe services such as Find My Device (Android) and Find My iPhone or Find My (Apple iOS) to locate your device if it is lost or stolen
- Encrypt the device and its backups

- Perform Periodic Backup and Synchronization
- Filter emails by configuring the server-side settings of the corporate email system
- Strengthen Browser Permission Rules
- Design and Implement Mobile Device Policies
- Control devices and applications
- Prohibit USB keys
- Manage the operating and application environments
- Press the power button to lock the device when not in use



Kaspersky Internet Security for Android

-  Kaspersky Internet Security for Android **blocks suspicious apps**, websites, and files
-  It allows you to **control access** to specific apps and stops spyware monitoring calls, texts, and location
-  It includes **anti-theft tools** to protect mobiles and data

Android Security Tools



<https://my.kaspersky.com>

-  **Avira Antivirus Security**
<https://www.avira.com>
-  **Avast Mobile Security**
<https://www.avast.com>
-  **McAfee Mobile Security**
<https://www.mcafeemobilesecurity.com>
-  **Lookout Mobile Security and Antivirus**
<https://www.lookout.com>
-  **Sophos Mobile Security**
<https://www.sophos.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Security Tools

- **Kaspersky Internet Security for Android**

Source: <https://my.kaspersky.com>

Kaspersky Internet Security for Android blocks suspicious apps, websites, and files. It allows you to control access to specific apps and stops spyware monitoring calls, texts, and location. It includes anti-theft tools to protect mobiles and data. It uses machine learning to combat new threats.

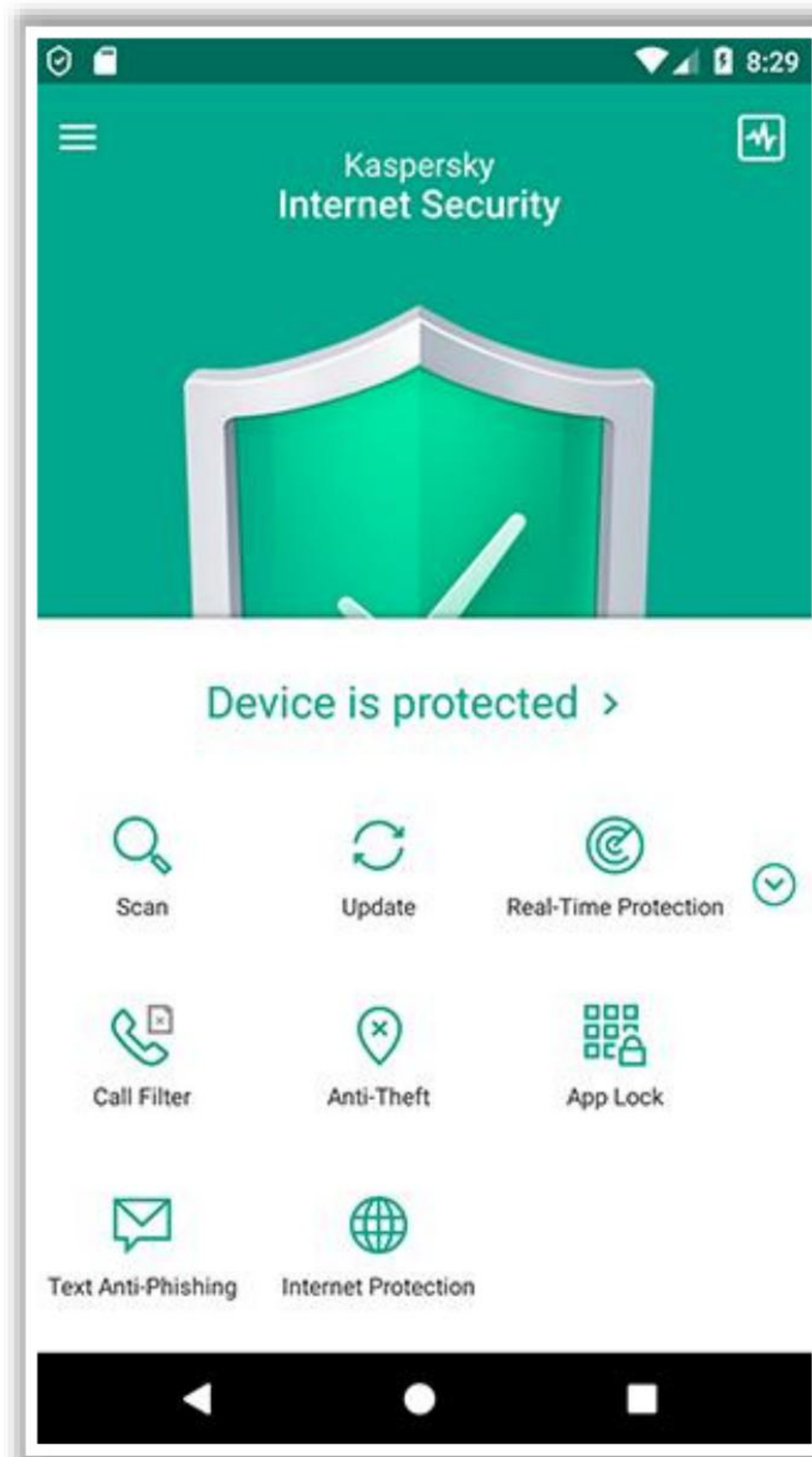


Figure 12.8: Screenshot of Kaspersky Mobile Antivirus

Following are some additional Android security tools:

- Avira Antivirus Security (<https://www.avira.com>)
- Avast Mobile Security (<https://www.avast.com>)
- McAfee Mobile Security (<https://www.mcafeemobilesecurity.com>)
- Lookout Mobile Security and Antivirus (<https://www.lookout.com>)
- Sophos Mobile Security (<https://www.sophos.com>)

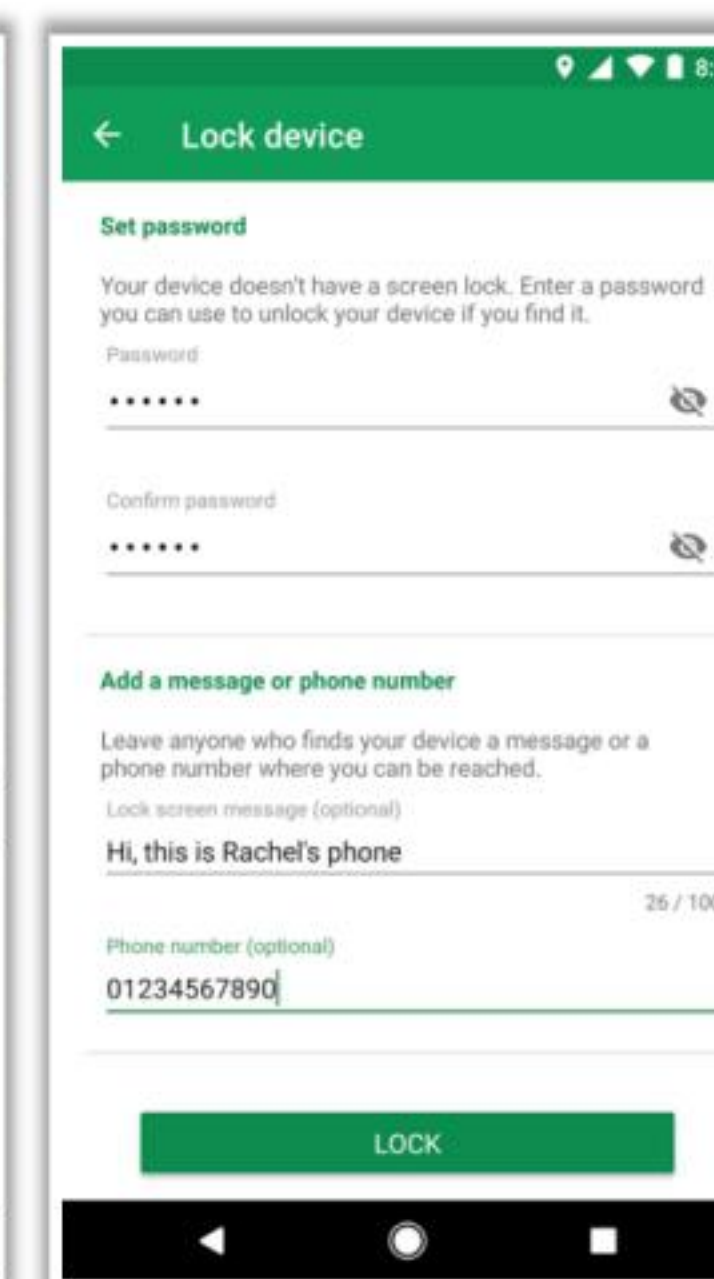
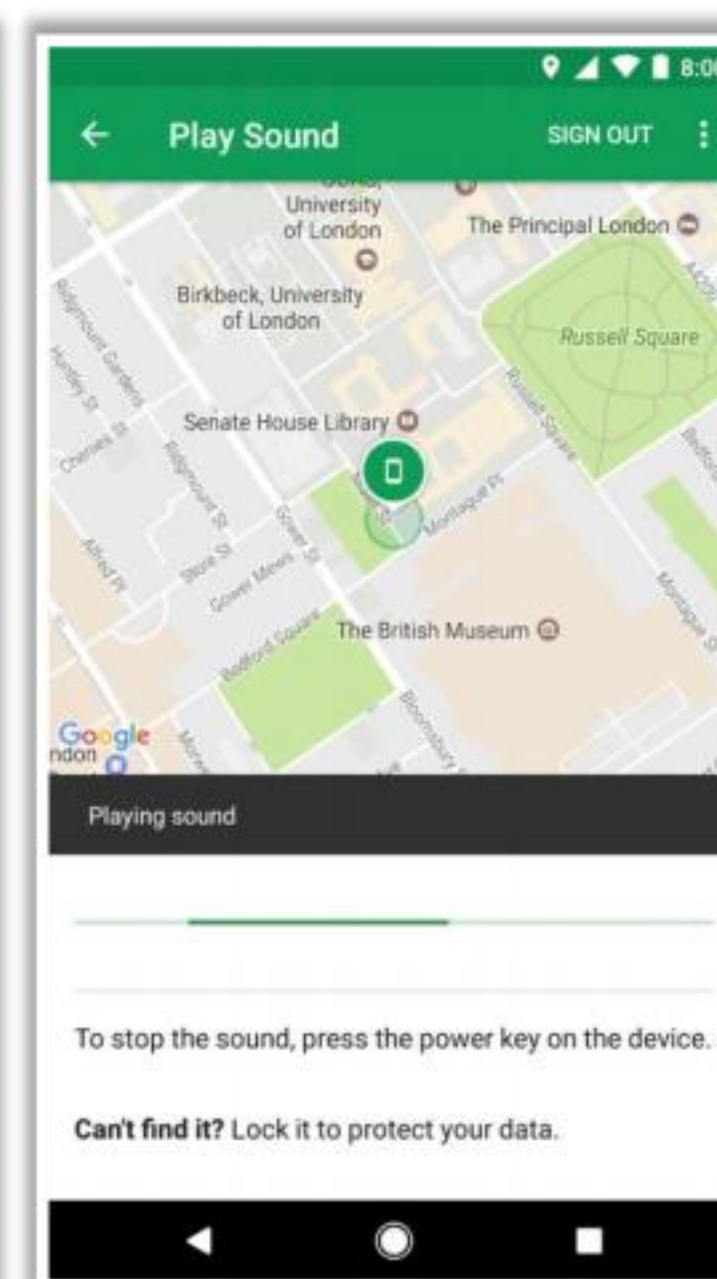
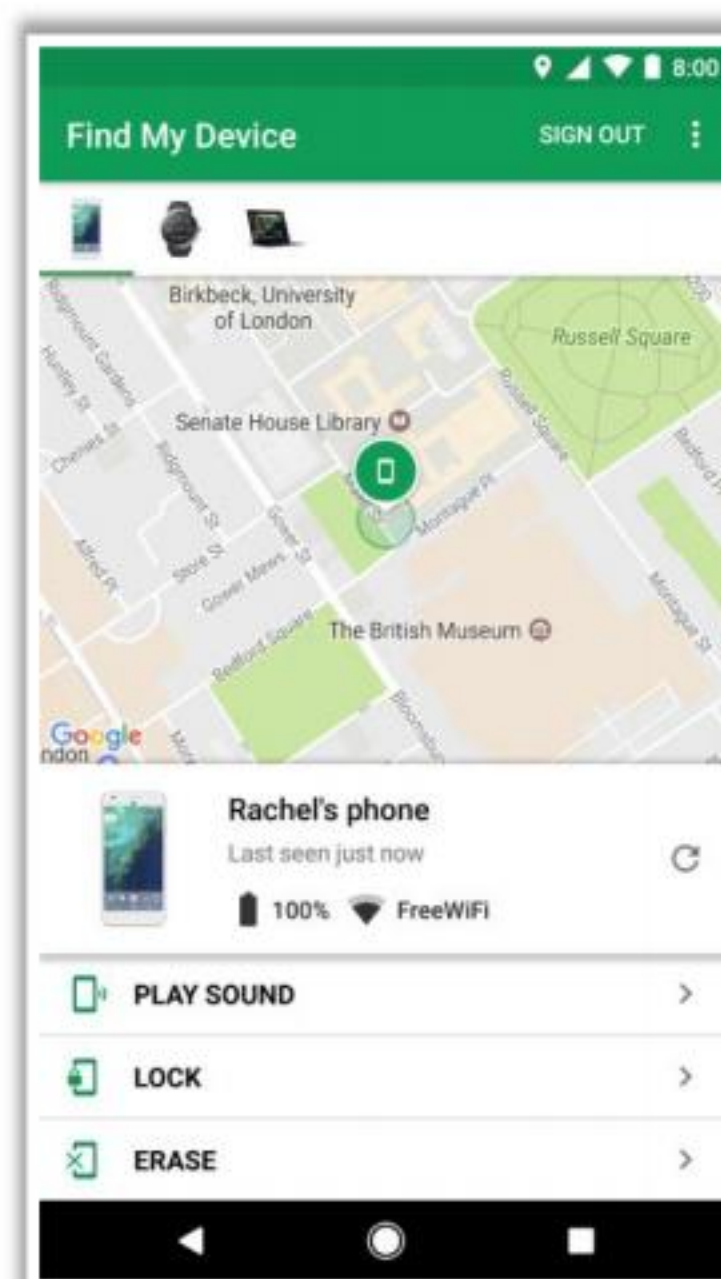
Android Device Tracking Tools: Google Find My Device



- Google's Find My Device helps you easily **locate a lost Android device** and keeps your information on the missing device safe while you look for it

To find, lock, or erase a lost or stolen device:

- Go to <https://www.google.com/android/find> and sign in to your Google Account
- If you have more than one device, click "**Lost device**" at the top of the screen
- The device gets a **notification**
- Locate the device on the map
- Pick what you want to do. If needed, first click "**Enable lock & erase**"
 - Play sound**: Rings your device at full volume for 5 minutes
 - Secure Device**: Locks your device with your PIN, pattern, or password
 - Erase Device**: Permanently deletes all data on your device



<https://www.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Tracking Tools: Google Find My Device

Android device tracking tools help you track and find the location of your Android device if it is lost, stolen, or misplaced.

Some widely used Android device tracking tools are listed below:

- Google Find My Device**

Source: <https://www.google.com>

Google Find My Device helps you to easily locate your lost Android device and keeps your information safe in the meantime. It also allows you to erase the information on the lost or stolen device. If users have Google Sync installed on a supported mobile device (including Android) with the Google Apps Device Policy app, they can use the Google Apps control panel to remotely find, lock, or erase a lost Android device.

One can select this service when a device is lost or stolen to erase all the data on the device and perform a factory reset. All the data are erased from the device (and SD card, if applicable), including email, calendar, contacts, photos, music, and the user's personal files.

To use Find My Device, your lost device must

- Be turned on
- Be signed in to a Google Account
- Be connected to mobile data or Wi-Fi
- Be visible on Google Play

- Have Location turned on
- Have Find My Device turned on

To find, lock, or erase a lost or stolen device, follow the steps given below:

- Go to **<https://www.google.com/android/find>** and sign in to your **Google Account**.
- If you have more than one device, click the lost device at the top of the screen.
- The device gets a notification.
- On the map, see where the device is.
 - The location is approximate and might not be accurate.
 - If your device cannot be found, then you will see its last known location, if available.
- Pick what you want to do. If needed, first click **Enable lock & erase**.
 - **Play Sound:** Rings your device at full volume for 5 minutes, even if it is set to silent or vibrate.
 - **Secure Device:** Locks your device with your PIN, pattern, or password. If you do not have a lock, you can set one. To enable someone to return your device to you, you can add a message or phone number to the lock screen.
 - **Erase Device:** Permanently deletes all data on your device (but might not delete SD cards). Subsequently, Find My Device will not work on the device.

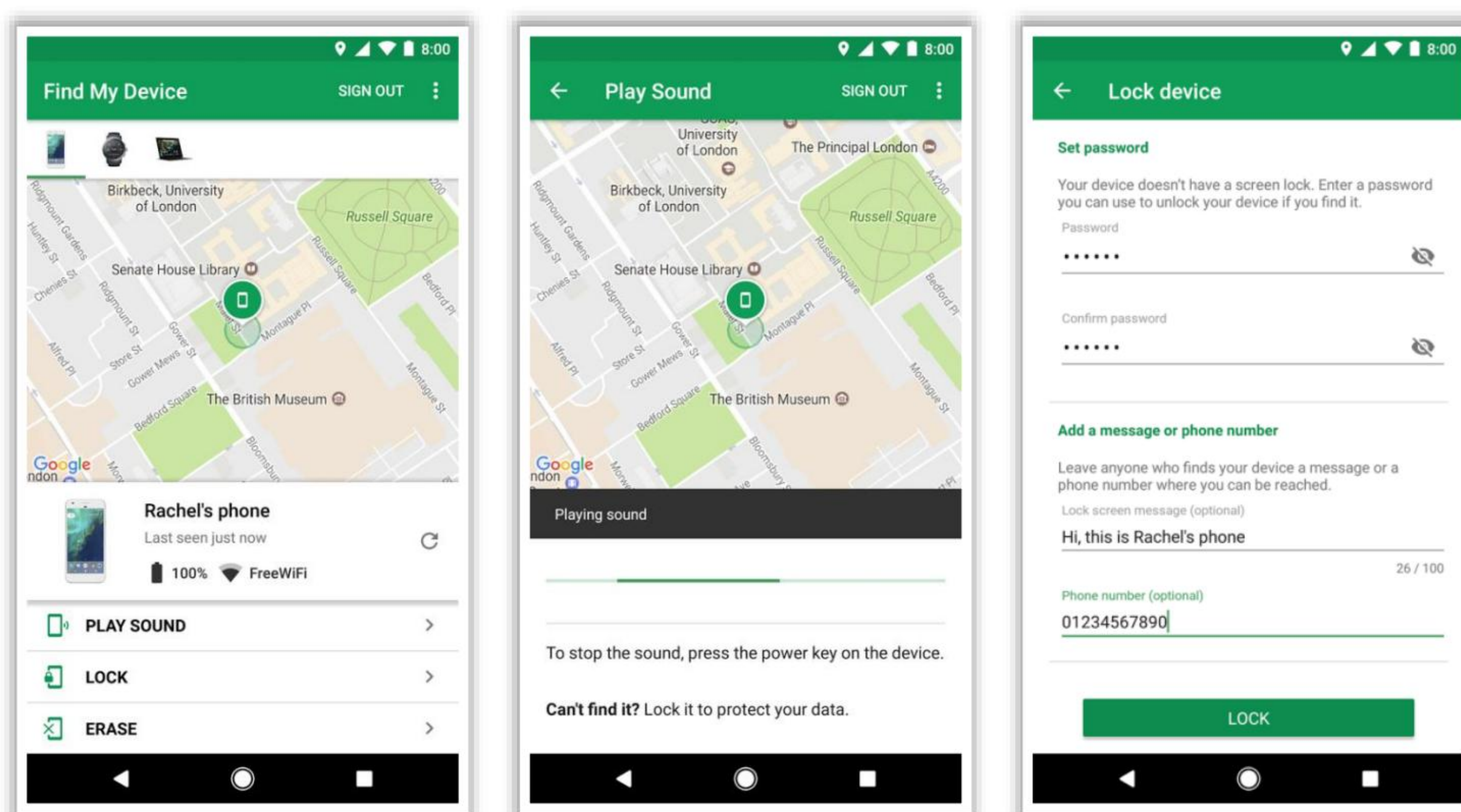


Figure 12.9: Screenshot of Find My Device service

iOS Device Security Tools

Avira Mobile Security

This tool provides features such as **web protection** and **identity safeguarding**, identifies phishing websites that target you personally, secures emails, tracks your device, identifies suspicious activities, organizes the device memory, and backs up all contacts



<https://www.avira.com>

**Norton Mobile Security**
<https://us.norton.com>

**LastPass Password Manager**
<https://www.lastpass.com>

**Lookout Mobile Security**
<https://www.mylookout.com>

**SplashID Safe Password Manager**
<https://www.splashid.com>

**Webroot Mobile Security**
<https://www.webroot.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Device Security Tools

- **Avira Mobile Security**

Source: <https://www.avira.com>

Avira Mobile Security provides features such as web protection and identity safeguarding, identifies phishing websites that target a specific user, tracks a device, organizes the device memory, and backs up all contacts and other data for all iOS devices.

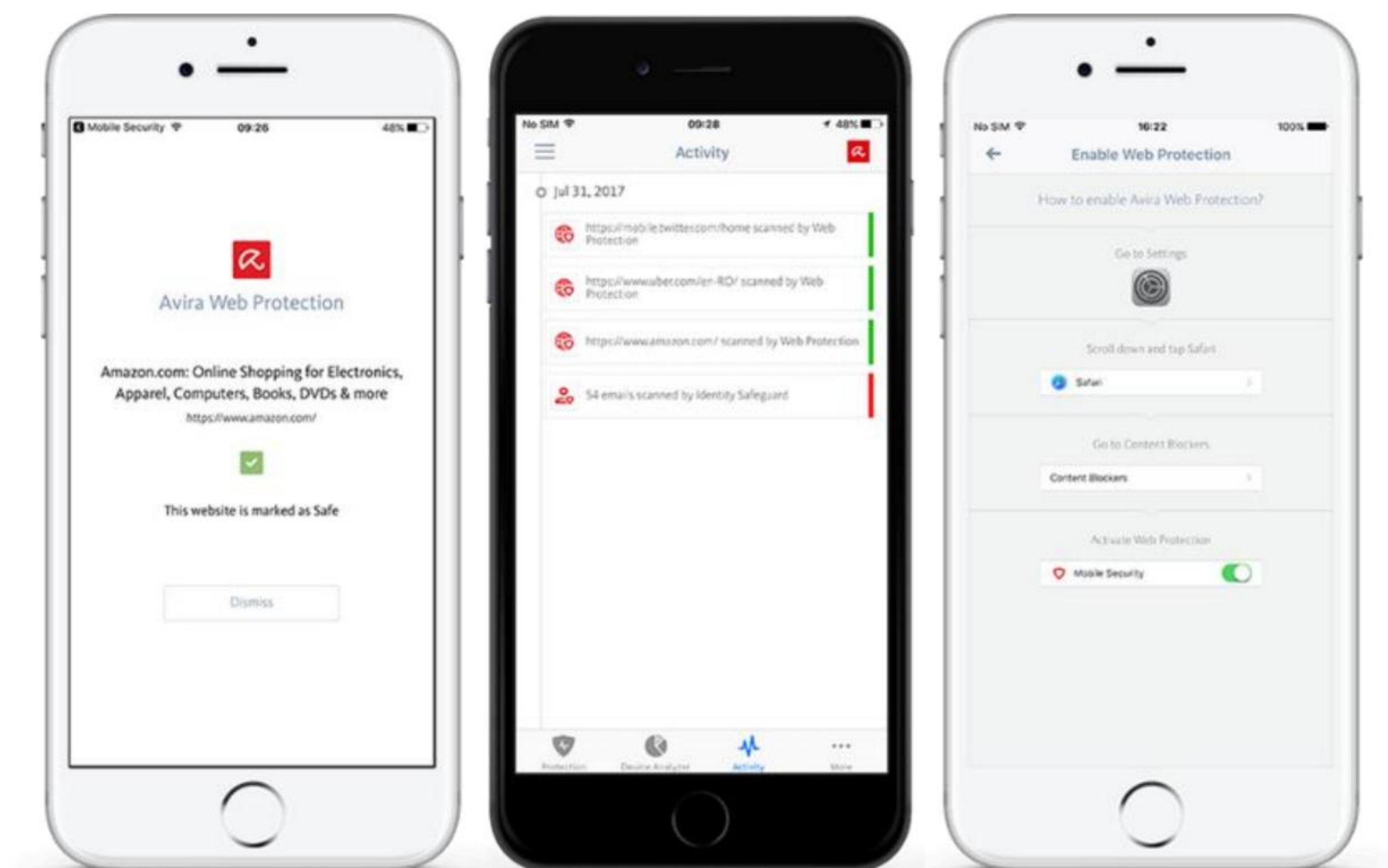


Figure 12.10: Screenshots of Avira Mobile Security

Following are some additional iOS device security tools:

- Norton Mobile Security (<https://us.norton.com>)
- LastPass Password Manager (<https://www.lastpass.com>)
- Lookout Mobile Security (<https://www.lookout.com>)
- SplashID Safe Password Manager (<https://www.splashid.com>)
- Webroot Mobile Security (<https://www.webroot.com>)

Module Summary

- ❑ This module has discussed various mobile device connection methods
- ❑ It has discussed the concepts of mobile device management as well as the common mobile usage policies in enterprises
- ❑ Furthermore, it has discussed the security risks and guidelines associated with enterprise mobile usage policies
- ❑ Moreover, this module discussed enterprise-level mobile security management solutions
- ❑ Finally, this module presented an overview of general security guidelines and best practices for mobile platforms
- ❑ In the next module, we will discuss IoT device security in detail



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module has discussed various mobile device connection methods. It has discussed the concepts of mobile device management as well as the common mobile usage policies in enterprises. Furthermore, it has discussed the security risks and guidelines associated with enterprise mobile usage policies. Moreover, this module discussed enterprise-level mobile security management solutions. Finally, this module presented an overview of general security guidelines and best practices for mobile platforms.

In the next module, we will discuss IoT device security in detail.