

Module 08

Mobile Device Security



Module Objectives

1

2

3

4

5

6

Module Flow

1. **Understand Various Mobile Device Connection Methods**
2. **Discuss Mobile Device Management Concepts**
3. **Discuss Common Mobile Usage Policies in Enterprises**



4. **Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies**
5. **Discuss and Implement Enterprise-level Mobile Security Management Solutions**
6. **Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms**

Mobile Device Connection Methods



Near-field Communication (NFC)

- It employs **electromagnetic induction** to enable communication between the devices connected within 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

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



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



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 **radio-frequency technology**, which identifies a person or object using their tags (unique labels)

Module Flow

1. Understand Various Mobile Device Connection Methods
2. **Discuss Mobile Device Management Concepts**
3. Discuss Common Mobile Usage Policies in Enterprises



4. Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
5. Discuss and Implement Enterprise-level Mobile Security Management Solutions
6. Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms

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

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

Mobile Security Management

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



Enterprise Mobility Management

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

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**

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 a message from an application to a mobile device without any explicit request from the user

Mobile Device Management (MDM) (Cont'd)



Geolocation

real-world geographical location

Full Device Encryption

encrypt all the information

Geofencing

virtual fence

gather sensitive data

Containerization

personal organizational data are segregated

Module Flow

1. Understand Various Mobile Device Connection Methods
2. Discuss Mobile Device Management Concepts
3. **Discuss Common Mobile Usage Policies in Enterprises**
4. Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
5. Discuss and Implement Enterprise-level Mobile Security Management Solutions
6. Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms



Mobile Use Approaches in Enterprise

Organizations follow **four** types of approaches to grant permissions to employees to use mobile devices for business purposes.

1

BYOD (Bring Your Own Device)

2

COPE (Company Owned, Personally Enabled)

3

COBO (Company Owned, Business Only)

4

CYOD (Choose Your Own Device)





- 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

BYOD Policy Implementation



1. Define the requirements
2. Decide how to manage the employee devices and their data access
3. Develop policies
4. Security
5. Support



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**

CYOD Policy Implementation



1. Define approved set of devices
2. Allow employees to select a device from the approved set of devices and build a technology portfolio
3. Develop policies
4. Security
5. Support

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 organization

COPE Benefits

1. **Greater control and authority to the organization**
2. **Retains ownership of the devices**
3. **Less expensive than BOYD**
4. **Prevents employee from carrying multiple devices (phones)**

COPE Policy Implementation

1

Purchase computing resources and devices

2

Allow employees to work with the company-owned device (including personal work) and build a technology portfolio

3

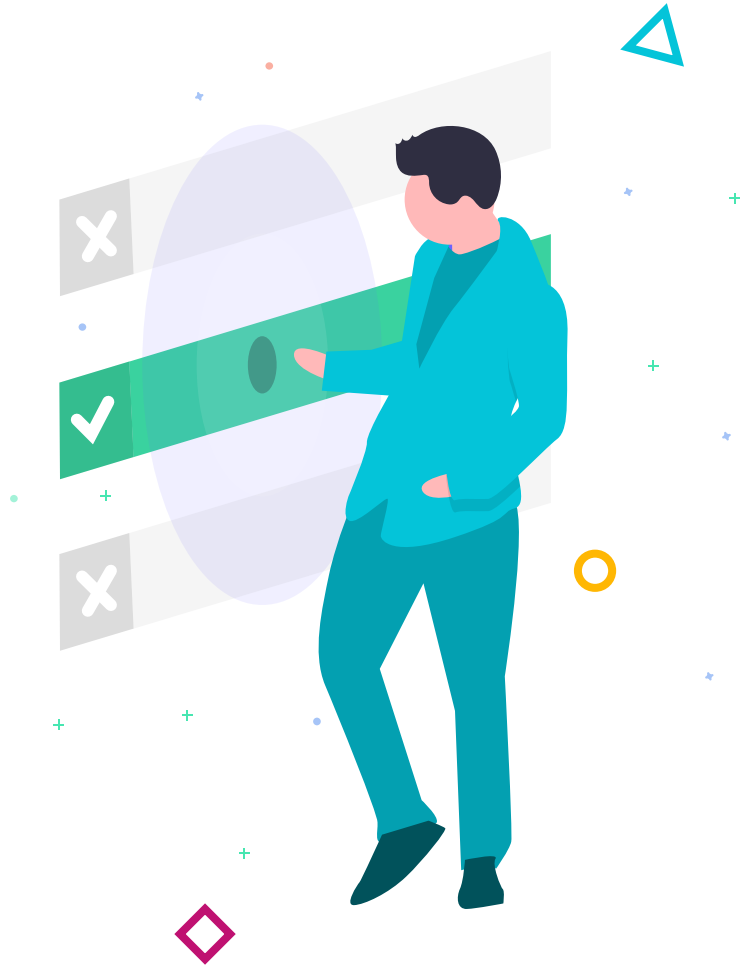
Develop policies

4

Security

5

Support



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** their usage for business purposes only



COBO Benefits

1. Prevents data leakage
2. Full control and authority to the organization

COBO Policy Implementation

Prohibit personal use of devices — 01

Allow employees to work with a device running a single application and build a technology portfolio — 02

Develop policies — 03

Security — 04

Support — 05



Module Flow

1. Understand Various Mobile Device Connection Methods
2. Discuss Mobile Device Management Concepts
3. Discuss Common Mobile Usage Policies in Enterprises



4. **Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies**
5. Discuss and Implement Enterprise-level Mobile Security Management Solutions
6. Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms

Enterprise Mobile Device Security Risks and Challenges

Security Risks

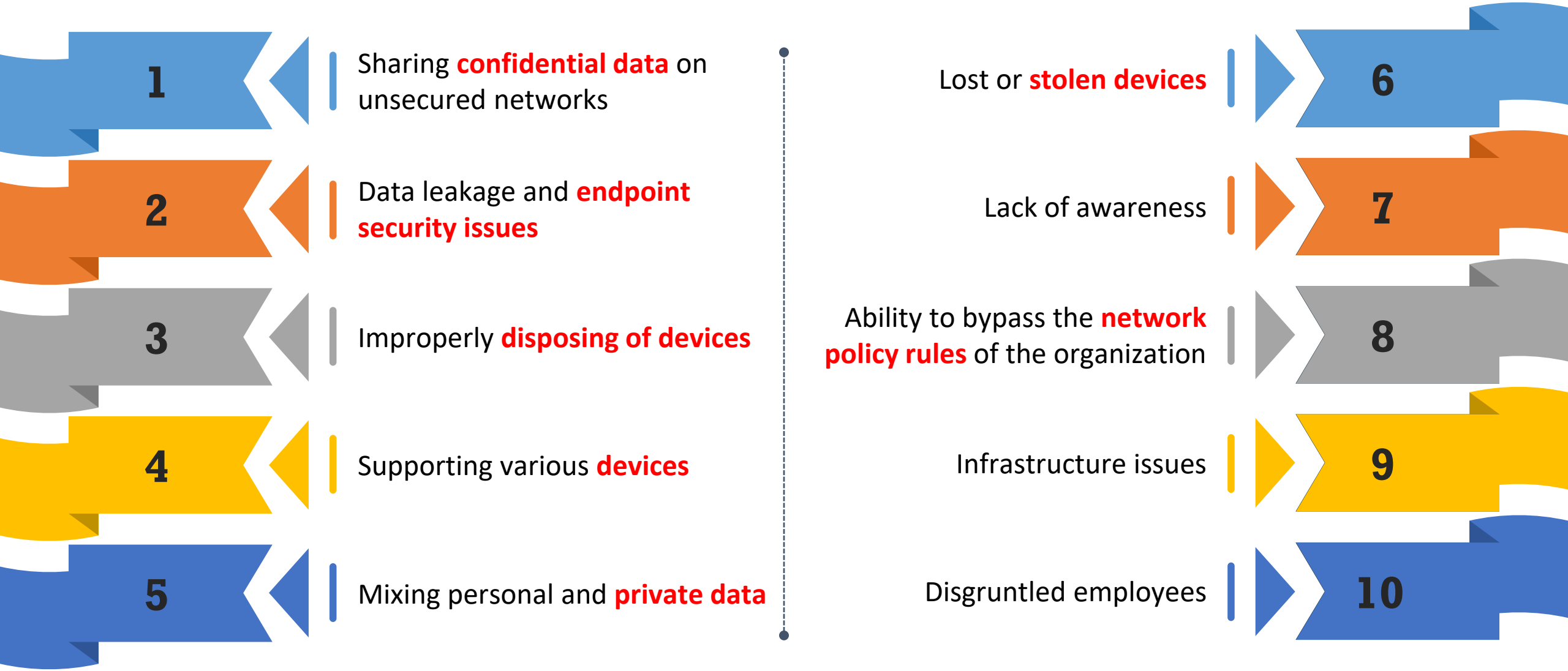
- ✓ The use of mobile devices in a work environment has changed the approach of organizational security. Mobile usage in enterprises has created a new set of security risks and challenges
- ✓ Hence, enterprise mobile device security encounters additional security challenges besides the **mobile device-level 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 allows mobile devices at the workplace

Security Challenges

- ✓ Mobile devices are **harder** to track and secure
- ✓ Mobile device 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



Risk Associated with BYOD, CYOD, COPE, and COBO



Security Guidelines for BYOD, CYOD, COPE, and COBO



For Security Professional

- 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



For Employee

- 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

Module Flow

1. Understand Various Mobile Device Connection Methods
2. Discuss Mobile Device Management Concepts
3. Discuss Common Mobile Usage Policies in Enterprises



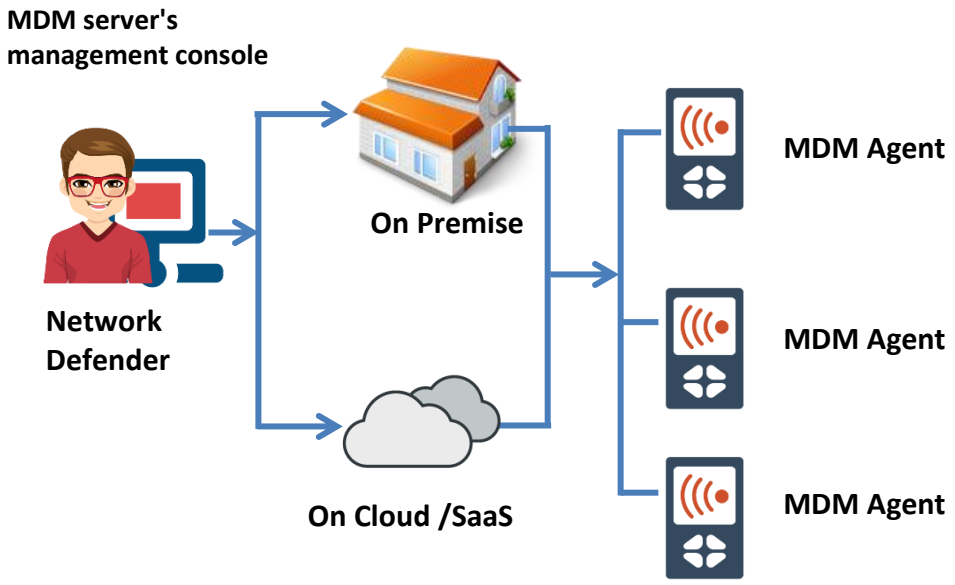
4. Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
5. **Discuss and Implement Enterprise-level Mobile Security Management Solutions**
6. Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms

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

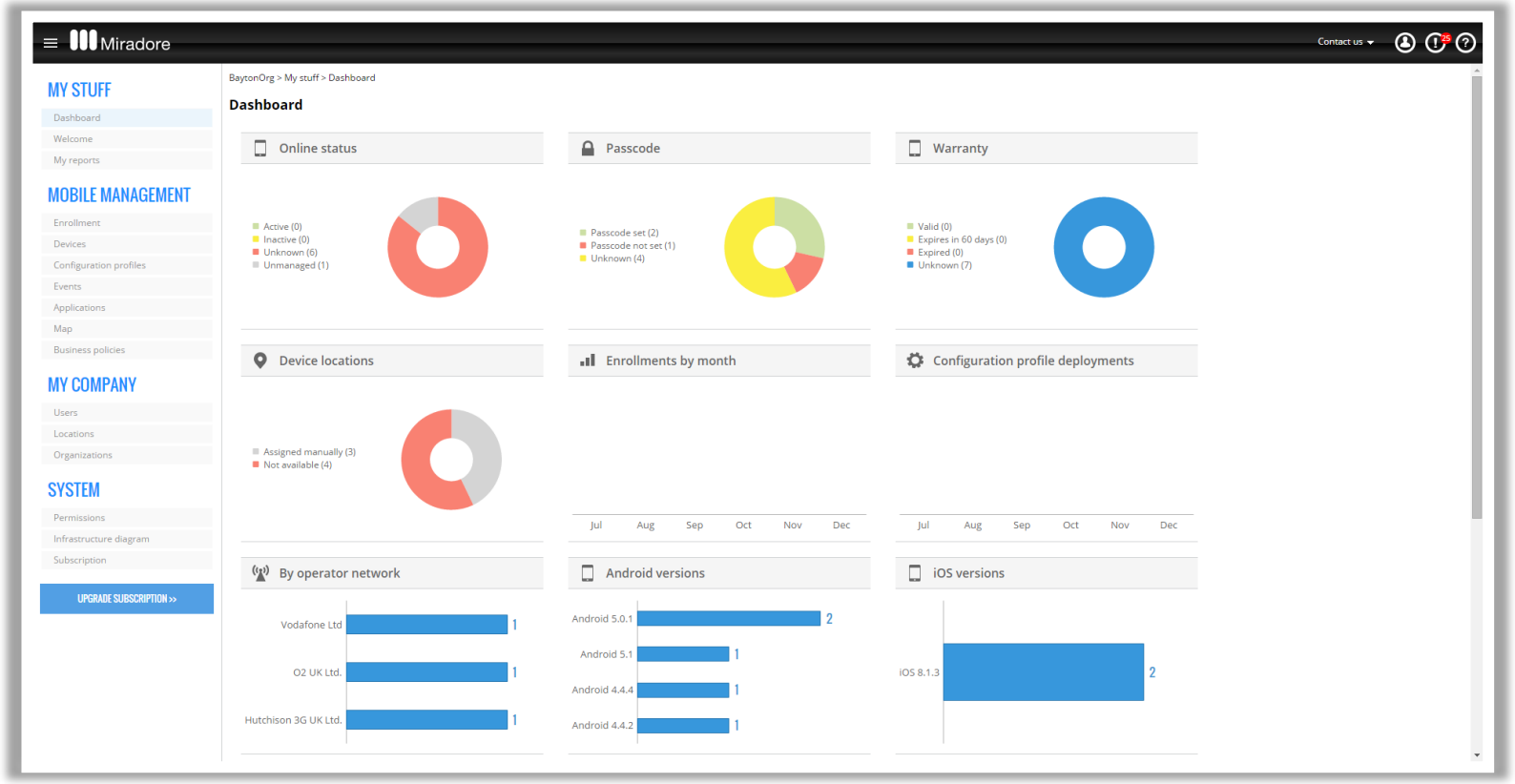
MDM Solution Deployment



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

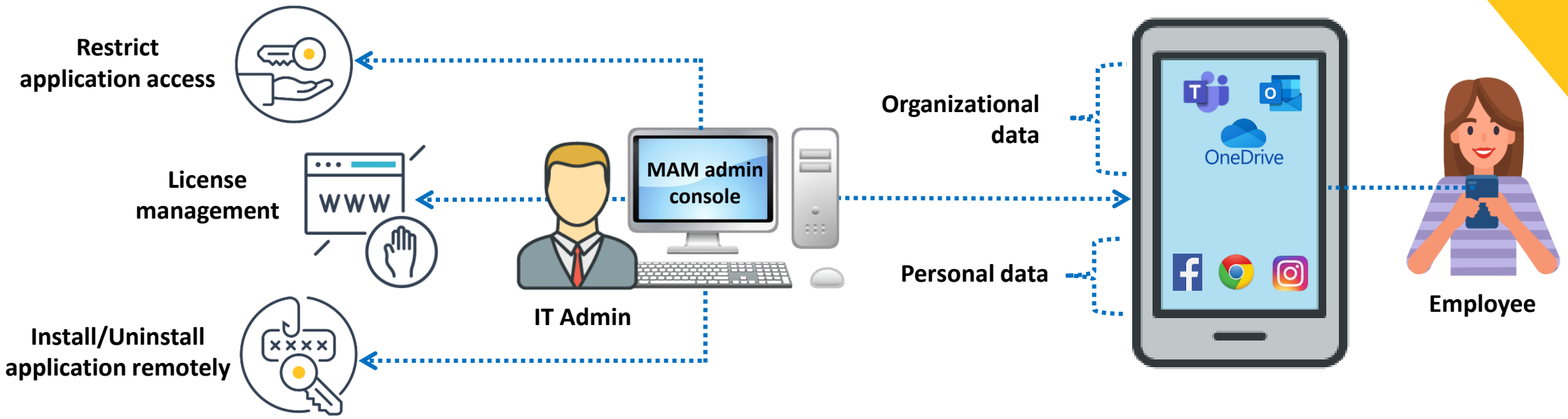
IBM MaaS360
https://www.ibm.com

XenMobile
https://www.citrix.com

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

Mobile Application Management Solutions

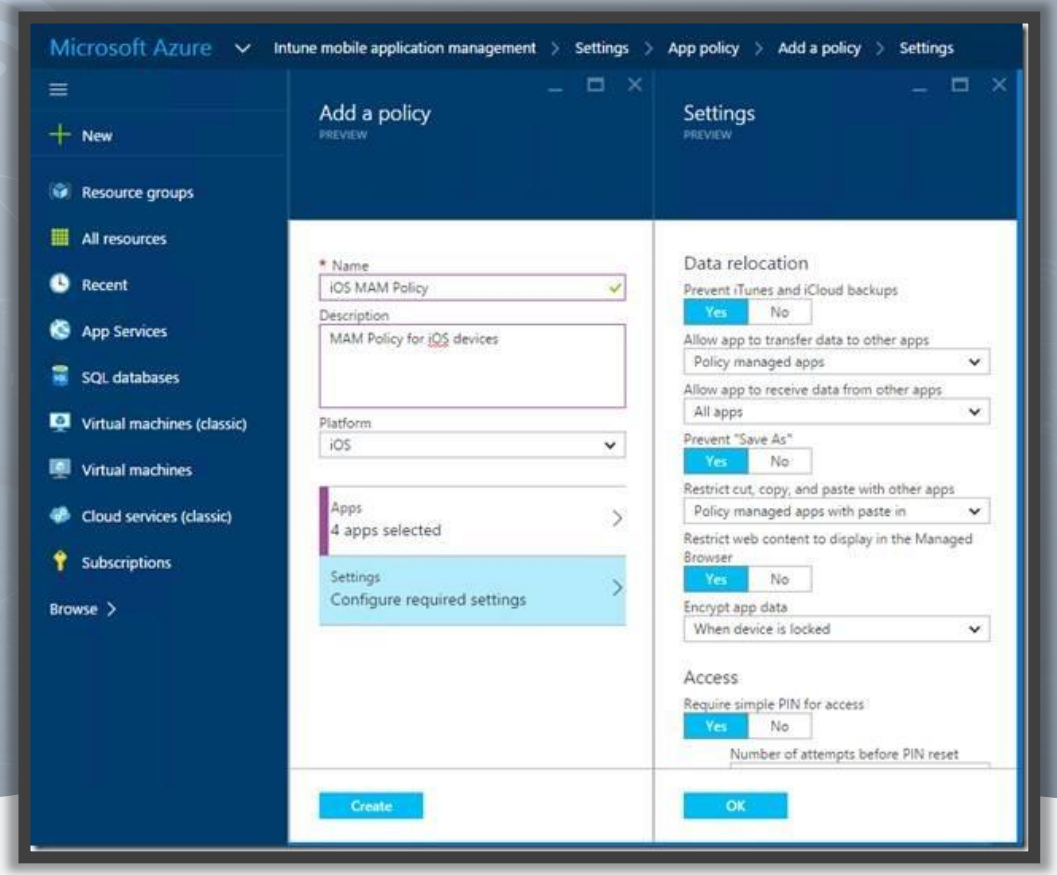
Mobile application management (MAM) is a software or service that enables network defenders to **secure**, **manage**, and **distribute** enterprise applications on employee mobile devices



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

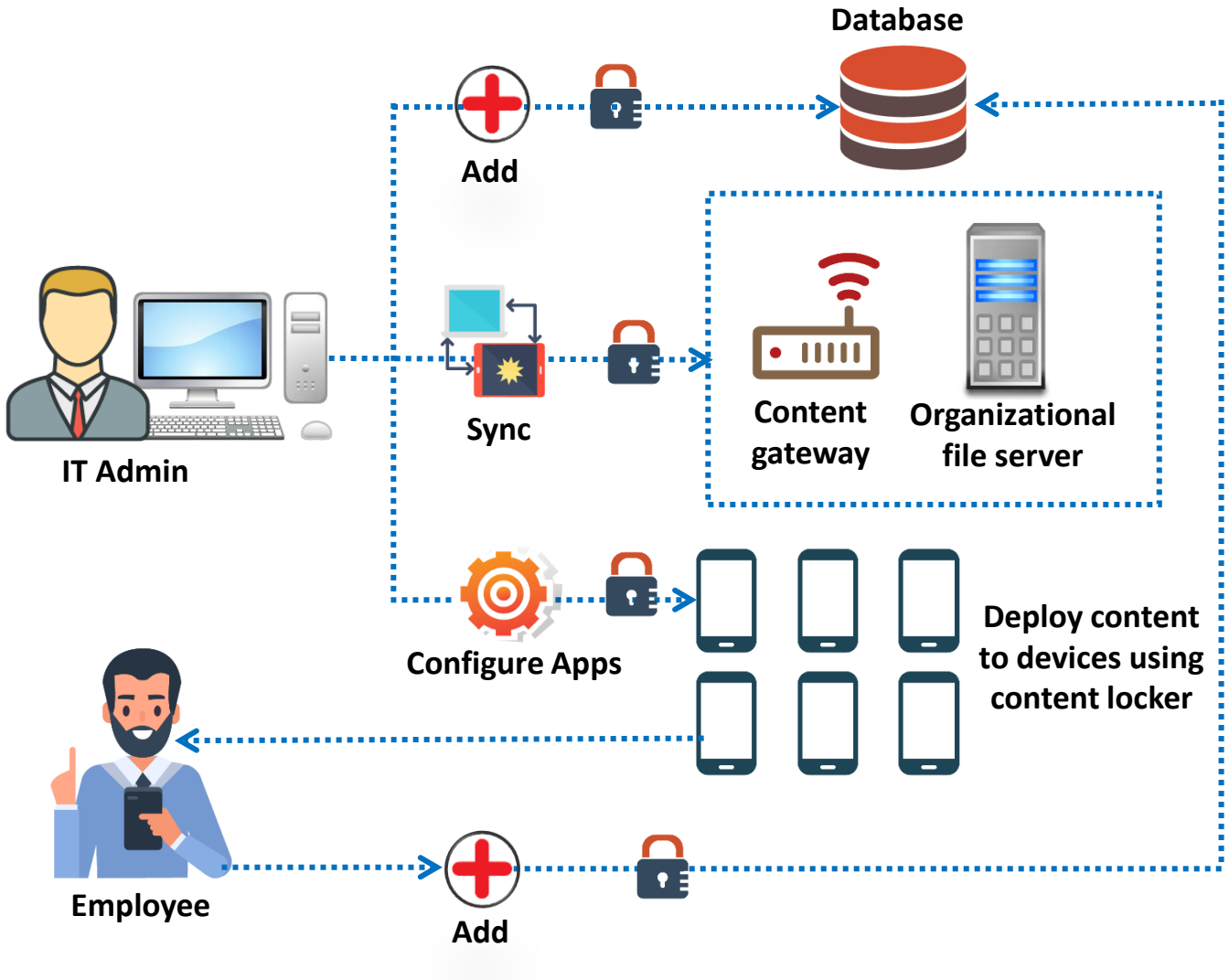
- ✓ **AppStation's MAM** *https://www.mobileiron.com*
- ✓ **Scalefusion Application Management** *https://scalefusion.com*
- ✓ **ManageEngine Mobile Device Manager Plus** *https://www.manageengine.com*
- ✓ **Apriorit Enterprise Mobile Device and Application Management** *https://www.apriorit.com*
- ✓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

Mobile Content Management Solutions

- Mobile content management (MCM) or mobile information management (MIM) solutions provide **secure access** to corporate data on smartphones, tablets, and other mobile devices
- It enables 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 Solutions

- **Vaultize**
  https://www.vaultize.com
- **MobileIron**
  https://www.mobileiron.com
- **AppTec360°**
  https://www.apptec360.com



Mobile Threat Defense Solutions

Mobile threat defense (MTD) aims to secure mobile devices against advanced **malicious threats**, **network attacks**, and **device vulnerabilities**

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)

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

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

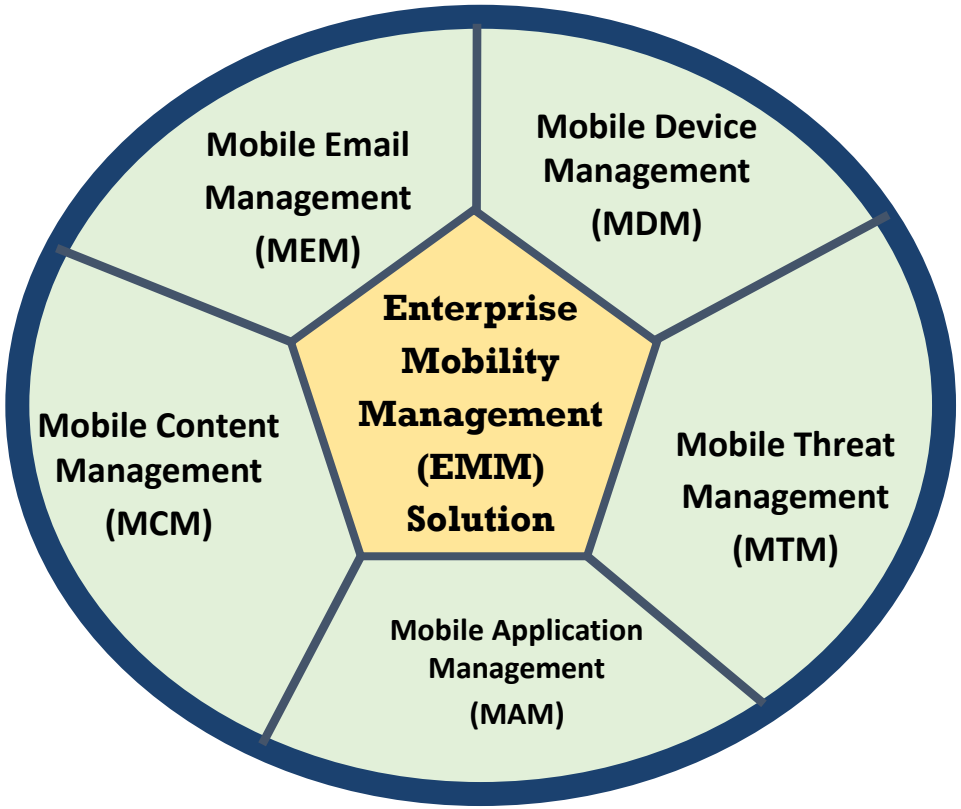
42Gears MEM
https://www.42gears.com

Hexnode Mobile Email Management
https://www.hexnode.com

Mimecast Mobile Email Management
https://www.mimecast.com

Enterprise Mobility Management Solutions

Enterprise mobility management (EMM) is a **comprehensive** solution for MDM, MAM, MTM, MCM, and MEM



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

Module Flow

1. Understand Various Mobile Device Connection Methods
2. Discuss Mobile Device Management Concepts
3. Discuss Common Mobile Usage Policies in Enterprises



4. Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
5. Discuss and Implement Enterprise-level Mobile Security Management Solutions
6. **Discuss and Implement General Security Guidelines and Best Practices on 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



Mobile Data Security Best Practices



01 Encrypt the data **stored** on the device

02 Enable **over-the-air** encryption using SSL, TLS, VPN, WPA2 etc.

03 **Backup** the mobile data periodically

04 Do not store **extremely sensitive** information on mobile devices

05 Do not store **passwords** or **PINs** as contacts on your phone

06 Use **private data centers** to store data and implement device authentication



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

General Guidelines for Mobile Platform Security

01 Do not install too many **applications** and avoid auto-uploading photos to **social networks**

02 Perform **security assessment** on the application **architecture**

03 Maintain **configuration** control and **management**

04 **Install** applications from trusted application **stores**



05 Securely **wipe or delete** the data when disposing of a device

06 Do not share any information within **GPS-enabled apps** unless required

07 Disable wireless access such as **Wi-Fi** and **Bluetooth** if not in use

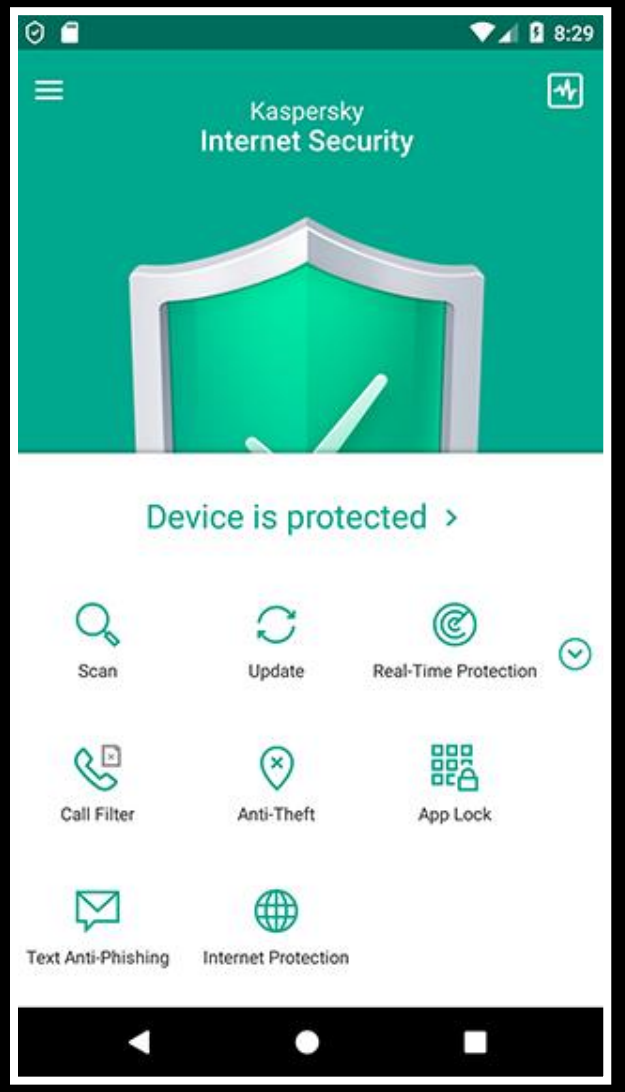
08 Never connect two separate networks such as **Wi-Fi** and **Bluetooth** simultaneously

Android Security Tools



Kaspersky Internet Security for Android

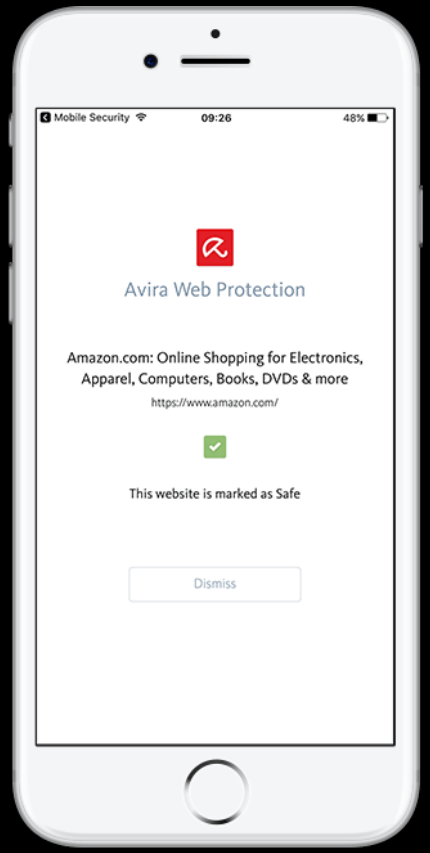
- blocks suspicious apps
- control access
- anti-theft tools

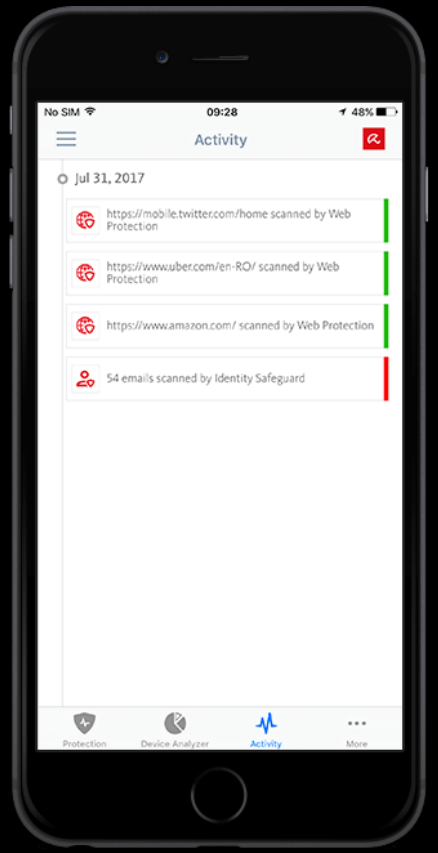


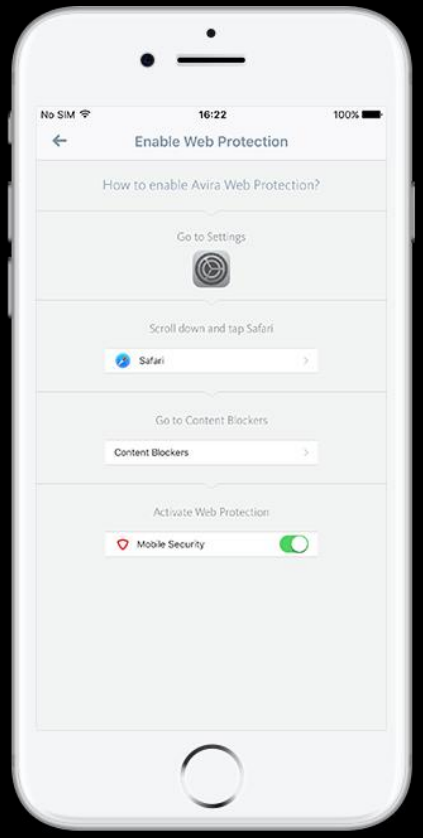
iOS Device Security Tools

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







Module Summary

- This module has discussed the various mobile device connection methods
- It has discussed the concepts of mobile device management
- It has also discussed the common mobile use approaches in enterprises
- It has discussed the security risk and guidelines associated with enterprise mobile usage policies
- This module also discussed enterprise-level mobile security management solutions
- Finally, this module ended with an overview of general security guidelines and best practices for mobile platforms
- In the next module, we will discuss on IoT device security in detail

