EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

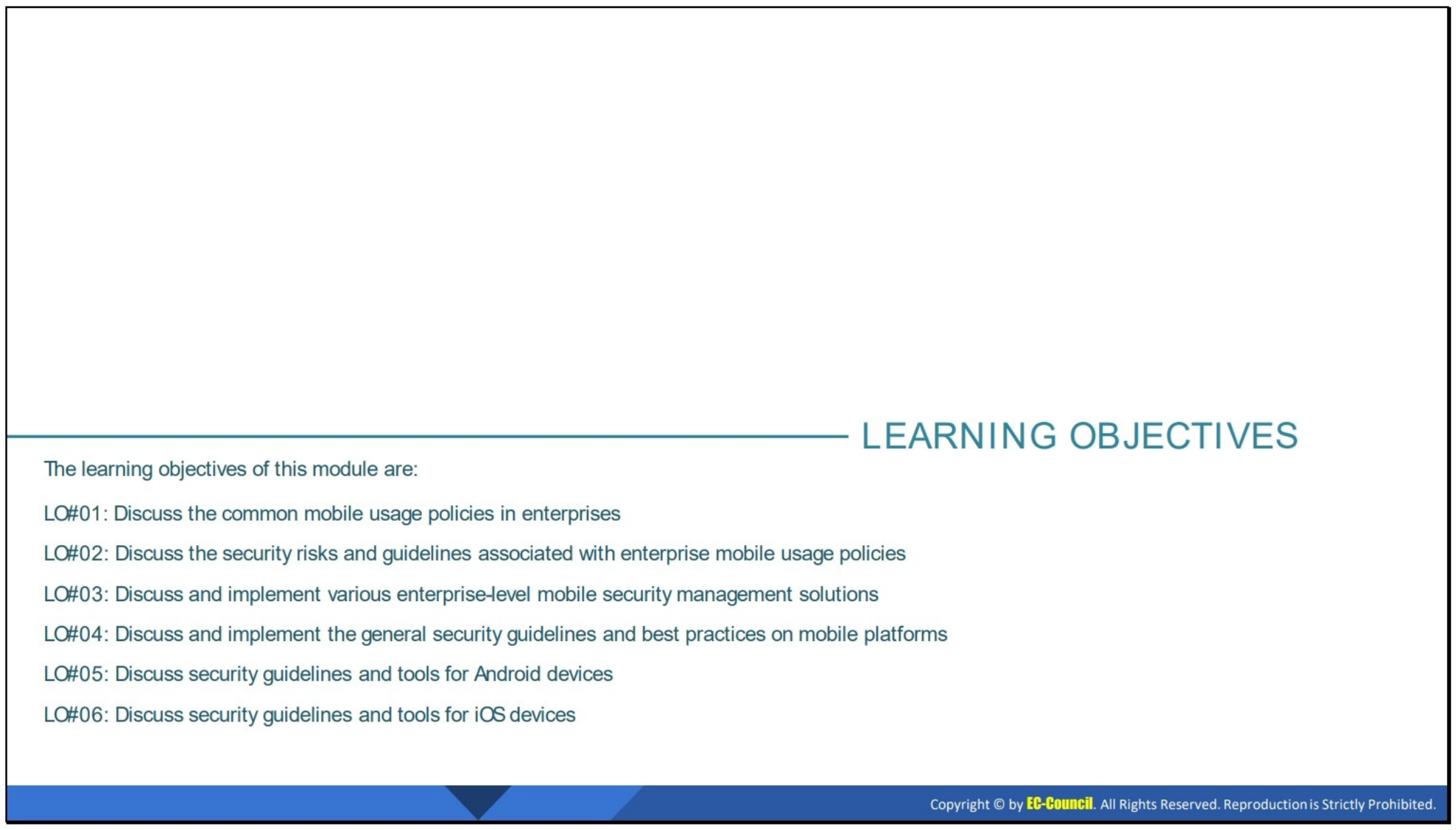
Certified Network Defender v3

MODULE 07

ENDPOINT SECURITY-MOBILE DEVICES

EC-Council Official Curricula

This page is intentionally left blank.

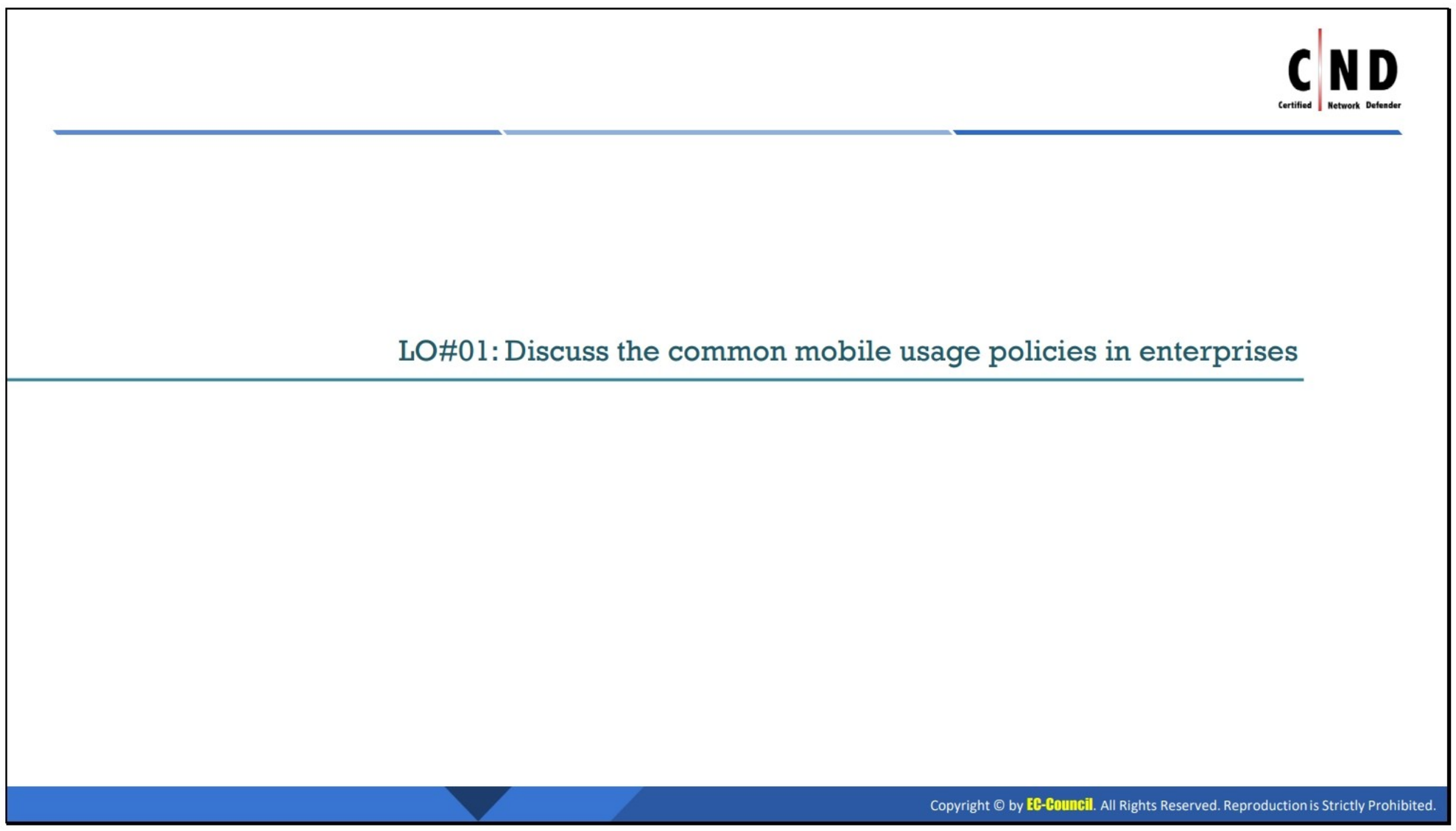


Learning Objectives

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.

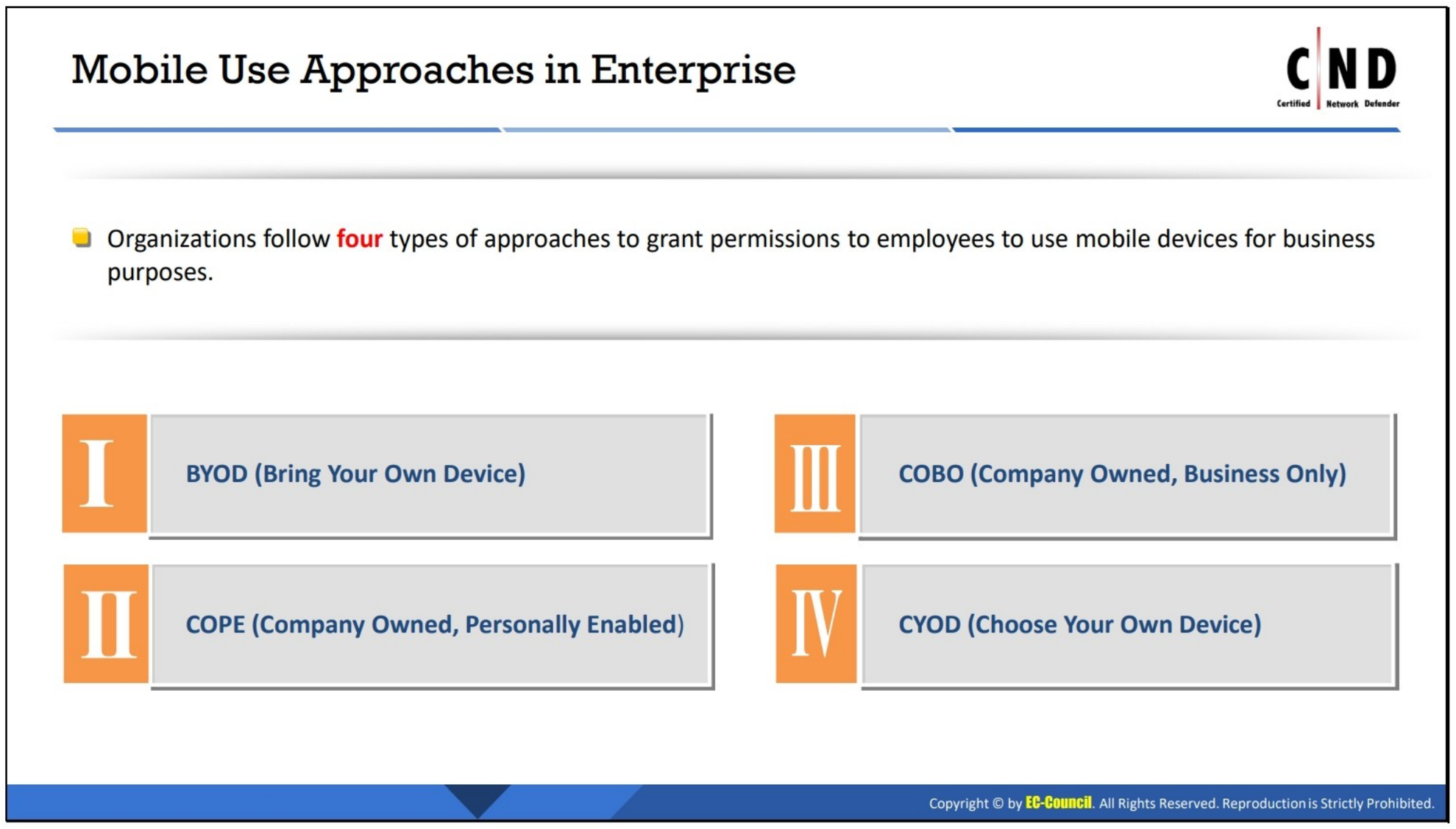
The objectives of this module include:

- Common mobile usage policies in enterprises
- Security risks and challenges associated with enterprise mobile usage policies
- Security guidelines to mitigate the risks associated with enterprise mobile usage policies
- Implementing various enterprise-level mobile security management solutions
- Implementing the general security guidelines and best practices on mobile platforms
- Security guidelines and tools for Android devices
- Security guidelines and tools for iOS devices



LO#01: 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.



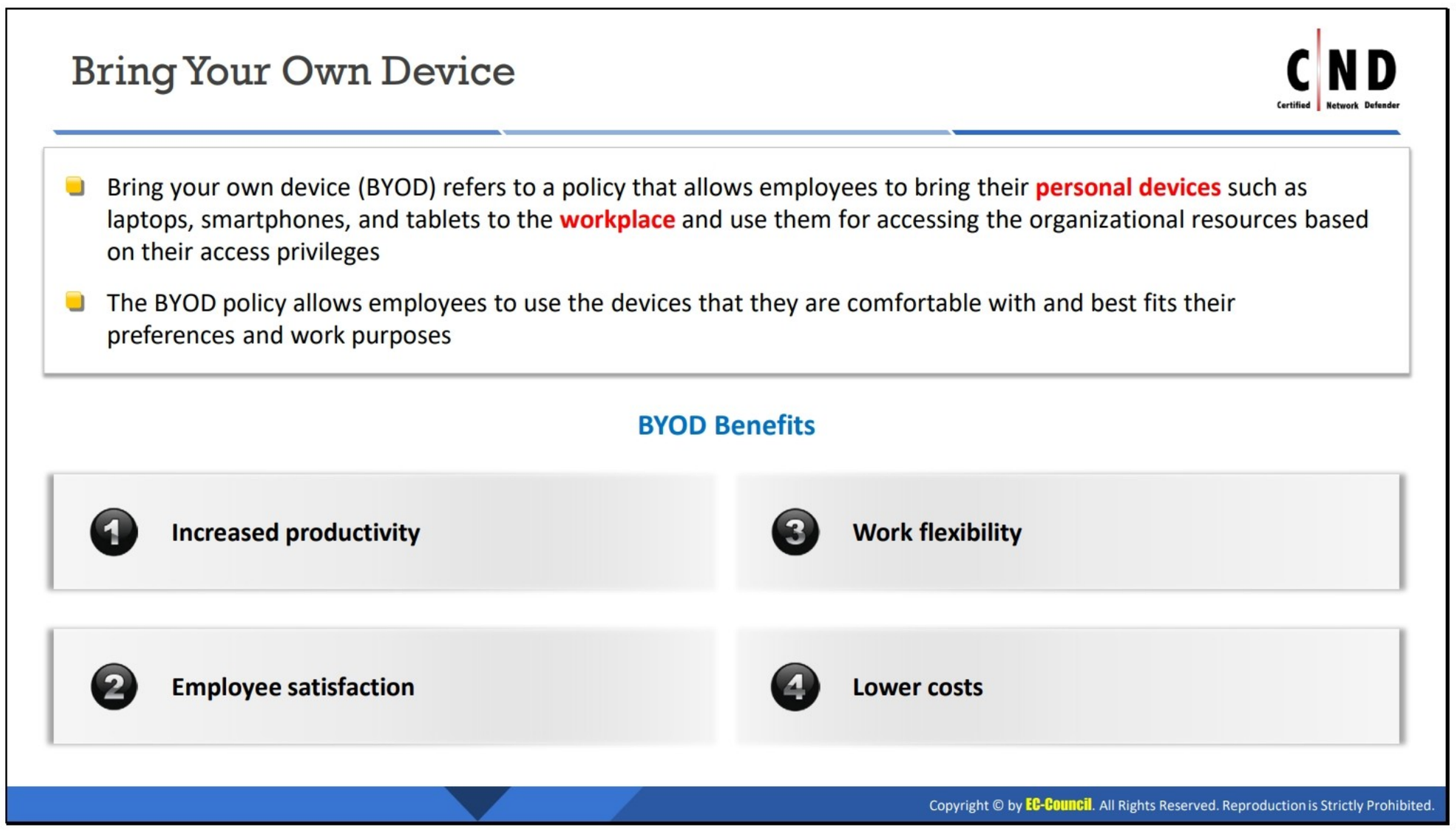
Mobile Use Approaches in Enterprise

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

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:**

  Employees become experts in using their devices; this increases the productivity of an organization. Additionally, these devices are regularly updated with cutting-edge technologies, which helps an organization to benefit from the latest features (both software and hardware) of the devices.

  By implementing BYOD, employees use devices of their own choice. Moreover, the implementation of this policy eliminates the usage of multiple devices for personal and corporate data because employees can store both in a single device. The employees need not work in the same office, sit in the same place, or use the same PC daily. They can work from home as well as while traveling. This motivates them, thereby increasing the organizational productivity.

- **Work Flexibility**

  Owing to the implementation of BYOD, employees can carry a single device to satisfy their personal and professional needs. The work usually done in the office can be done from anywhere in the world because the employees are provided with access to the corporate data. BYOD users have more freedom because their companies do not impose strict rules. It replaces the traditional client-server model with a mobile and cloud-centric strategy, which can have far-reaching benefits.

- **Lower IT Costs:**

  A business that employs BYOD does not spend on devices; instead, it saves money because the employees have their own devices. Additionally, the cost of data services is transferred to the employees who can take better care of their property (device).

- **Availability of Resources:**

  The devices often feature faster processors and advanced security features such as face recognition, fingerprint scanner, and iris scanner. The technologies used by employees in their devices are likely to be more up to date than those offered by organizations. This ensures that the employees have consistent access to the organizational resources.

BYOD Disadvantages

- **Maintaining Security Access in Organizational Networks**:

  Security can be practically non-existent because the businesses rely on their employees to use their own devices. If both the personal and corporate devices do not have the same security framework and if the company information is accessed via unsecured Wi-Fi networks, it could potentially expose the company network to the following security issues.

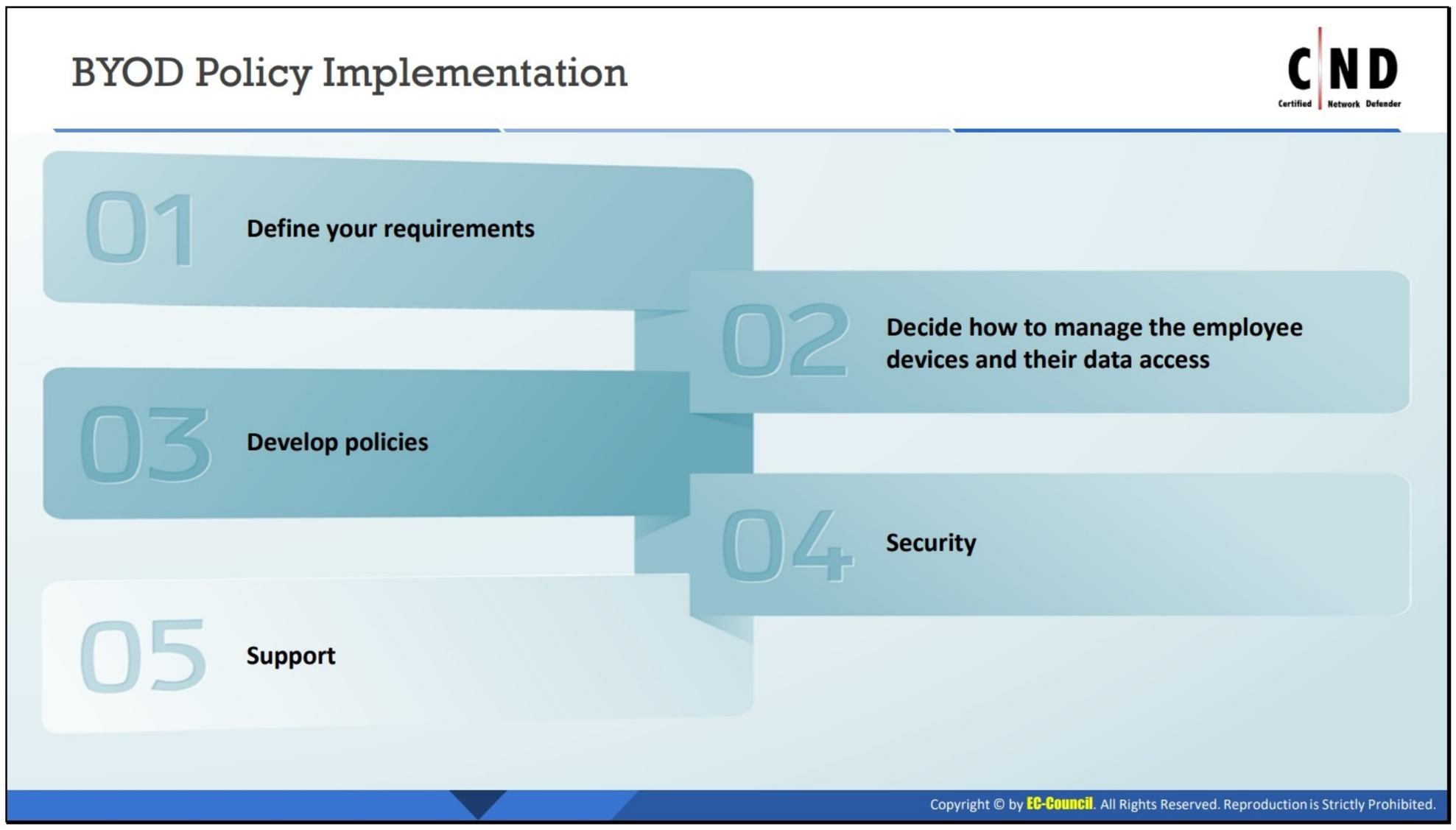
  - Lost, stolen, or unauthorized access to enterprise data
  - Malware attacks

- **Compatibility Issues**:

  Compatibility issues occur if the employees use various devices with different versions of different platforms (Windows, Apple, and Android). Companies may need to increase their IT staff for additional support. Moreover, it is difficult for companies to download software updates and secured patches for various devices speedily.

- **Scalability:**

  Many organizations do not have the suitable network infrastructure to maintain the incoming traffic from the multiple devices being used by employees.



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.

- **Defining organizational 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).

- **Deciding the management of 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 ensure that the corporate environment supports WLAN device connectivity and management.

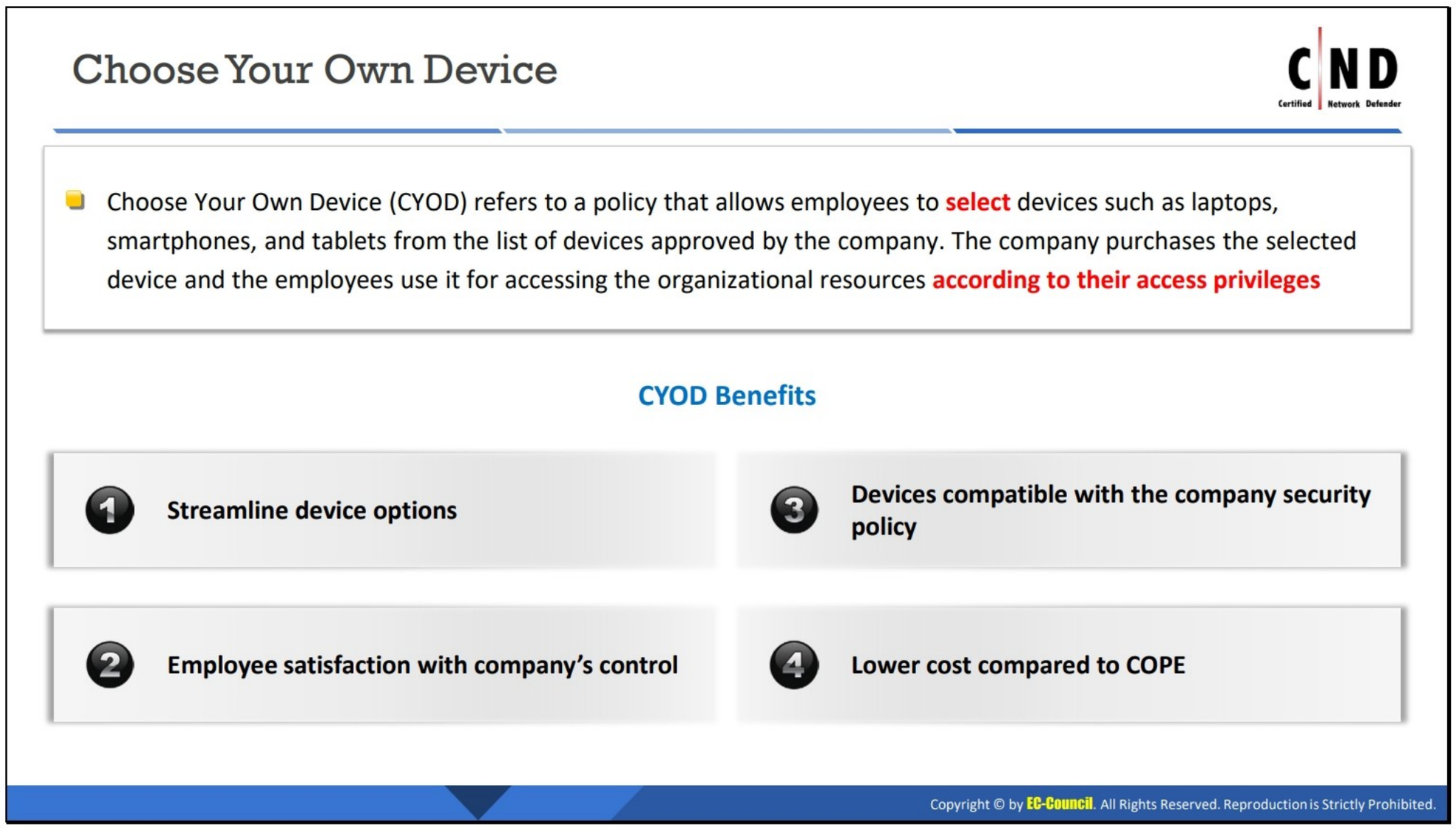
- **Develop policies:**
  - A delegation of company resources should develop the policies, instead of just IT. It should include key participants such as the HR, legal, security, and privacy. Following are the key components of a general BYOD policy:
    - Information security concerns
    - Data protection concerns
    - Confidentiality and ownership issues
    - Information regarding any tracking/monitoring
    - Considerations regarding the termination of employment
    - Guidelines regarding the assessment of the security of Wi-Fi networks
    - Acceptable and unacceptable behavior
  - 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. This will ensure managing the following risks
    - What will happen if there is a data breach?
    - Who will be liable?
    - What will happen if an employee leaves or is suspended?
    - Which applications are permitted to the staff?
  - 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

- The risks should be assessed and document in the following aspects:
  - Information security (for data, application, and user segment)
  - Operations security (for protecting user information)
  - Transmission security (for secured data transmission)
- It should be ensured that the organization covers all aspects (security, protecting resources, and controlling the expenses associated with BYOD) to protect the business and know which applications are permitted to be installed on devices that are not under the corporate network.
- Proper security procedures (encryption) should be implemented to protect the company data stored on the devices because the devices belong to employees. The passwords should be a combination of uppercase letters, lowercase letters, at least one number, and a symbol.
- Ensure that the network can be sufficiently locked down to stop malware attacks and the infrastructure possesses the capacity to run BYOD.
- Businesses should also have their own apps to manage that all apps downloaded on BYOD hardware.
- The data usage of employees should be monitored to track all activities (phone calls, texts, roaming) so that organizations can determine misuse or threats and prevent unnecessary bills for excessive bandwidth usage.

- **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

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.

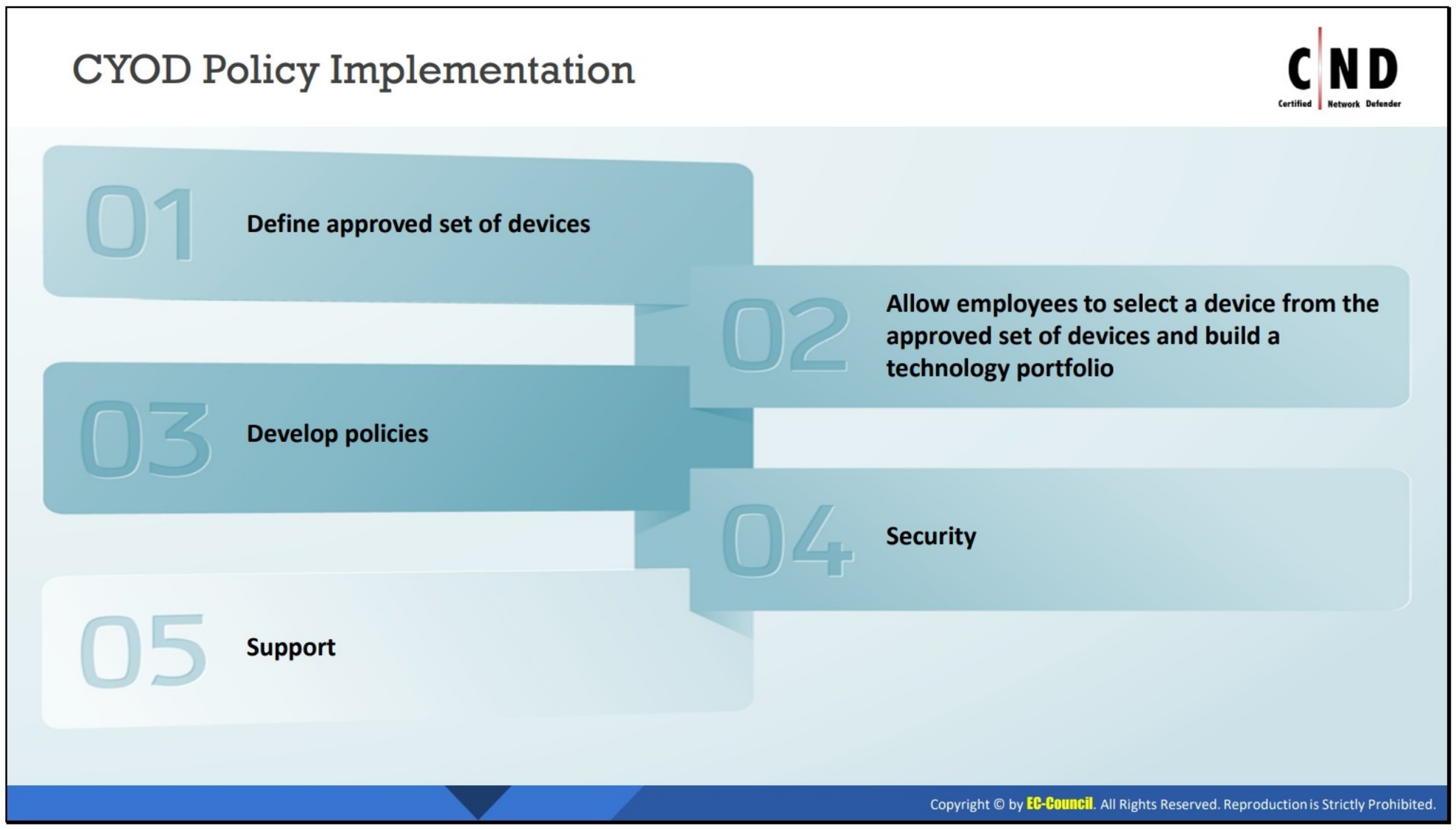
CYOD Advantages:

- 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 on organizations.
- It comprises a slower deployment timeframe.



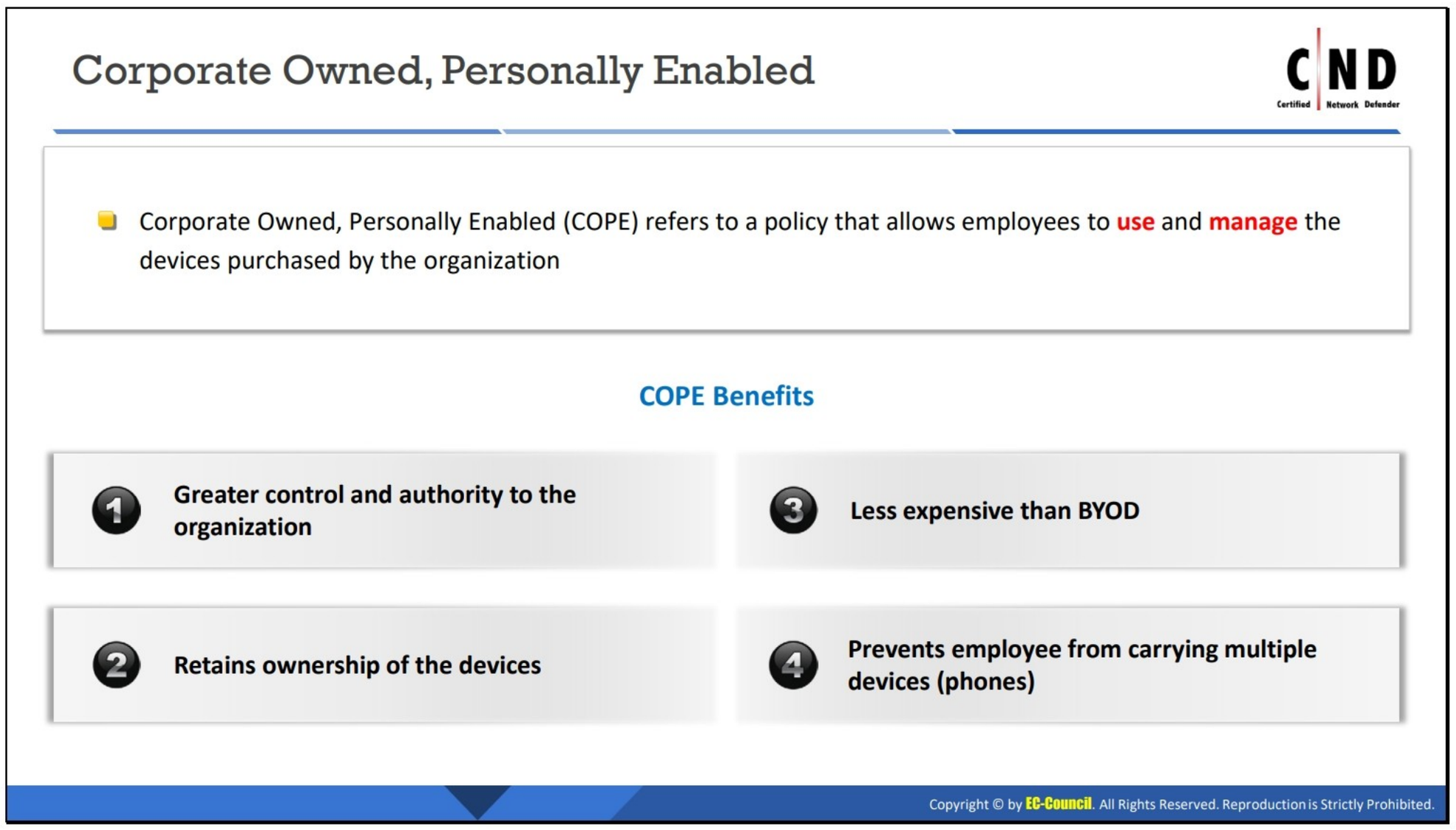
CYOD Policy Implementation

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

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.

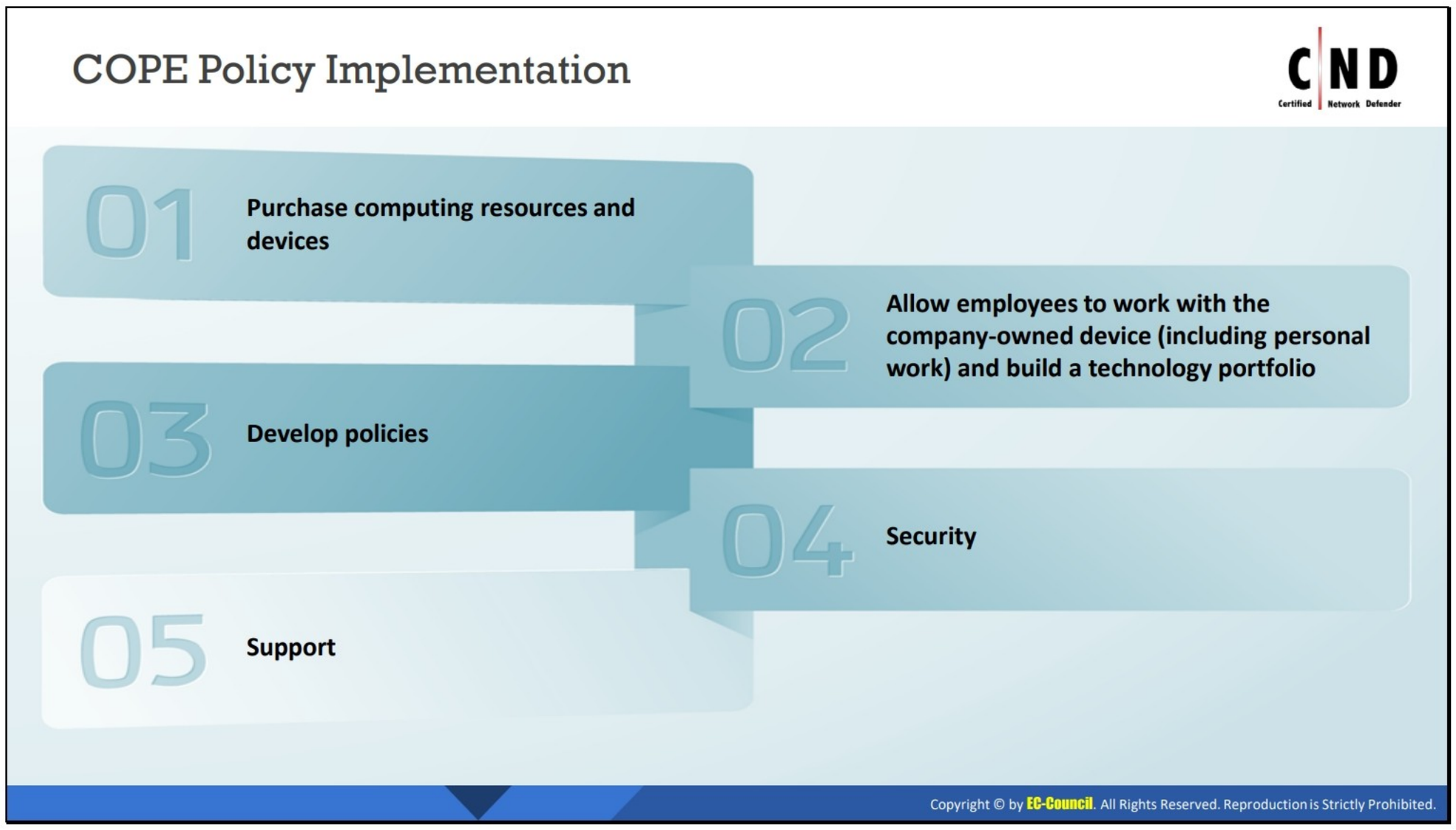
COPE Advantages:

- 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
- 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

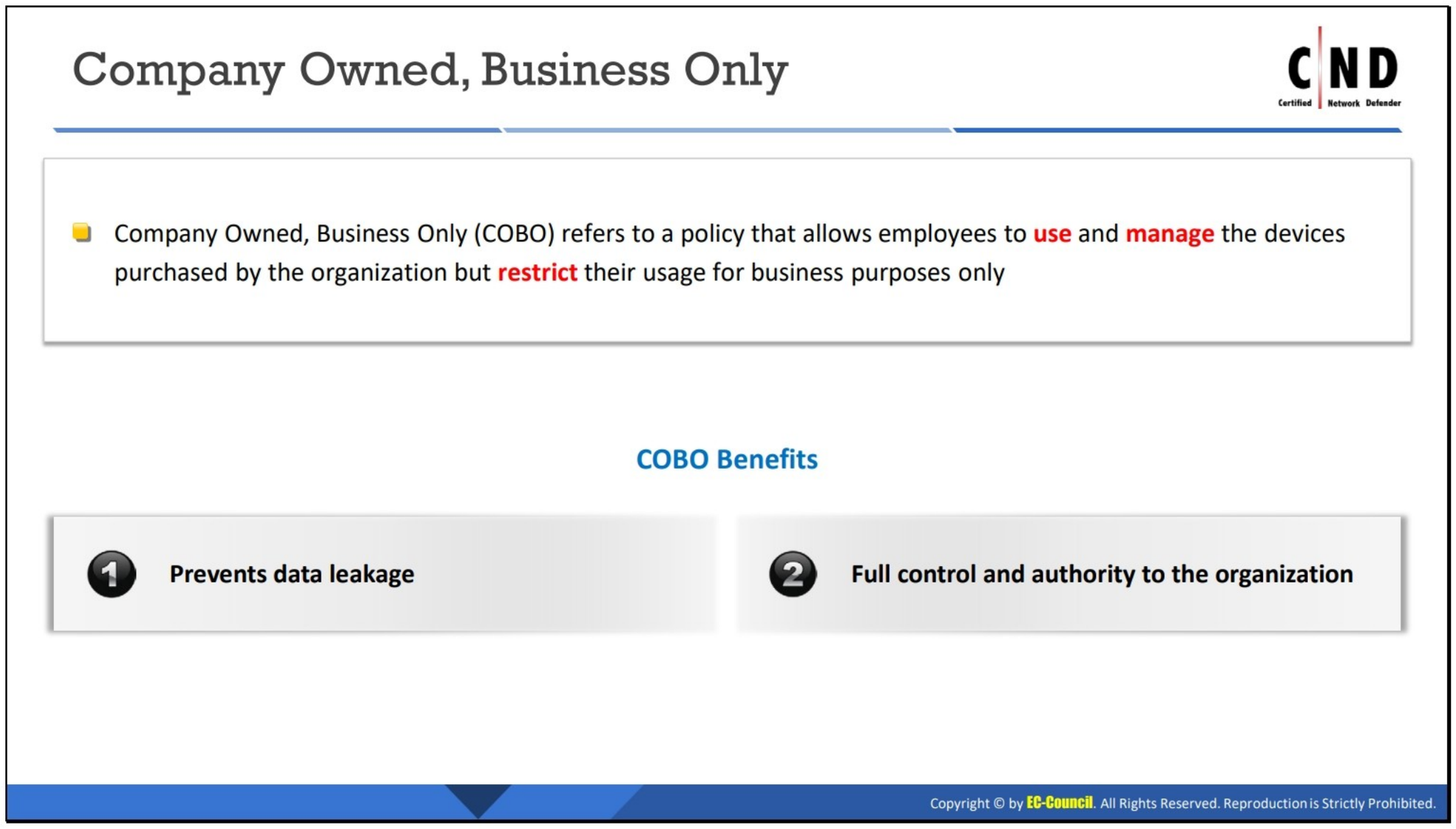


COPE Policy Implementation

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. Building a technology portfolio for the COPE approach includes
    - Containerization or the virtualization technology for separating the professional and personal use of a device.
    - Manage/prohibit data sharing between two containers.
    - Secure personally identifiable information with the organization data by controlling device network access.
    - Ensure the use of secured apps from trusted sources.
- **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

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,

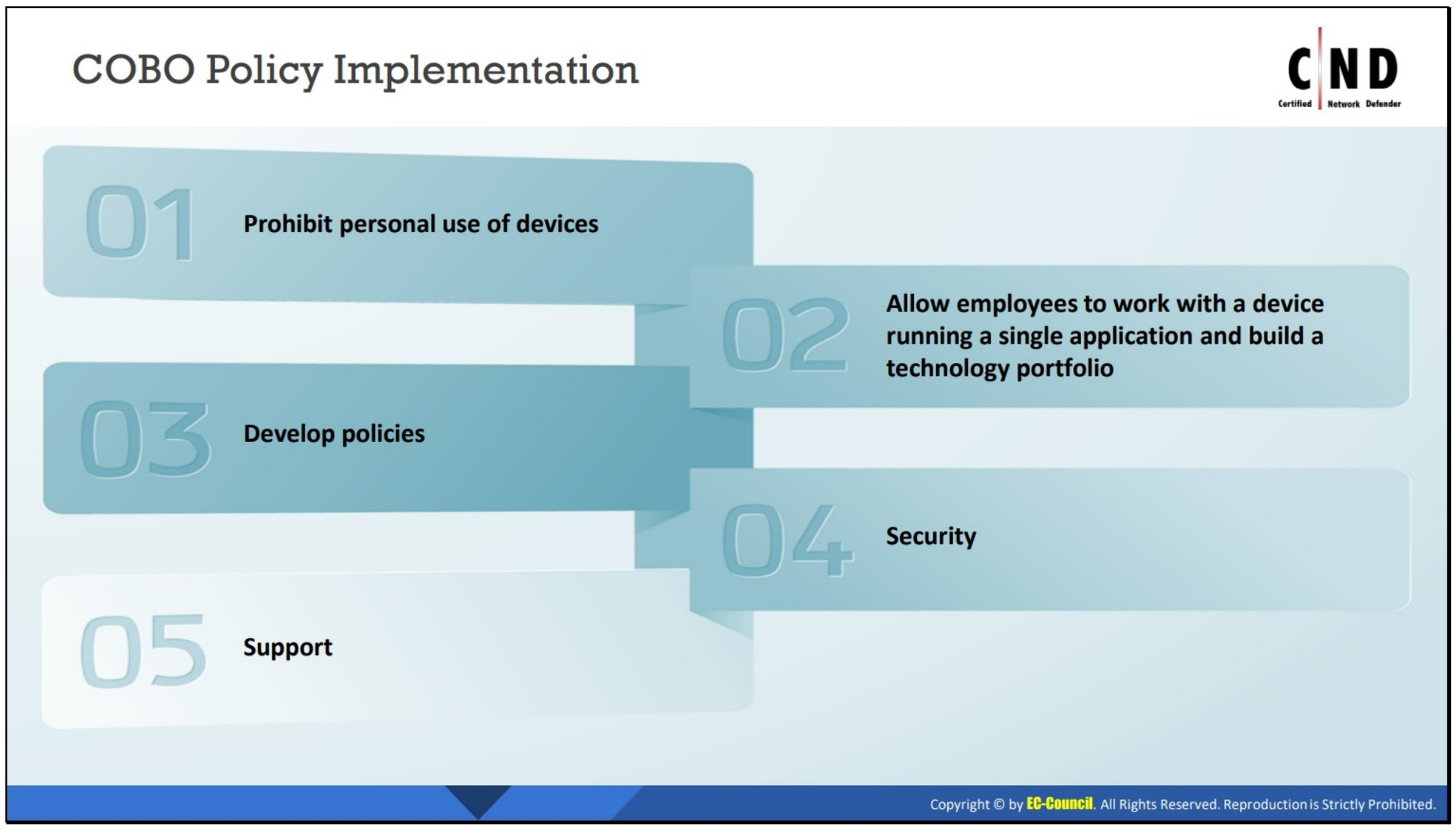
- An inventory system with an embedded barcode scanner.
- Blackberry is the best example of devices used in a COBO environment.

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.

COBO Disadvantages:

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



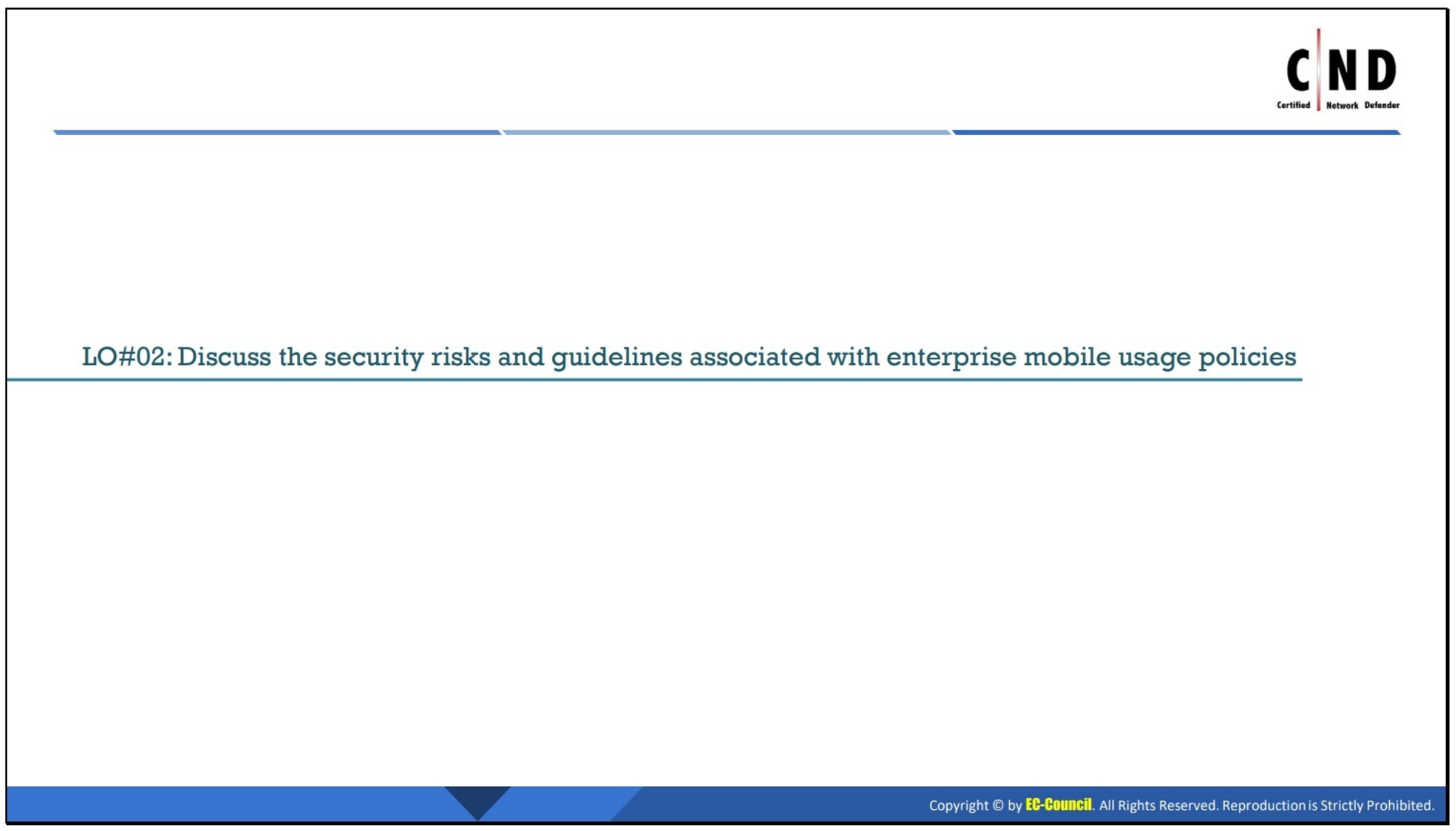
COBO Policy Implementation

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:**

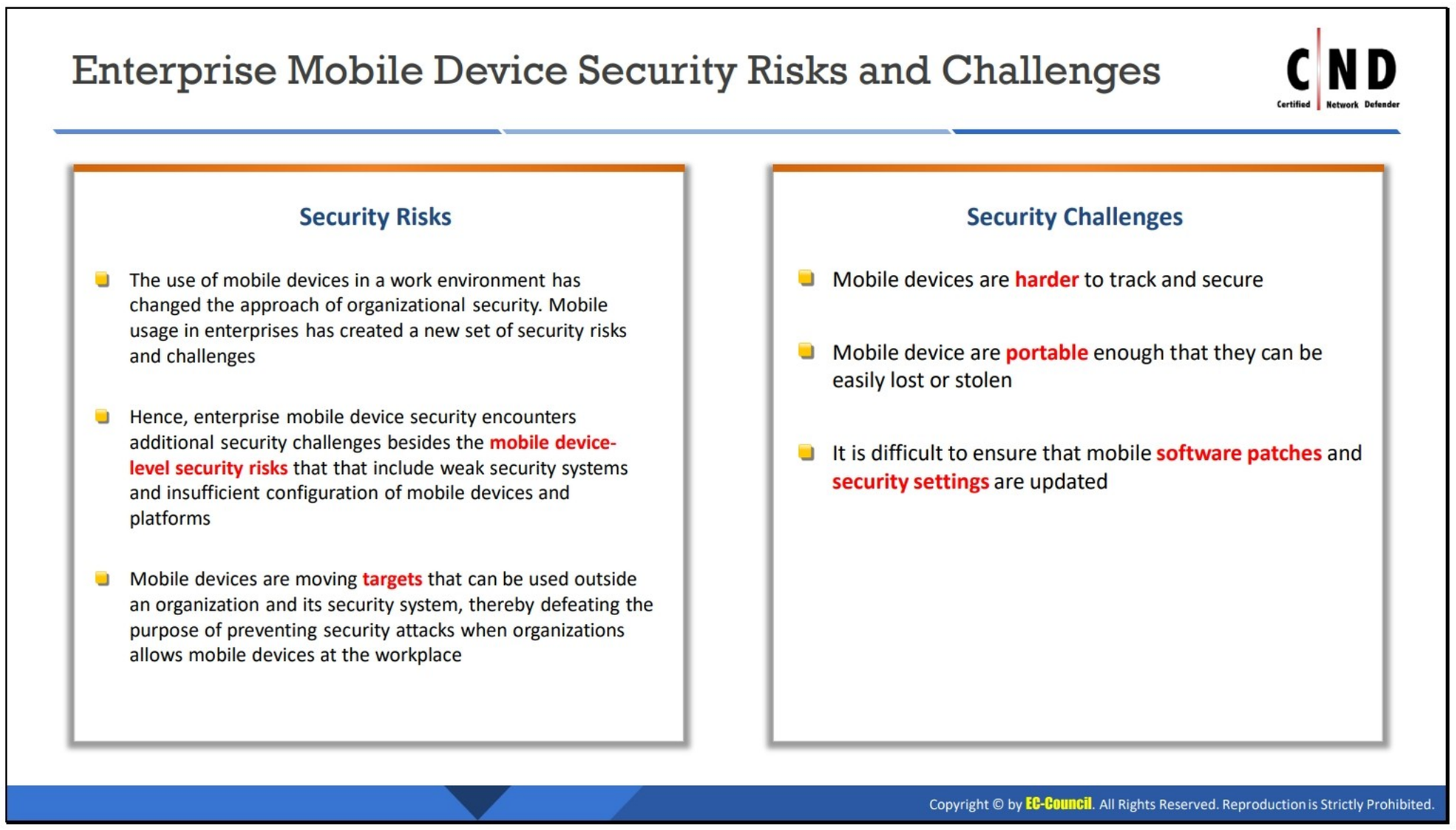
  Deploy expertise systems (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
  - Device troubleshooting

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



LO#02: Security Risks and Guidelines Associated with Enterprise 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

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. 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.

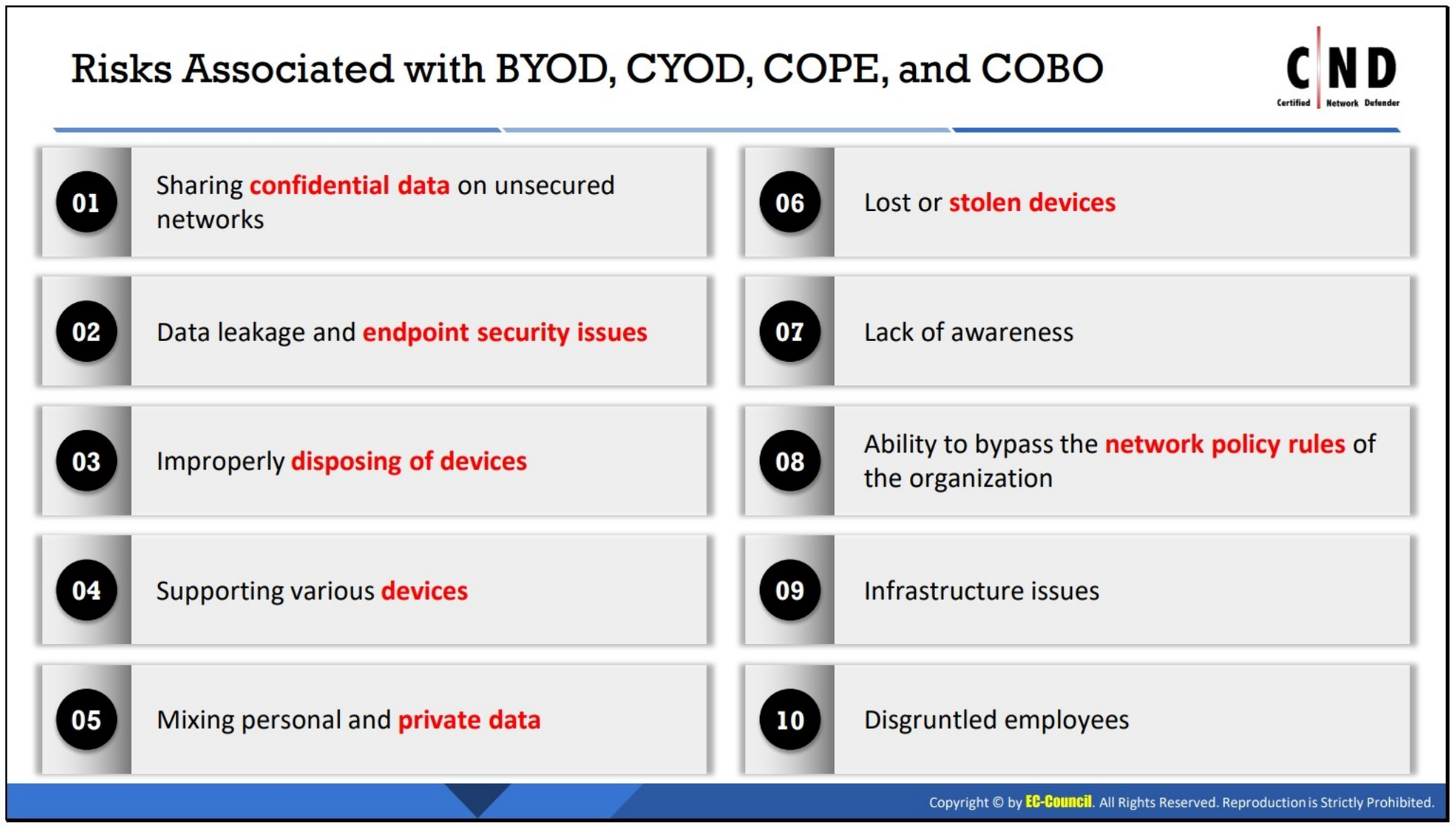
- **System-based Risks and Challenges**

  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.

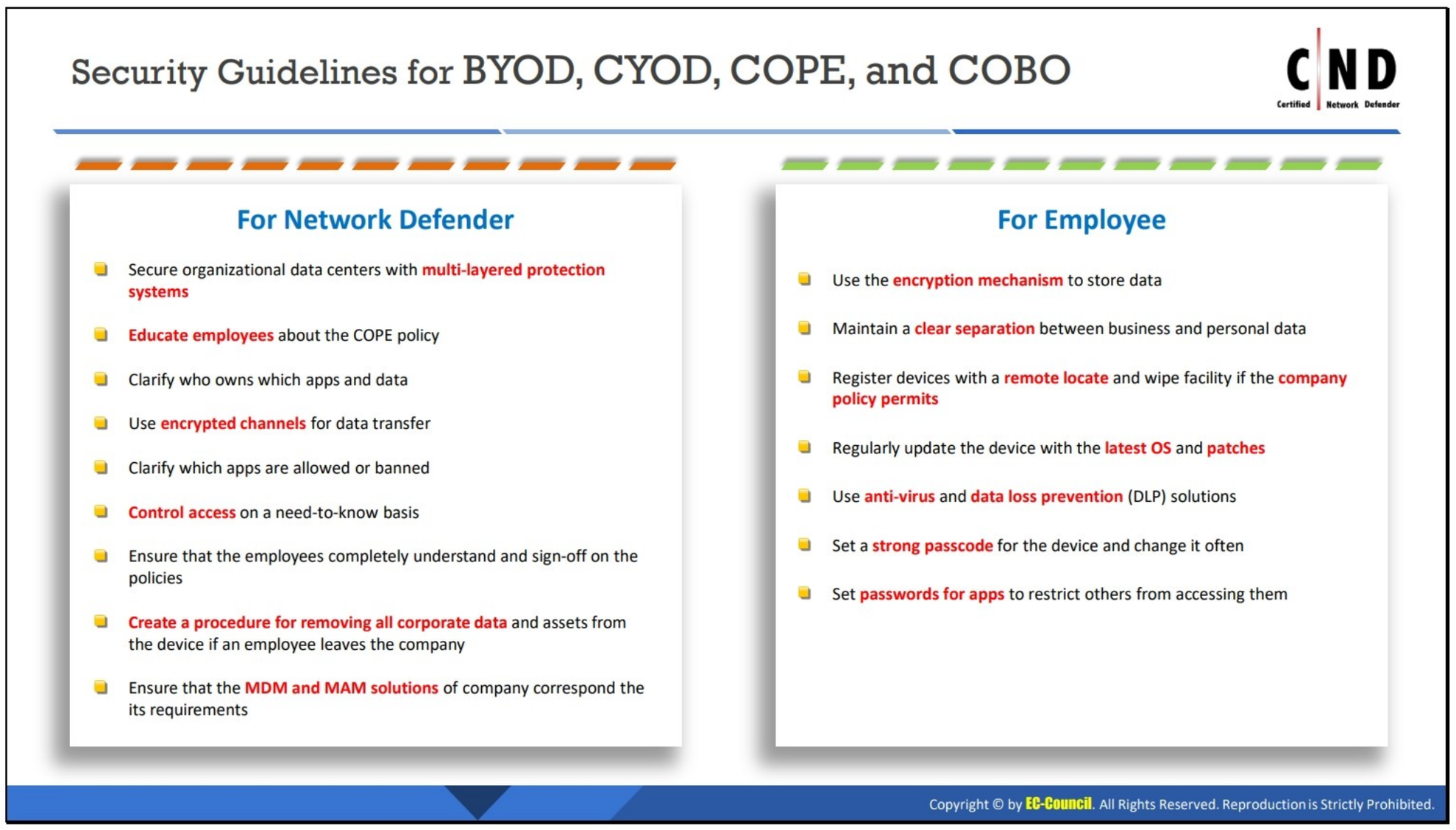


Risks Associated with BYOD, CYOD, COPE, and COBO

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

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 Administrator**

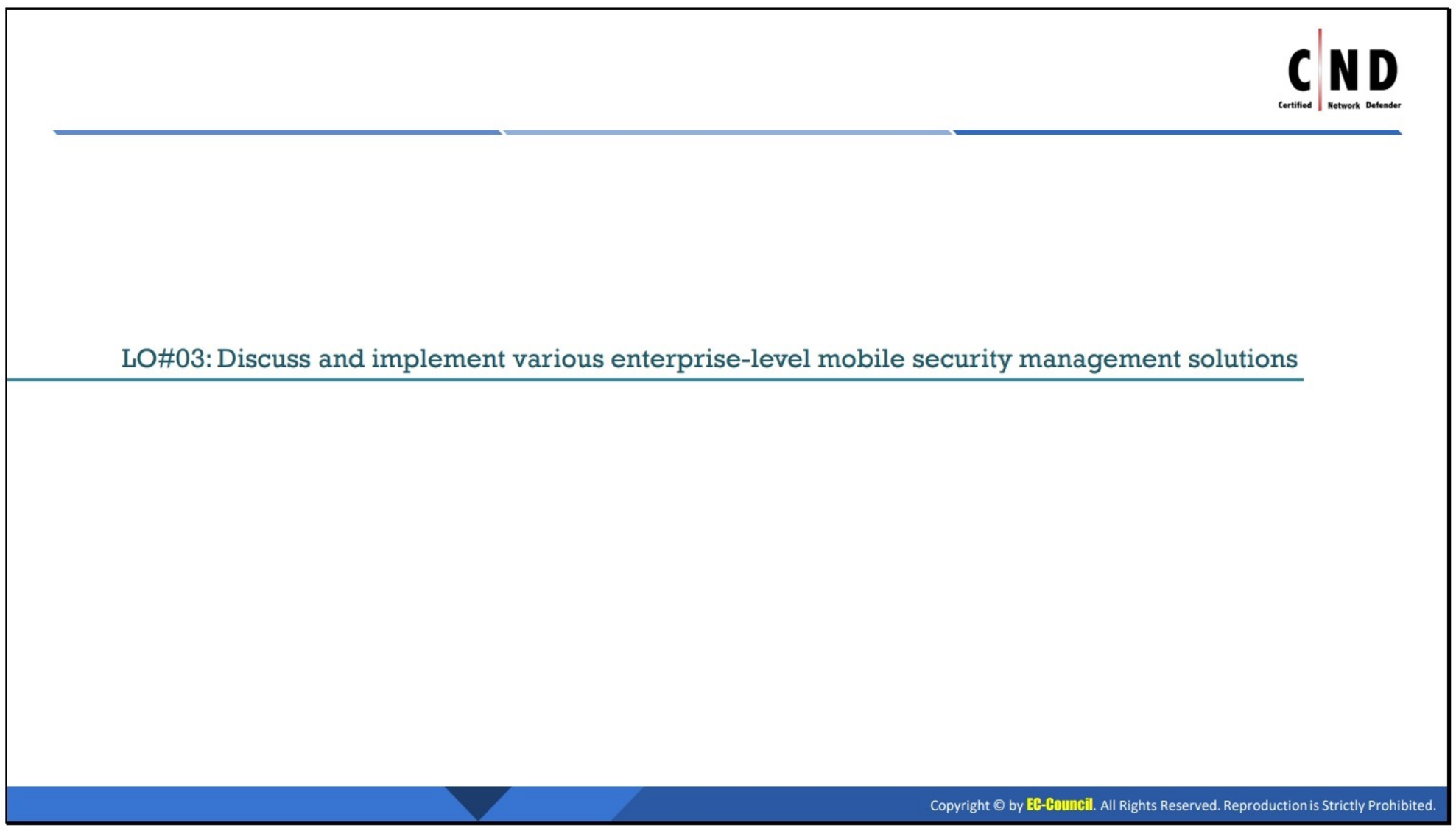
  With the increased use of tablets, smartphones, and other devices at work, mobile security has become a great concern. Listed below are the security guidelines that should be implemented to ensure the security of the network and data of an organization.

  - 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.

- **For Employees**

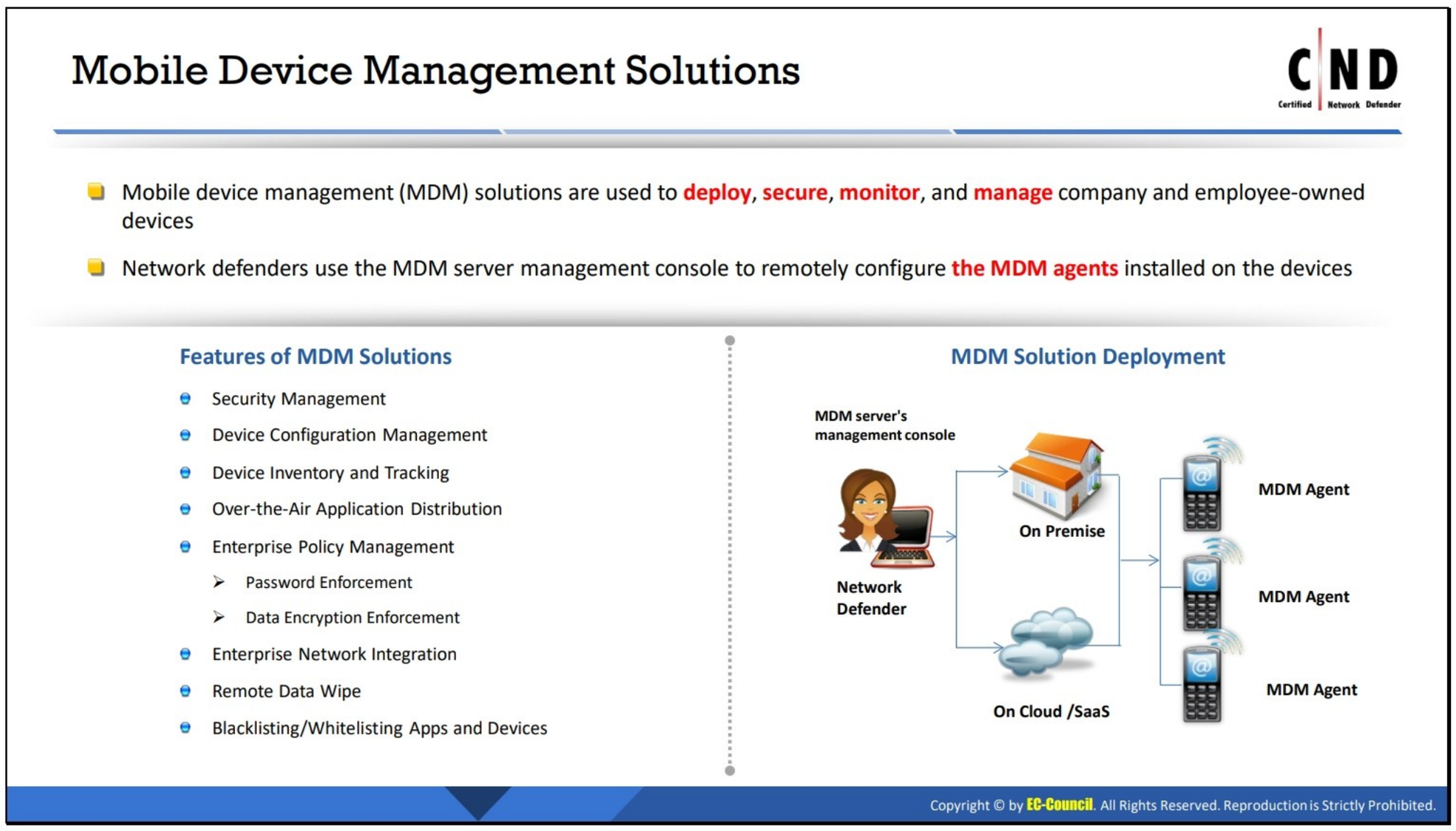
  - Impose company WLAN access when on-site.
  - Ensure the use of complex passcodes and change them frequently.

- 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.



LO#03: Implementing Various 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 mobiles 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) 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.

Delivery Methods for Deploying Best MDM

Based on the expertise and investment for deploying MDM, an organization can select any of the following MDM delivery methods.

- **Premise-based** MDM solutions are apt for
  - Organizations that want to maintain a high degree of control
  - Organizations that have reliable IT skills and resources
  - Organizations that want to control the system security and administration directly
  - Organizations that can bear a larger up-front investment
- **Software as a Service (SaaS)**-based MDM solutions are suitable for organizations that do not want to maintain servers at their site but still want management and admission. Organizations can negate or mitigate the up-front cost or pay monthly/annual fees for the system.
- **Managed services**-based MDM solutions are suitable for
  - Organizations that lack expertise or are over extended

- Organizations to turn the management function over to experts who handle it

This method features support without draining the internal resources and providing regular status reports, allowing organizations to be informed of the roll-outs, software/hardware updates, and asset/inventory control.

MDM Deployment

The key components of MDM include

- Preparing **a well-defined policy** to provide management direction and support for IT and information security.
- Implementing **a periodic assessment of risks** (**risk management).** Additional controls may be required to reduce the level of high risks. Moreover, minimal controls are sufficient for low or non-existent risks.
- **Managing configuration settings** that involve the automatic configuration of device settings such as password policy, email, Wi-Fi, and VPN. This phase can prevent user errors, reduce misconfiguration-related vulnerabilities, and reduce configuration lockdown according to the role-based permissions of users to implement IT mobility policies.
- Testing mobile applications separately to ensure their trustworthiness before distributing (**software distribution)** them over-the-air via MDM. Additionally, software distribution with configuration management allows whitelisting/blacklisting applications on mobile devices.
  - Define terms and conditions for **procurement issues** in policy and employee agreements after discussing with the HR and legal teams. Define liability for all parties in the agreement related to the private usage of corporate services.
  - Expense compensations
  - Employee privacy policy
  - Shared responsibilities for device and content security, and misuse
  - Secure wipe of the device, including personal data in case of device loss/theft.
- **Device policy compliance and enforcement** that include device supply, control, and tracking. It is important to perform asset-based inventory assessment to comply with
  - Corporate/regulatory mandates around policies
  - Jail-broken/rooted device detection
  - Encryption
  - Privacy-based separation of corporate content vs. personal content
- Implementing **enterprise activation/de-activation** to connect mobile devices to the organizational network minimizes the administrative burden of provisioning (for example, enabling encryption) and re-provisioning.

- **Asset disposition by de-commission,** which includes device exchange, upgrade, or permanent de-commissioning.

  The following procedures should be followed for asset disposition:

  - Notify inventory management
  - Generate user receipt
  - Accept user acknowledgment

  The following procedures should be followed for asset de-commissioning:

  - Secure wipe of corporate data
  - Handing over the device to employees without interfering with their personal data

- **Logging user activity** according to the laws, rules, and regulations of the country from where the organization conducts its activities.
- **Security settings** include:
  - **User security** that involves encryption, authentication, lock code, and selective wipe if remote wipe is issued.
  - **Data security** comprises wiping the corporate/private data if a device is lost/stolen.

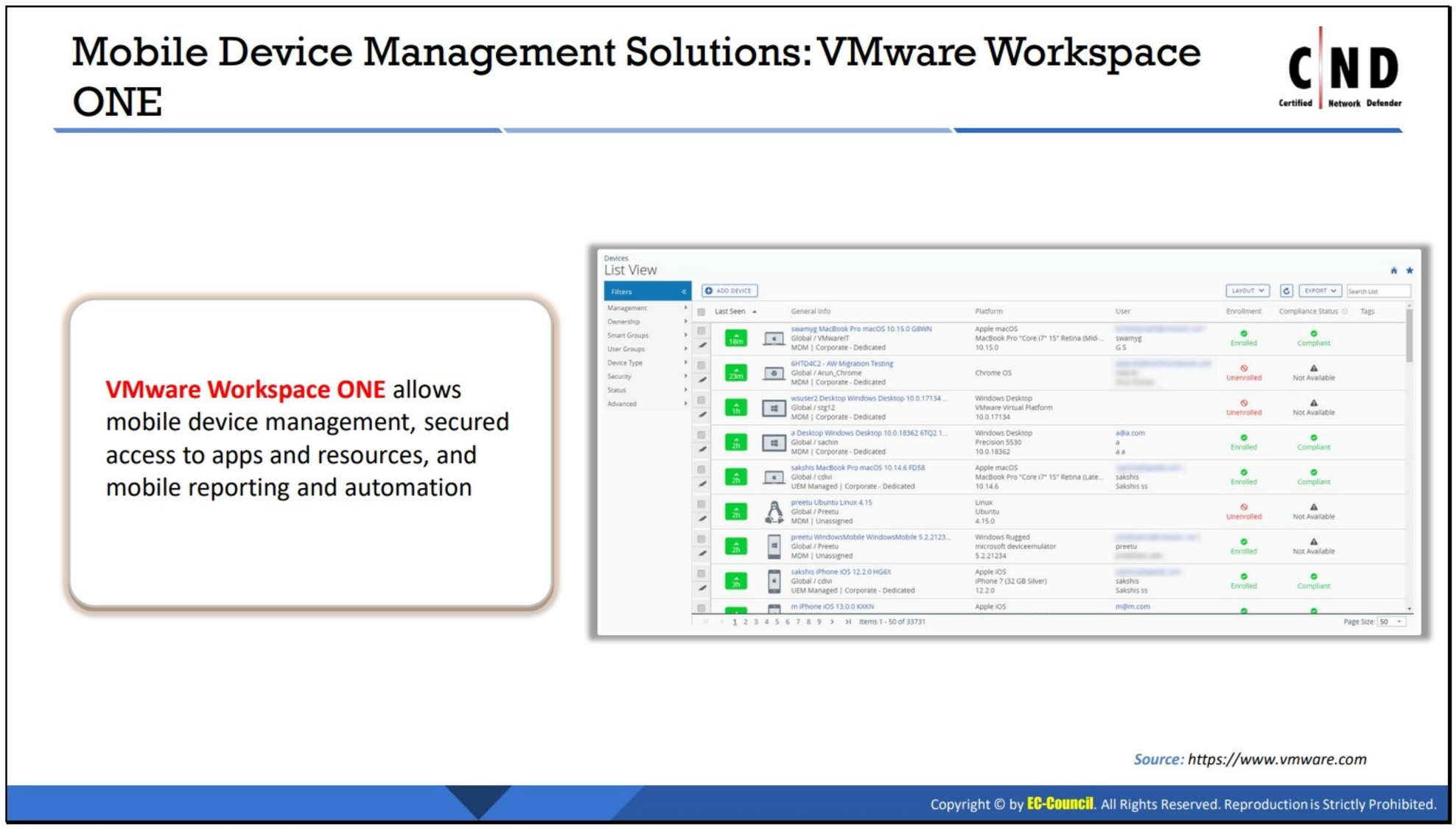
Challenges in MDM Implementation:

- An MDM solution may become cost-prohibitive if a BYOD policy is defined improperly/enforced ineffectively.
- An MDM may report false positives or a large number of false negatives if the device policies are improperly defined and implemented, resulting in reduced employee morale and creating confusion in the workplace.
- Unawareness about information security while using mobile devices may cause employees to freely share their devices with others, which may result in data breach.
- In the case of unwanted or intentional damage, identity theft, or fraud done by close associates, employees may have to suffer the consequences such as job dismissal.
- In the case of social engineering attacks, an unaware employee may share the organization data with others.

Factors to Consider Before Selecting an MDM Solution:

- **Deployment:** Analyze how effectively an MDM solution can be deployed.
- **Custom app store**: Know whether there is a feature for installing custom/unapproved apps and setting up a company app store experience.
- **Application security**: Know whether the MDM vendor offers built-in support for malicious application scanning.
- **Browser security:** Check whether the MDM solution provides filtered mobile web browsing.

- **Encryption levels:** Check whether to encrypt the entire device or encrypt company-specific/selected files and folders.
- **Data wiping**: Check whether there is a support for selective wipe.
- **Auto-provisioning of devices:** Check whether there is any option for automatic device provisioning.
- **Architecture**: Analyze the approach used by the vendor for the MDM solution such as sandbox, virtualization, or the integrated approach; this helps in understanding the technology used by the vendor and accordingly planning for the future.
- **Location capabilities and network access restrictions:** Determine whether the MDM solution supports policies to let employees use their device camera for personal use.
- **Inventory management:** Know whether individual mobile endpoints can be searches, custom filtered, and modified for hundreds of managed mobile devices.
- **Reports:** Know whether there is a built-in provision for reporting new devices, apps out of compliance, and devices that have not been checked-in for multiple days.



Mobile Device Management (MDM) Solutions: VMware Workspace ONE

VMware Workspace ONE is an intelligence-driven digital workspace platform that securely delivers and manages any app on mobile, anywhere with Workspace ONE.

Features:

- Quickly and efficiently add new devices to the enterprise network.
- Saves time by deploying mobile devices from one console.
- Send updates and configure new device settings over the air.
- Wipe or lock managed devices remotely.
- Guaranteed performance when using the latest web browsers.

Following are some examples of additional MDM solutions:

- **IBM MaaS360**

  Source: https://www.ibm.com

  MaaS360 supports the complete MDM lifecycle for smartphones and tablets, including iPhone, iPad, Android, Windows Phone, BlackBerry, and Kindle Fire. As a fully integrated cloud platform, MaaS360 simplifies MDM with rapid deployment and comprehensive visibility, and implements controls that span across mobile devices, applications, and documents.

- **XenMobile**

  Source: https://www.citrix.com

XenMobile MDM provides the role-based management, configuration, and security of corporate and user-owned devices. IT can enroll and manage devices, blacklist or whitelist apps, detect jailbroken or out-of-compliance devices and block their ActiveSync email access, and perform a full or selective wipe for lost or out-of-compliance devices.

- **Absolute Manage MDM**

  Source: http://www.absolute.com

  The Absolute platform allows organizations to see and secure all devices, data, applications, and users, thereby delivering zero-touch IT asset management, self-healing endpoint security, and always-on data visibility and protection.

- **Sicap Device Management Centre**

  Source: https://www.sicap.com

  Sicap Device Management Centre/Sicap DMC automatically detects new devices on network and configures them with the correct network settings in real time. Additionally, DMC provides white-labeled web tool and mobile applications for end users for device self-configuration. The DMC analytics tools provide a full and real-time breakdown view and segmentation of the device base on a network.

- **SOTI MobiControl**

  Source: https://www.soti.net

  SOTI MobiControl's MDM enhances enterprise mobility and enables BYOD initiatives. It offers remote control, helpdesk, location services, antivirus/malware protection, device provisioning, and asset management.

- **Scalefusion MDM**

  Source: https://scalefusion.com

  The Scalefusion MDM software features multi-OS management capabilities and is integrated with the Eva Communication Suite to drive effective team conversations.

- **ManageEngine Mobile Device Manager Plus**

  Source: https://www.manageengine.com

  ManageEngine Mobile Device Manager Plus MDM enables the management of smartphones, laptops, tablets, desktops, and multiple operating systems such as iOS, Android, Windows, macOS, and Chrome OS.

- **MobileIron MDM**

  Source: https://www.ivanti.com/

  MobileIron MDM provides the fundamental visibility and IT controls required to secure, manage, and monitor any corporate or employee owned mobile device or desktop that accesses business-critical data. It enables simple device enrollment, automated device

setup, mobile access control and secure connectivity, device compliance, and policy enforcement.

- **MediaContact**

  Source: https://en.telelogos-mediacontact.com

  MediaContact manages remote devices (laptop PCs, smartphones, tablets, rugged devices, embedded devices) running on Windows, Windows Mobile, or Android.

- **Beachhead's SimplySecure Management System**

  Source: https://www.beachheadsolutions.com

  Beachhead's SimplySecure management system allows organizations to remotely secure vulnerable mobile devices, including those owned by employees.

  Features:

  - Customizable reporting of status and device risks/conditions
  - Remote enforcement of password and security policy
  - Full encryption of all sensitive data on the devices
  - Immediate data access elimination with instant, administrator-enabled remote restoration
  - Complete data wipe capability when devices are stolen
  - Broad range of administrator-enabled and automatic security responses to threat conditions

- **Microsoft Intune**

  Source: https://www.microsoft.com

  Microsoft Intune offers MDM and its key features and advantages include:

  - Supporting a diverse mobile environment and managing iOS, Android, Windows, and macOS devices securely.
  - Ensuring that the devices and apps comply with the security requirements of an organization.
  - Creating policies that help keep the organization data safe on organization-owned and personal devices.
  - Using a single, unified mobile solution to enforce these policies, and help in managing devices, apps, users, and groups.
  - Protecting information by helping to control the ways in which the workforce accesses and shares its data.

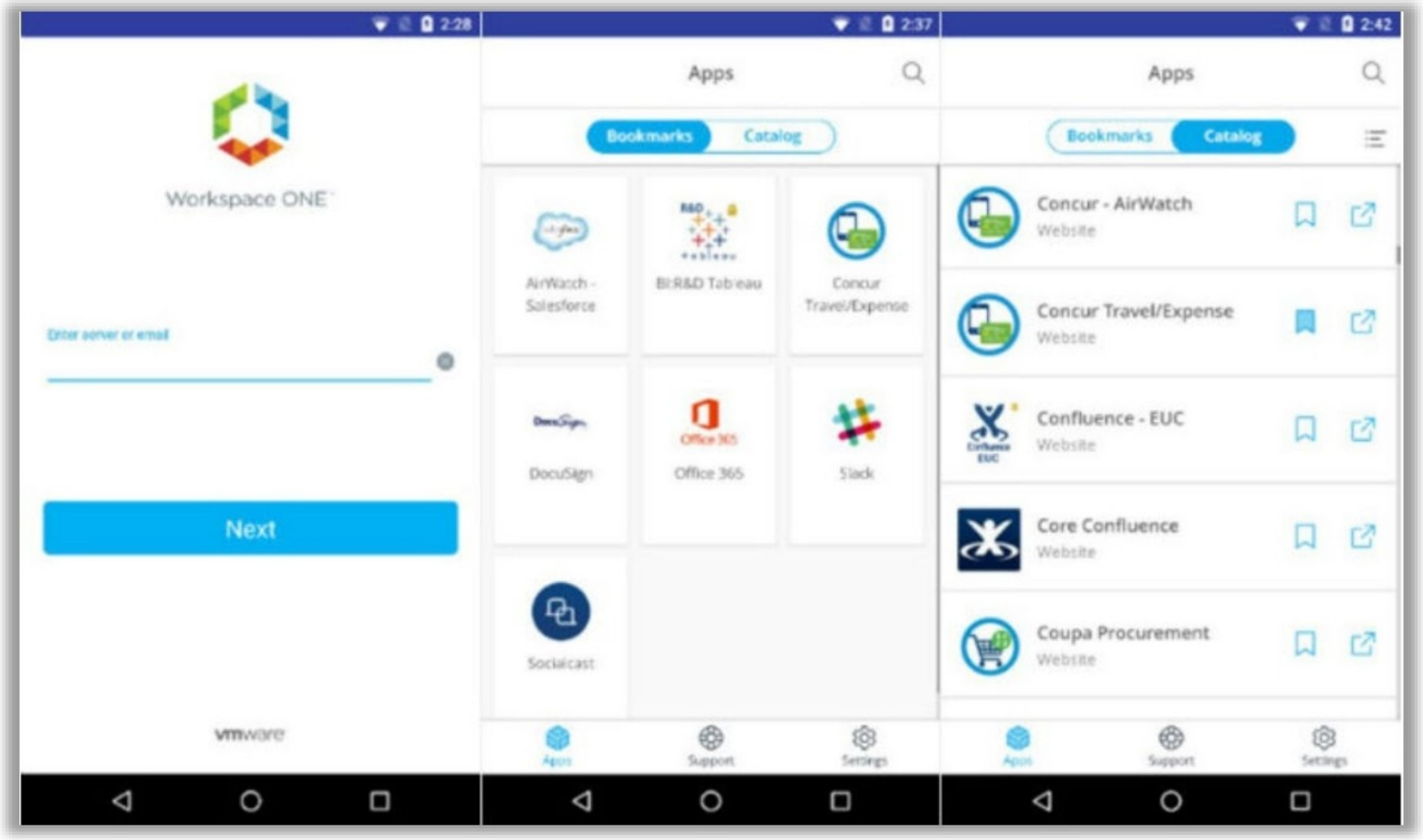
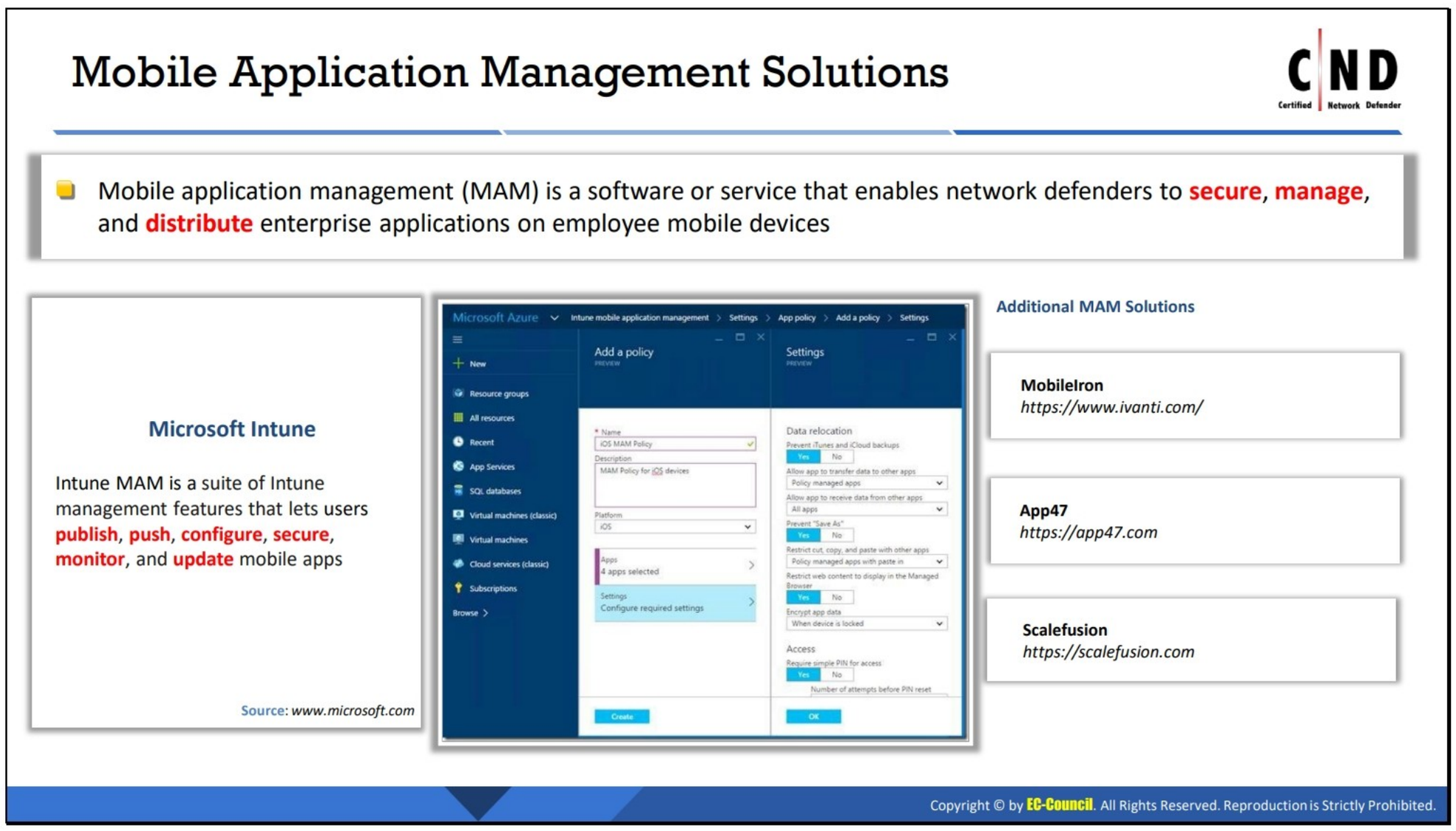


Figure 7.1: VMware Workspace ONE app



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.

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.

- **MobileIron's Mobile Application Management (MAM)**

  Source: https://www.mobileiron.com

  MobileIron MAM drives business productivity with a mobile application security framework that enables the distribution, protection, and management of apps.

- **App47's Mobile Application Management (MAM)**

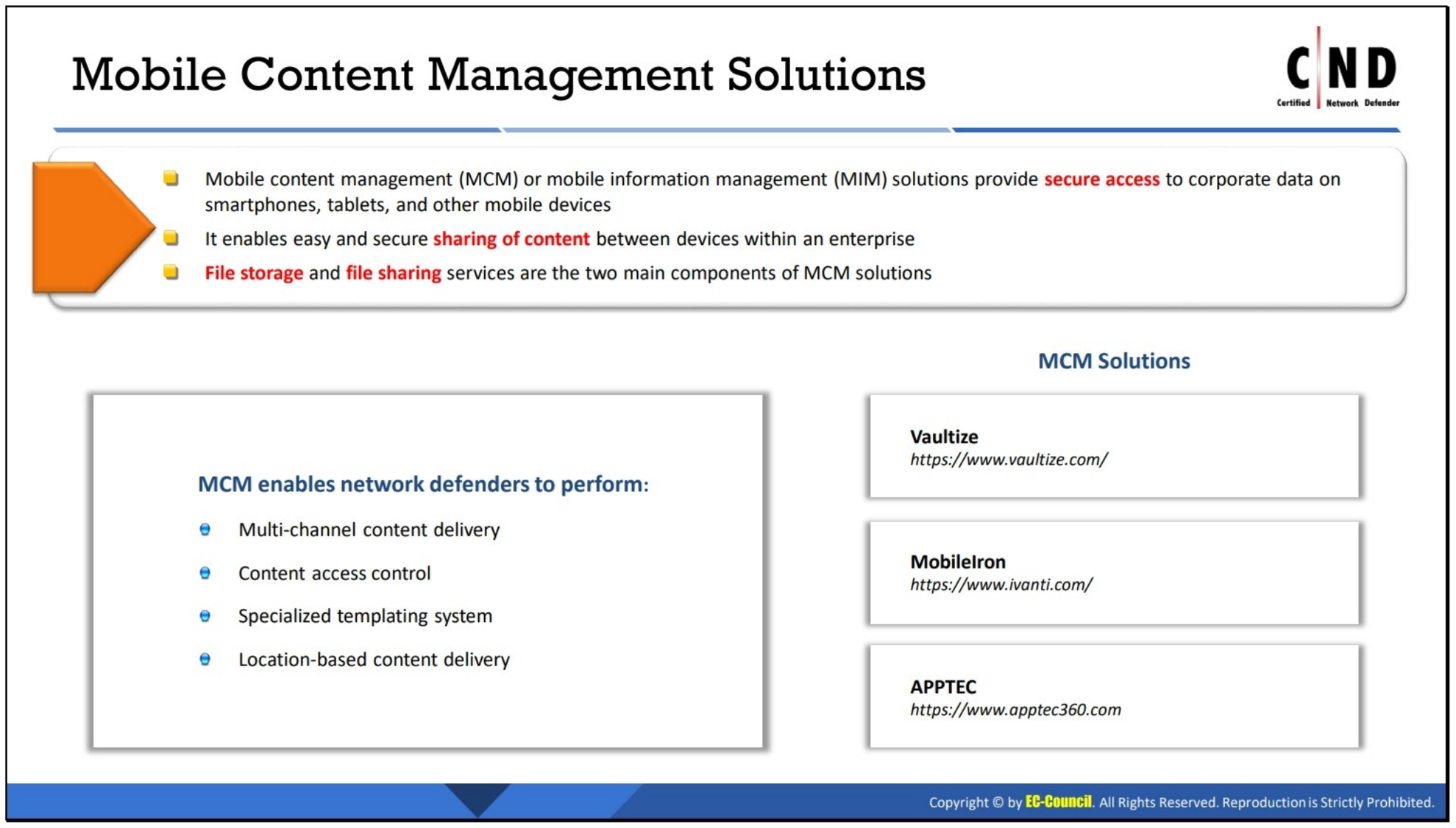
  Source: https://app47.com

  App47 securely and efficiently delivers mobile applications to a diverse audience of employees or customers.

- **Scalefusion Mobile Application Management (MAM)**

  Source: https://scalefusion.com

  Scalefusion MAM securely distributes in-house and public apps to devices that use the Scalefusion Enterprise Store or Google Play.



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.

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 MCM**

  Source: https://www.vaultize.com

  Vaultize's mobile data containerization provides end-to-end data security on all leading devices and industry MCM tools. These tools ensure the encryption of important files and data, as well as track and wipe them from the source to mobile devices within the organization and beyond.

- **MobileIron MCM**

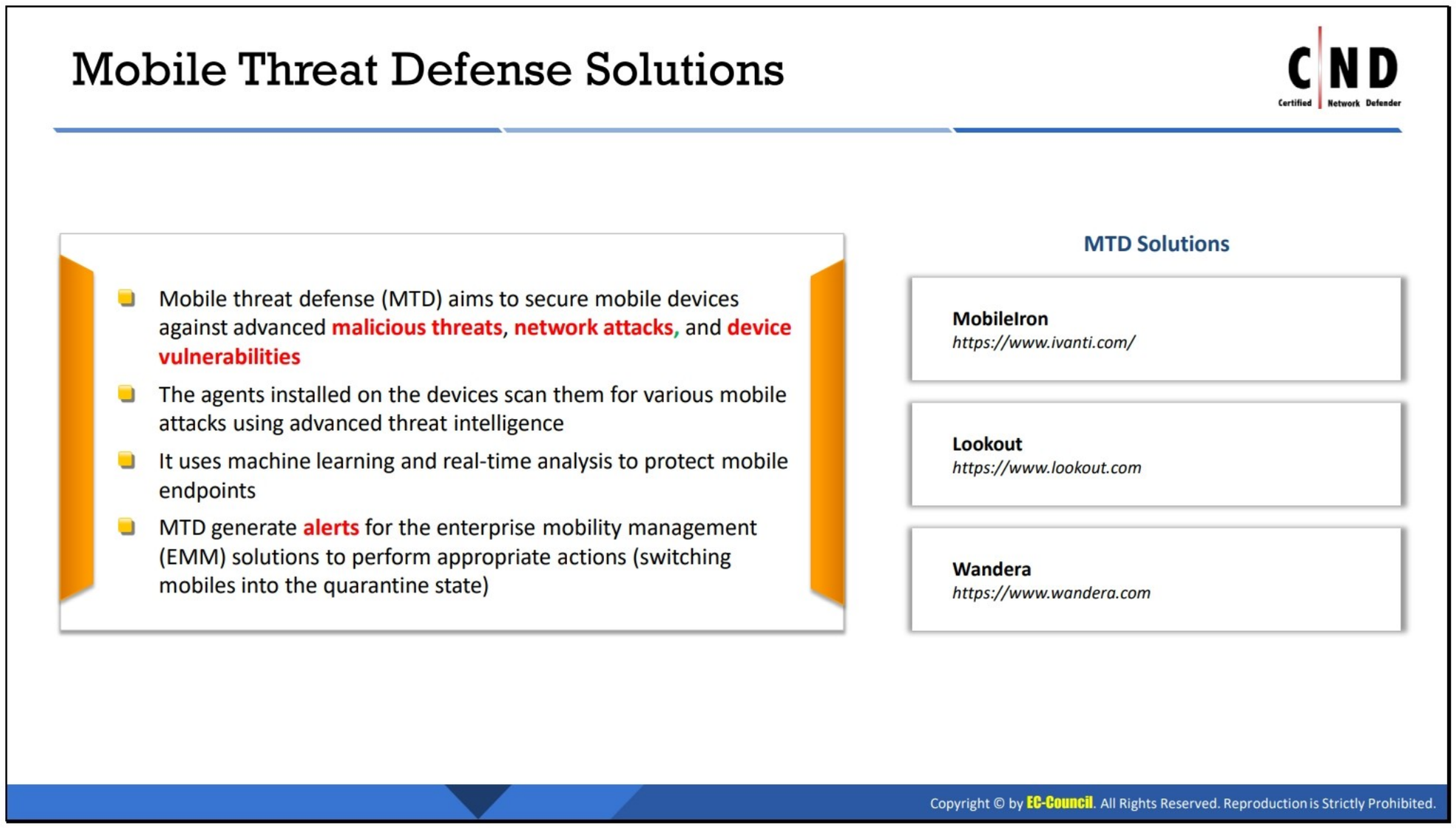
  Source: https://www.ivanti.com

  MobileIron MCM allows employees to access critical business content and collaborate seamlessly across any network on any device without security prompts interrupting their workflow.

- **APPTEC MCM/ContentBox**

  Source: https://www.apptec360.com

  APPTEC ContentBox provides a tool to work productively with simple, ordered, but functional mobile applications, while enabling control over confidential data.



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 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.

- MTD secures against device/physical threats by adding active threat detection and risk-based mobile management for more educated policy enforcement.
- MTD secures against malware by
  - Scanning devices and applications for the signs of malicious activity
  - Informing the security teams of the existence of any malware
  - Finding zero-day-threats
  - Monitoring connections to suspicious domains
  - Blocking any attempts for downloading malicious files before they even reach the device
  - Preventing outbound connections attempted by malware
- MTD secures against phishing by

- Providing visibility if an employee navigates to a known mobile phishing page
- Blocking access to phishing links quickly if an employee tries to access it

- MTD secures against network attacks by
  - Encrypting traffic automatically when connecting to open Wi-Fi networks
  - Scanning the real-time data communications made with each website and mobile app
  - Identifying instances when data are being transmitted insecurely
  - Identifying data leaks to block access to risky content, thereby removing the possibility of man-in-the-middle (MITM) attacks.

MTD Security at Different Levels of Mobile Enterprise

MTD solutions provide security at different levels of a mobile enterprise.

- **Device Level**

  MTD solutions can

  - Monitor the following indicators to identify security misconfigurations, device vulnerabilities, and malicious activity.
    - OS versions
    - Security update versions
    - System parameters
    - Device configuration
    - Firmware
    - System libraries
  - Check for
    - Modification of system libraries
    - Modification of configuration
    - Privilege escalation (such as jailbreak or rooting)

- **Network Level**

  MTD solutions can

  - Monitor cellular and wireless network traffic for unauthorized access
  - Monitor malicious behavior
  - Check for invalid or spoofed certificates
  - Strip off Transport Layer Security (TLS) or Secure Sockets Layer (SSL)
  - Perform customized MITM detection techniques

- **Application Level**

  MTD solutions can

  - Identify grayware and malware through application sandboxing and code analysis.
  - Use application security techniques such as
    - Signature-based anti-malware filtering
    - Code emulation or simulation
    - Application reverse engineering
    - Static and dynamic app security testing

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 MTD**

  Source: https://www.ivanti.com

  MobileIron MTD provides always-on mobile threat protection solutions with machine learning algorithms to block all types of mobile device threats on any device.

- **Lookout MTD**

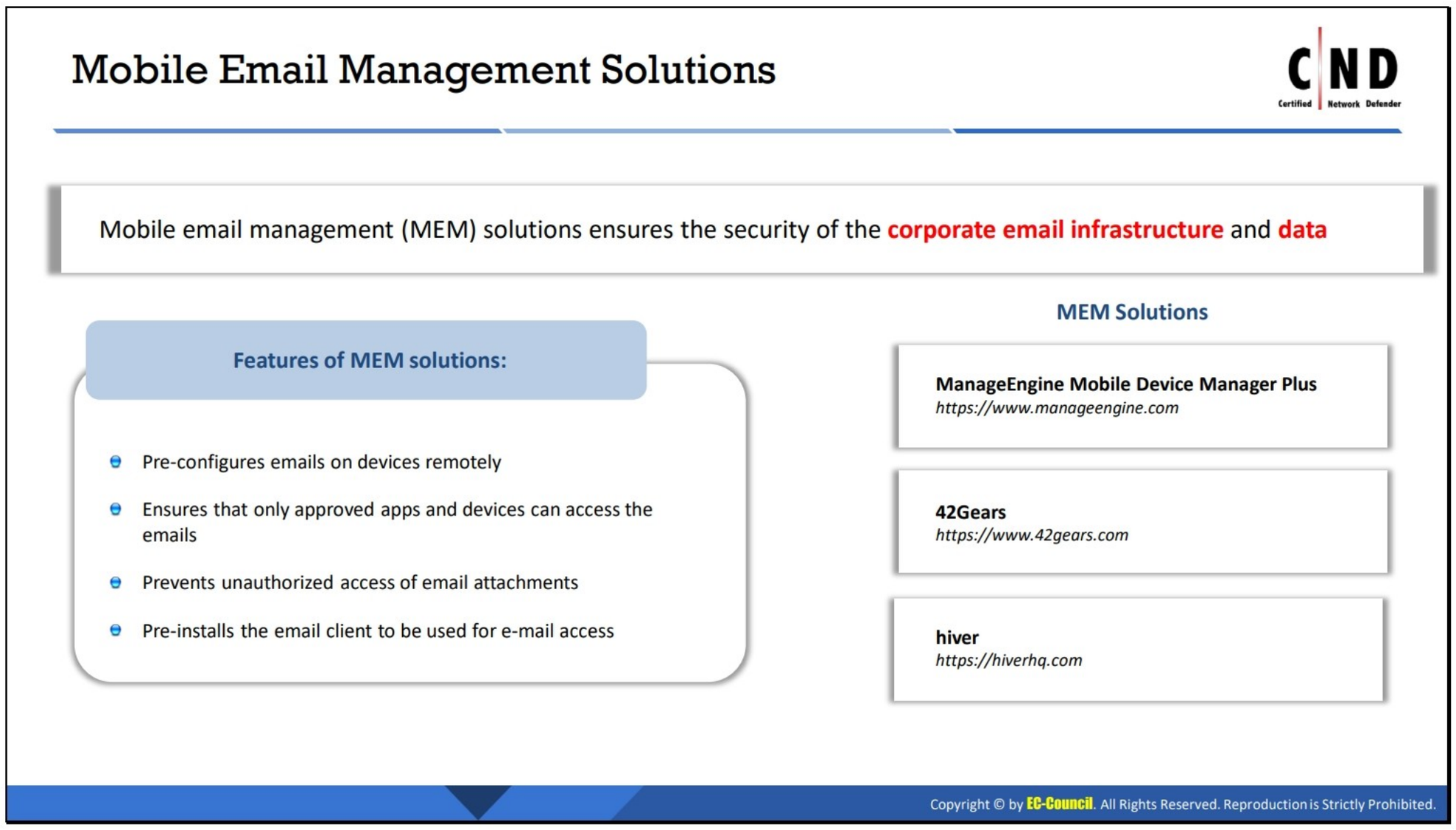
  Source: https://www.lookout.com

  Lookout MTD addresses all mobile device security issues. It protects against phishing, content filtering, and VPN.

- **Wandera MTD**

  Source: https://www.wandera.com

  Wandera MTD provides multi-level protection for mobile users, endpoints, and corporate applications. It can exempt employees from cyber threats, control unwanted access, and prevent data breaches.



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:

- **ManageEngine Mobile Device Manager Plus MSP**

  Source: https://www.manageengine.com

  The MEM of Mobile Device Manager Plus MSP allows to configure, secure and manage corporate mobile email accounts.

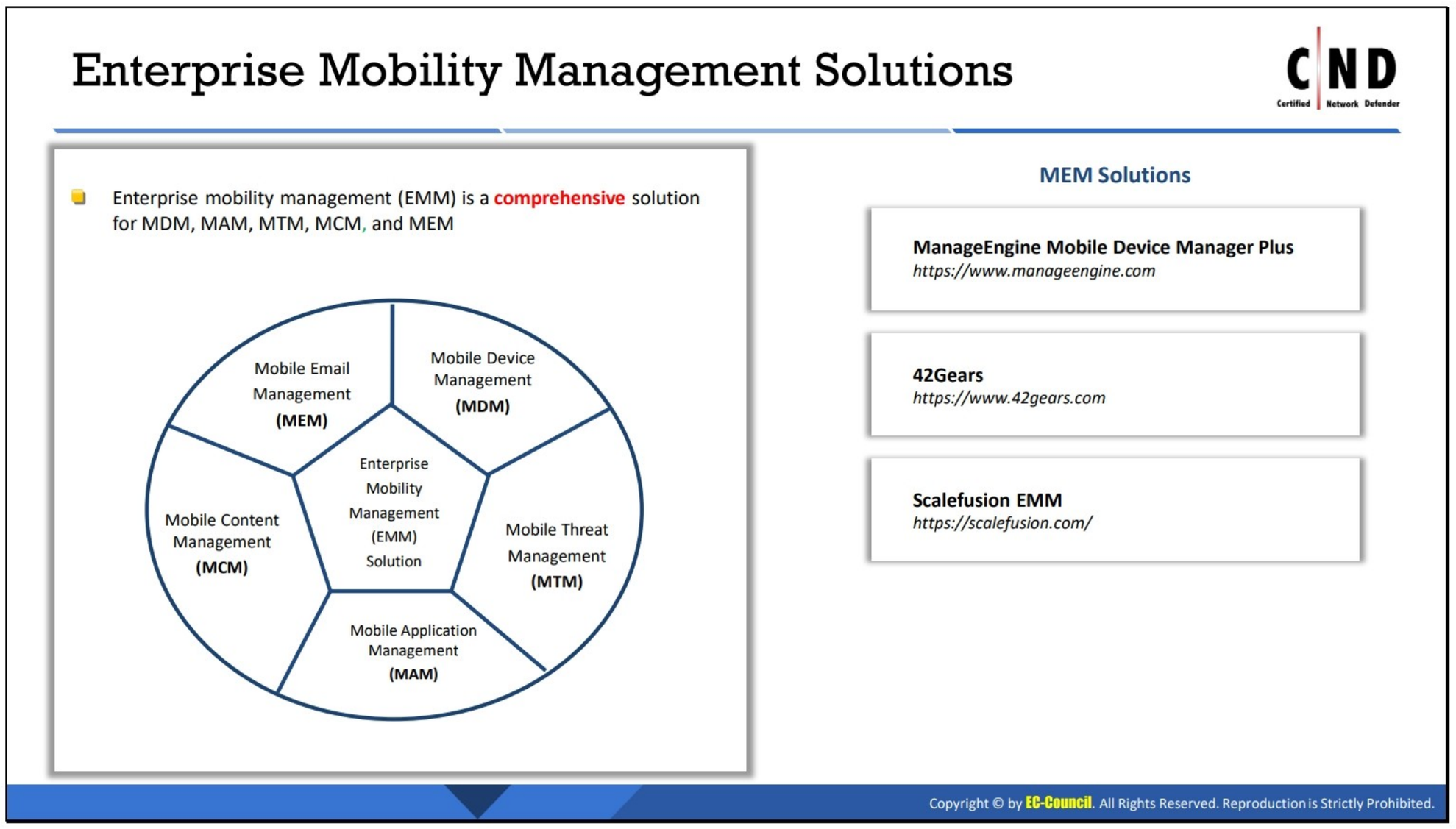
- **42Gears MEM**

  Source: https://www.42gears.com

  42Gears MEM allows to control of the mobile devices that access emails, prevents data loss, enforces strict compliance policies, and encrypts sensitive corporate data.

- **Hiver**

  Source: https://hiverhq.com
  Hiver brings email, live chat, knowledge base, and voice communication inside Gmail. Ensures end-to-end accountabilities for all incoming emails.



Enterprise Mobility Management Solutions

Enterprise mobility management (EMM) is a comprehensive solution responsible for safeguarding the enterprise data accessed and used by employee mobile devices. 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

EMM Solution Deployment Process

The deployment of EMM solutions can be categorized into the following four phases:

Plan: It is important to understand the EMM implementation requirements from an organizational perspective and collect feedback from the key stakeholders. Addressing the following considerations will help in developing a proper EMM deployment plan.

- Employee/user expertise on using mobile devices
- Mobile OSes and device support
- Organization network complexity
- IT governance framework, policies, and process
- Employee training resources
- Organization security requirements

Design: In this phase, the policies for mobility management are defined.

- Define roles: Define the various administrative tasks to be implemented and identify the administrative users and their responsibilities.
- Define visibility: Determine the role of each administrator and their access to the devices being managed by them.
- Assign actors: Identify and assign the actions that should be performed by each administrator.
- Manage distribution: Identify the apps, policies, and configurations to be deployed; identify the users who will deploy them and when.

Deploy: In this phase, the deployment approach to be followed for implementing EMM is determined. The pricing models (subscription rate or perpetual licensing) are examined while selecting either cloud-based solutions or the on-premise approach.

Implement: Before implementation, ensure that the helpdesk staff is prepared. Following key considerations should help in preparing the helpdesk team.

- Train the helpdesk team about various devices, servers, and network issues that may arise.
- Define the troubleshooting steps, escalation process, and responsibilities to resolve issues.
- Provide helpdesk with the required resources to support the users.
- Educate them about device upgrades.

Consideration for EMM Solution Implementation

The following factors will help an organization to successfully implement an EMM solution.

- Understand the requirements
- Understand the end users and the IT infrastructure
- Determine the deployment approach to follow
- Understand the total cost for EMM implementation
- Ensure that the current infrastructure will be suitable for EMM
- Select EMM vendor
- Manage changes to IT and helpdesk
- Design EMM policies
- Training for end users
- Create an actionable timeline and implement EMM
- Launch EMM

Examples of MEM Solutions

- **ManageEngine Mobile Device Manager Plus**

  Source: https://www.manageengine.com

  ManageEngine Mobile Device Manager Plus is a comprehensive mobile device management solution designed to empower enterprise workforce with the power of mobility, by enhancing employee productivity without compromising on corporate security. It lets manage smartphones, tablets, laptops, desktops, TVs, and rugged devices and multiple operating systems such as Android, iOS, iPadOS, tvOS, macOS, Windows, and Chrome OS.

- **42Gears MEM**

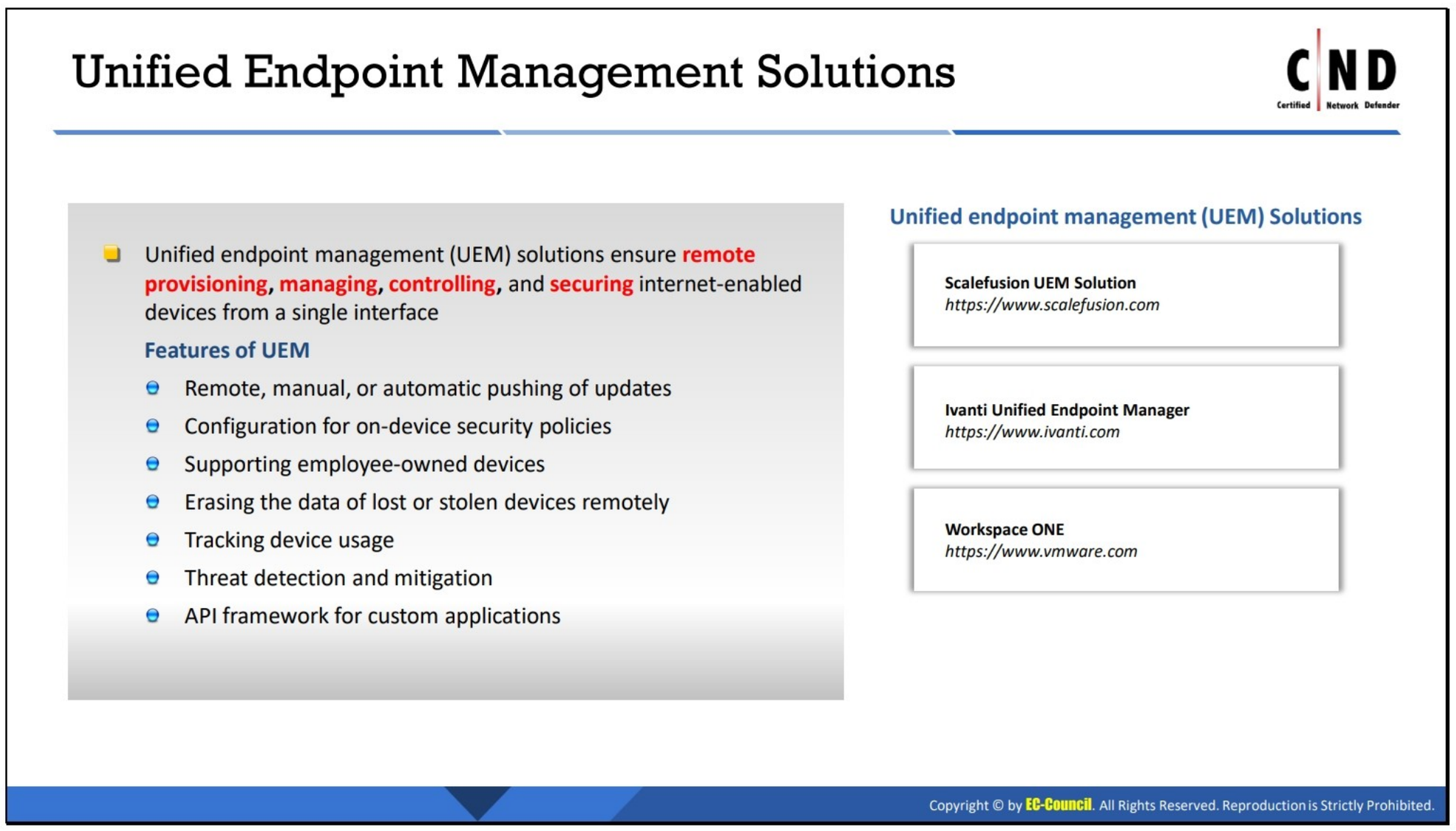
  Source: https://www.42gears.com

  42Gears MEM allows control of the mobile devices that access emails, prevents data loss, enforces strict compliance policies, and encrypts sensitive corporate data.

- **Scalefusion EMM**

Source: https://scalefusion.com

Scalefusion EMM (Enterprise Mobility Management): Employers can increase productivity and efficiency by using Scalefusion to secure and manage both company-owned and BYO devices. By offering a single platform to manage and secure endpoints, an enterprise communications suite, and a set of capabilities to streamline device management operations, Scalefusion EMM Software enables an organization to implement a perimeter-less mobility strategy.



Unified Endpoint Management Solutions

Unified endpoint management (UEM) solutions helps 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.

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:

- **Scalefusion UEM**
  Source: https://scalefusion.com

Scalefusion secures and manages endpoints that include tables, smartphones, digital signages, and rugged devices. Use Scalefusion API for a customized management experience.

- **Ivanti Unified Endpoint Manager**

  Source: https://www.ivanti.com

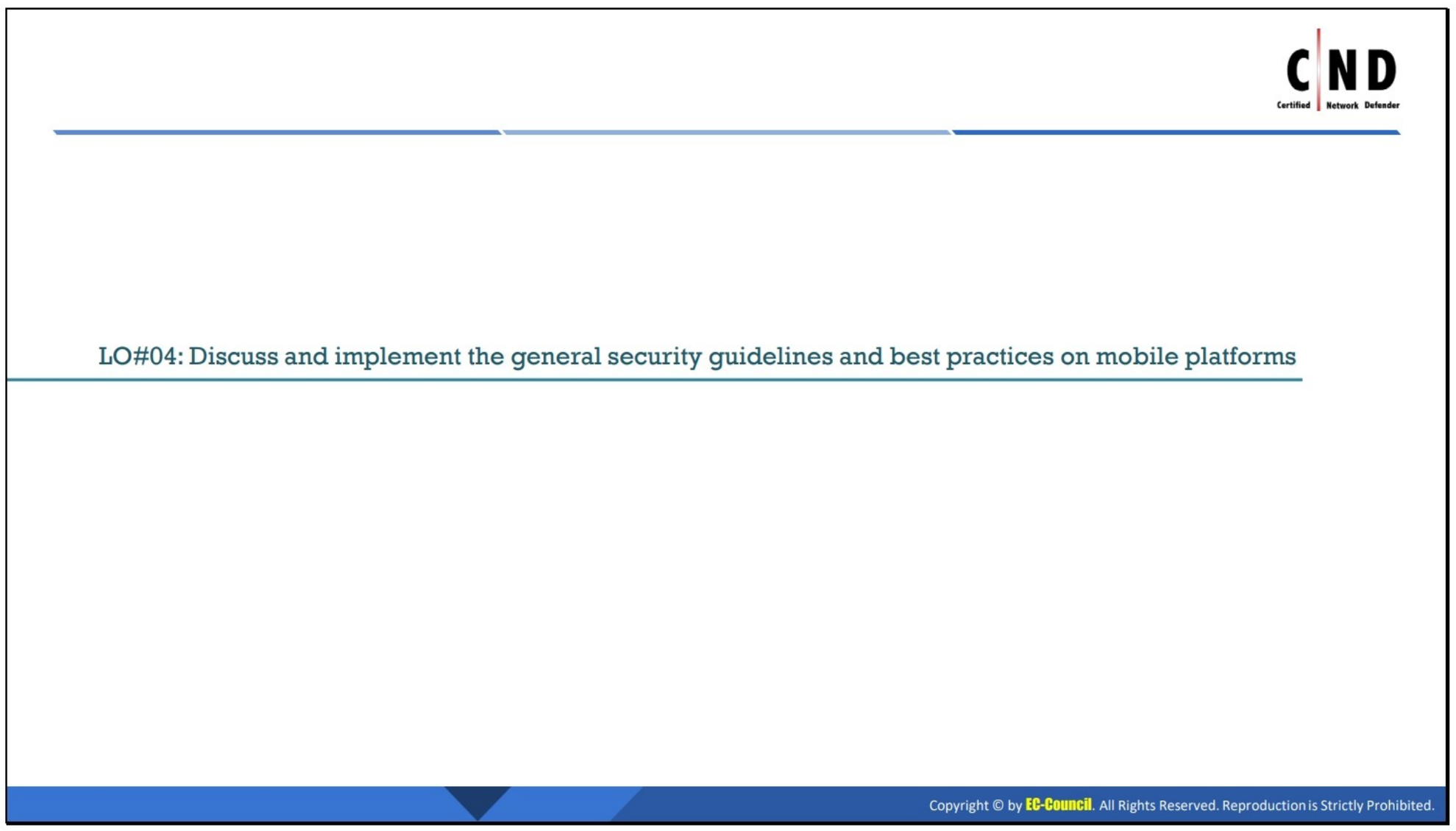
  Ivanti Unified Endpoint Manager is a user-profile management software that helps in

  - Discovering everything that touches the enterprise network
  - Automating software delivery
  - Reducing issues related to the login performance
  - Integrating actions with multiple IT solutions.

- **Workspace ONE UEM**

  Source: https://www.vmware.com

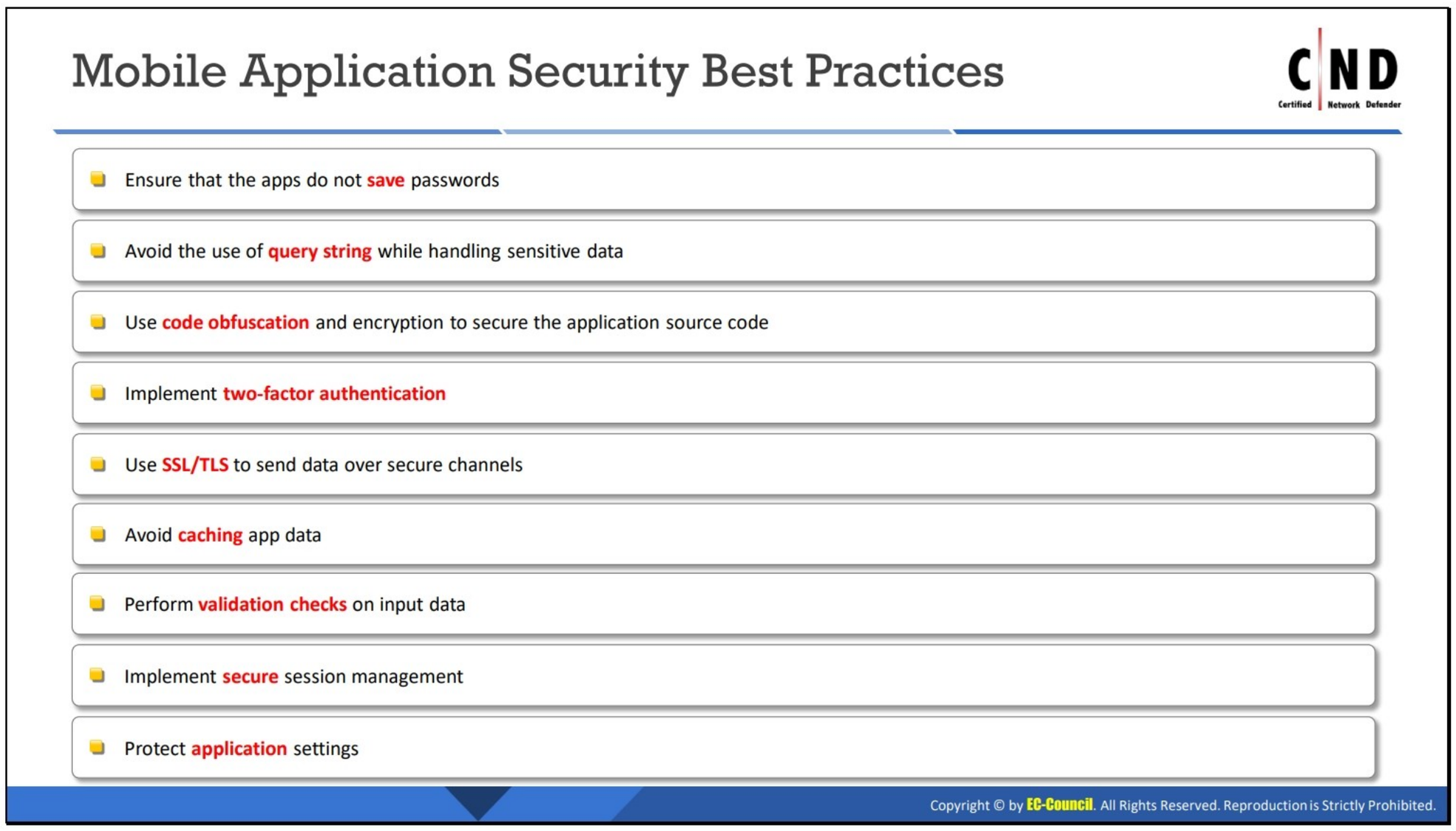
  Workspace ONE UEM, powered by the AirWatch technology, can reduce costs and improve security with modern, over-the-air management of mobile enterprise, and ensure enterprise security at each layer.



LO#04: Implementing the General Security Guidelines and Best Practices on Mobile Platforms

The objective of this section is to explain the general security guidelines and best practices to be implemented for securing mobile platforms.

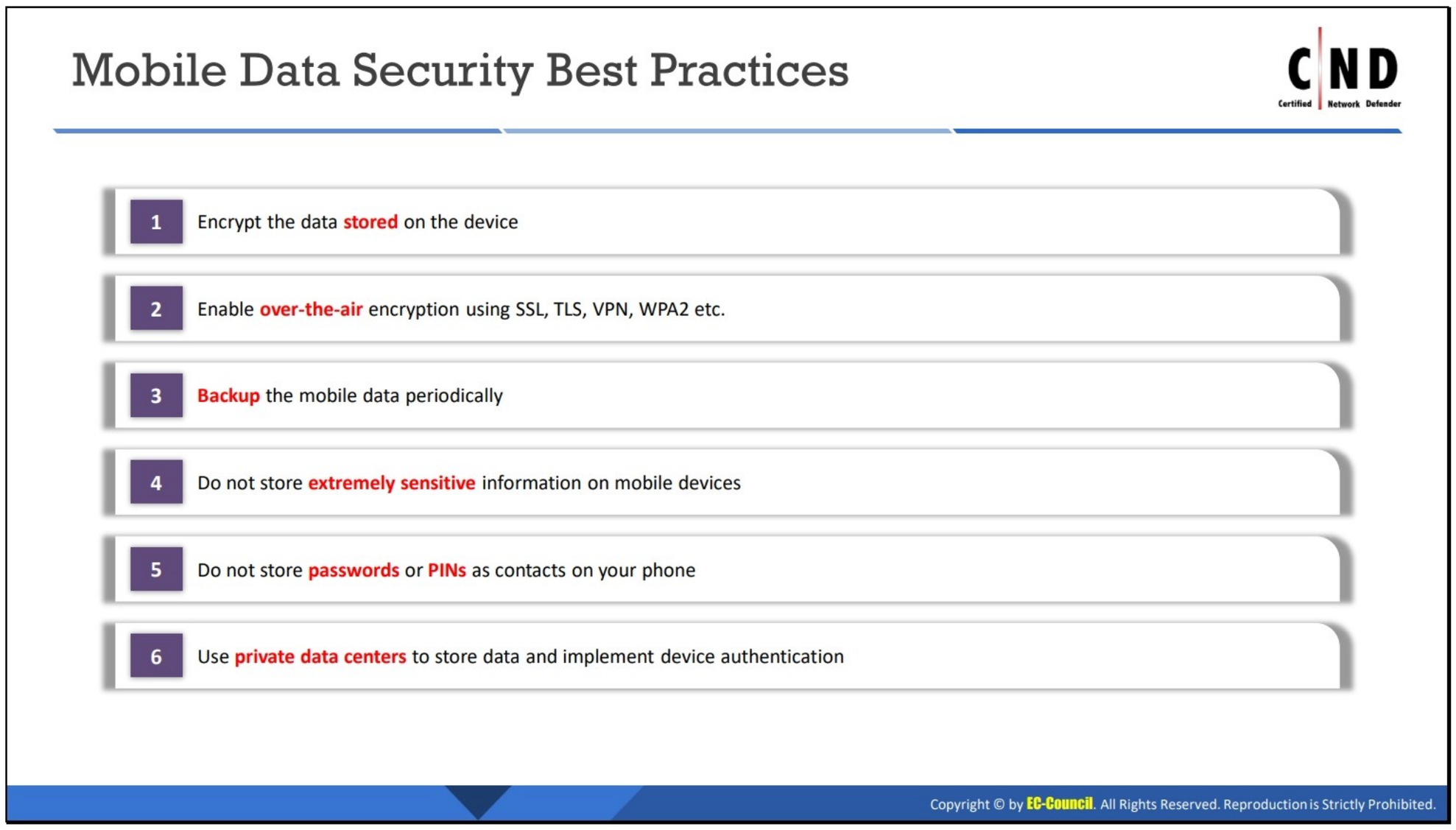
Enterprise-level mobile security management solutions can only deliver their promised benefits if they are backed by strong mobile device security practices.



Mobile Application Security Best Practices

Security best practices that protect mobile applications:

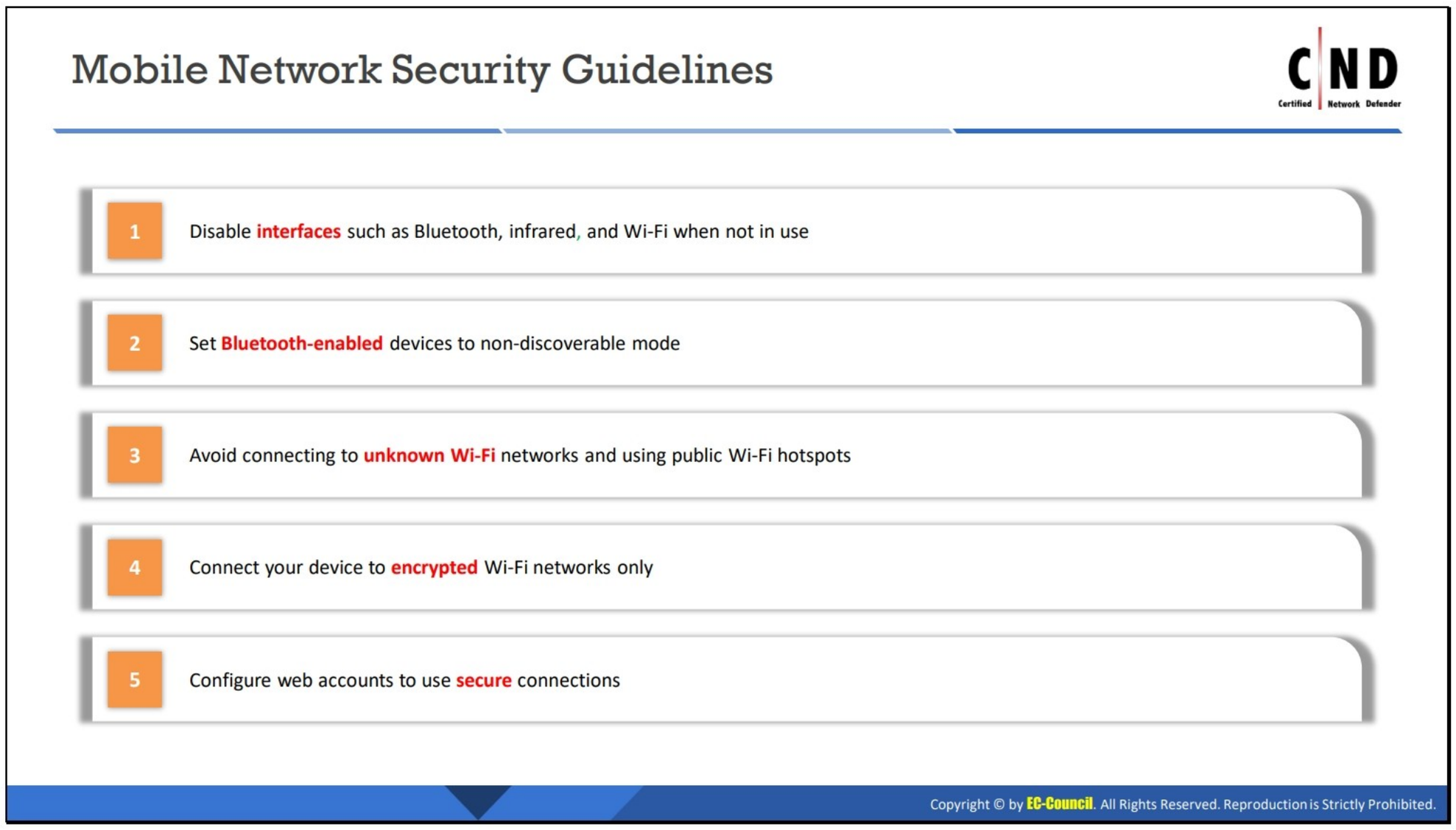
- Ensure that the apps do not save passwords
- Avoid using query string while handling sensitive data
- Use code obfuscation and encryption to secure the application source code
- Implement two-factor authentication
- Use SSL/TLS to send data over a secure channel
- Avoid caching app data
- Perform validation 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:

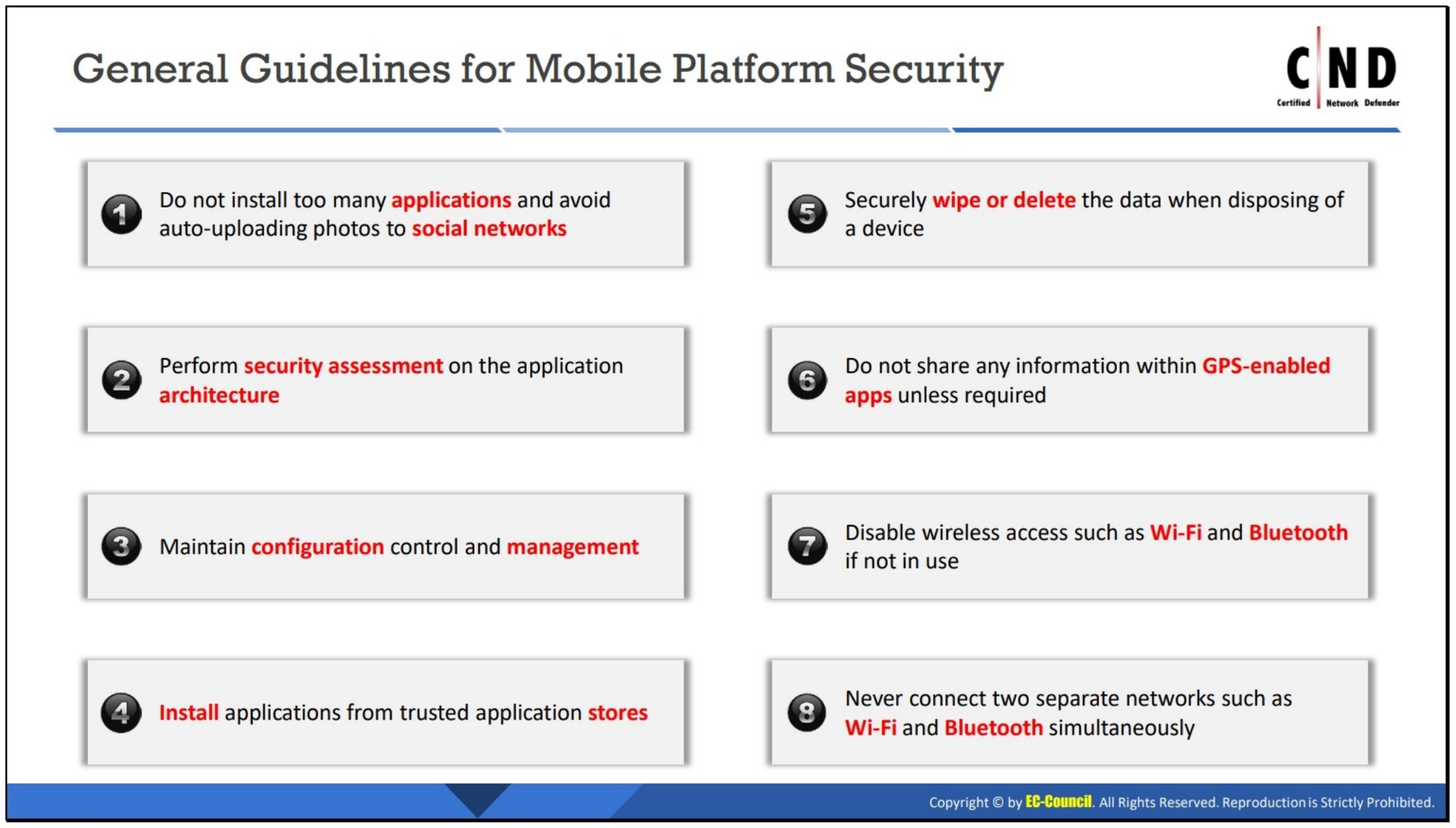
- Secure mobile infrastructure and strengthen the endpoints
- Encrypt the data stored on devices
- Enable over-the-air encryption using SSL, TLS, VPN, and WPA2
- Backup mobile data periodically
- Do not store extremely sensitive information on mobile devices
- Do not store passwords or PINs as contacts 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

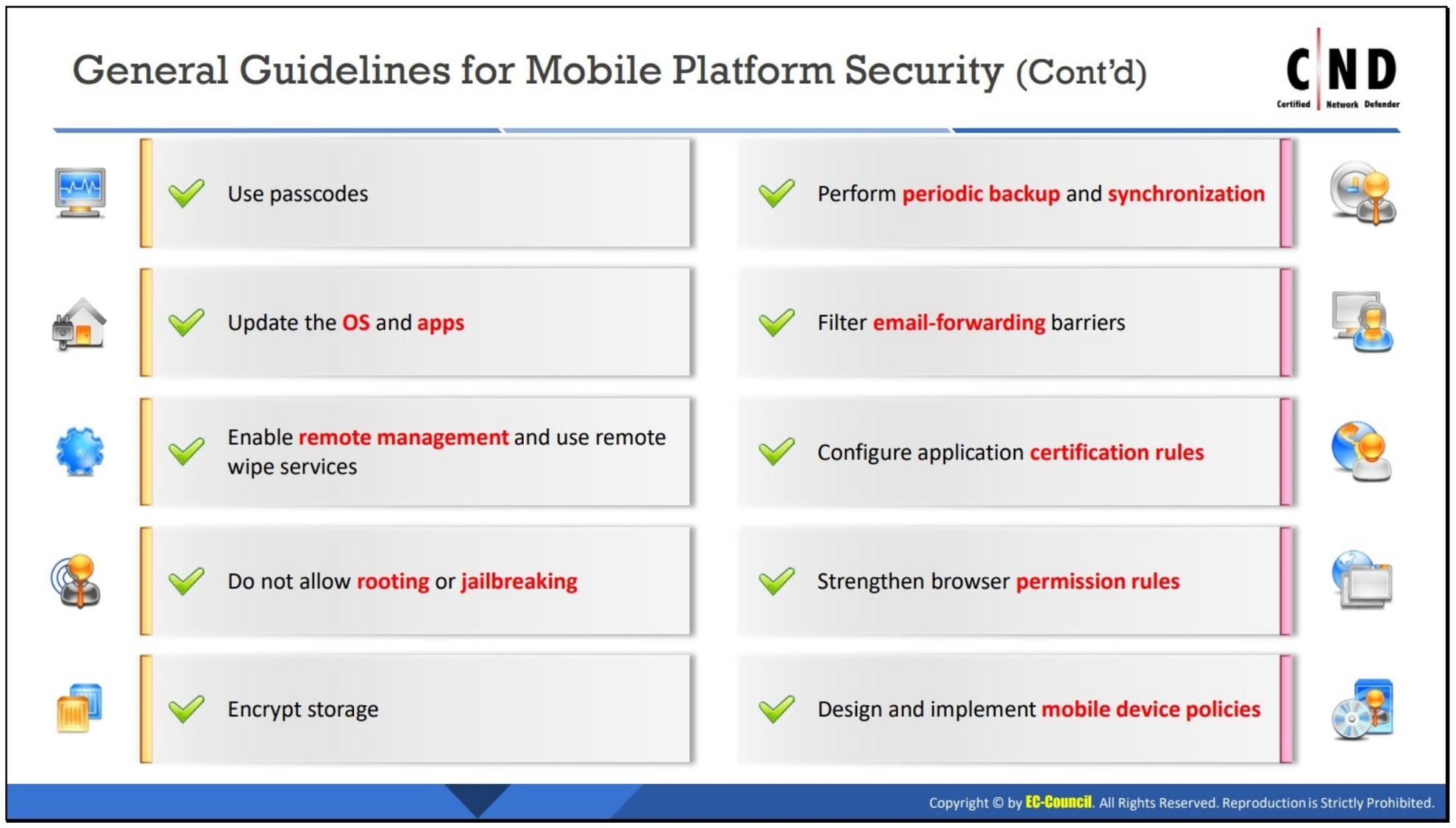


Mobile Network Security Guidelines

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

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
  - Ensure that your Bluetooth is "off" by default. Turn it on whenever it is necessary.
  - Disable wireless access such as Wi-Fi and Bluetooth if not in use to avoid illegal wireless access to devices.
  - Disable sharing/tethering internet connections over Wi-Fi and Bluetooth when not in use.
- **Use Passcode**
  - Configure a strong passcode with the maximum possible length.
  - Set an idle timeout to automatically lock the phone when not in use.
  - Enable the lockout/wipe feature after a certain number of attempts.
  - Consider eight-character passcodes
  - Prevent passcode guessing by setting erase data to ON.
- **Update OS and Apps**
  - Update the OS and apps to keep them secure.
  - Install software updates when new releases are available.
  - Perform regular software maintenance.
- **Enable Remote Management**
  - In an enterprise environment, use MDM solutions to secure, monitor, manage, and support mobile devices deployed across an organization.
- **Do Not Allow Rooting or Jailbreaking**
  - Ensure that the employed MDM solutions prevent or detect rooting/jailbreaking attempts.
  - Include this clause in the mobile security policy of the organization.
- **Use Remote Wipe Services**
  - Use remote wipe services such as Find My Device (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device if it is lost or stolen.
  - Report a lost or stolen device to IT so that they can disable the certificates and other access methods associated with the device.

- **Encrypt Storage**
  - If supported, configure your mobile device to encrypt its storage with hardware encryption.
  - Use device encryption and patch applications.
  - Encrypt the device and its backups.
- **Perform Periodic Backup and Synchronization**
  - Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization.
  - Backup to your Google account (Android) so that sensitive enterprise data are not backed up on the cloud.
  - Control the location of backups.
  - Encrypt backups.
  - Keep sensitive data away from shared mobile devices. If enterprise information is locally stored on a device, then it is recommended that this device not be openly shared.
  - Limit logging data stored on device.
  - Use secure data-transfer utilities or encrypt the data in transit to or from the device to ensure confidentiality and data integrity.
- **Filter Email-forwarding Barriers**
  - Filter emails by configuring the server-side settings of the corporate email system
  - Use commercial data loss prevention filters
  - Prevent local caching of emails
- **Configure Application Certification Rules**
  - Enable the installation and execution of signed applications only
  - Configure wireless to ask to join networks
  - Sandbox application and data
  - Enable auto-lock and set it to 1 min
  - Consider the privacy implications before enabling location-based services and limit the usage to trusted applications
  - Configure location services to disable location tracking for applications
  - Configure notifications to disable the ability to view notifications while the device is locked to prevent displaying sensitive data

- Configure AutoFill: Auto-fill names and passwords in browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by the enterprise policy)
- Disable the collection of diagnostics and usage data under **Settings → General → About**

- **Strengthen Browser Permission Rules**
  - Strengthen the browser permission rules according to the company security policies to avoid attacks.
- **Design and Implement Mobile Device Policies**
  - Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices.
- 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
- Verify the location of printers before printing sensitive documents
- Ask the IT department about the use of Citrix technologies to store data in data centers and maintain the privacy of personal devices.
- If sensitive data must be stored on a mobile device, use Follow-Me-Data and ShareFile as an enterprise-managed solution.

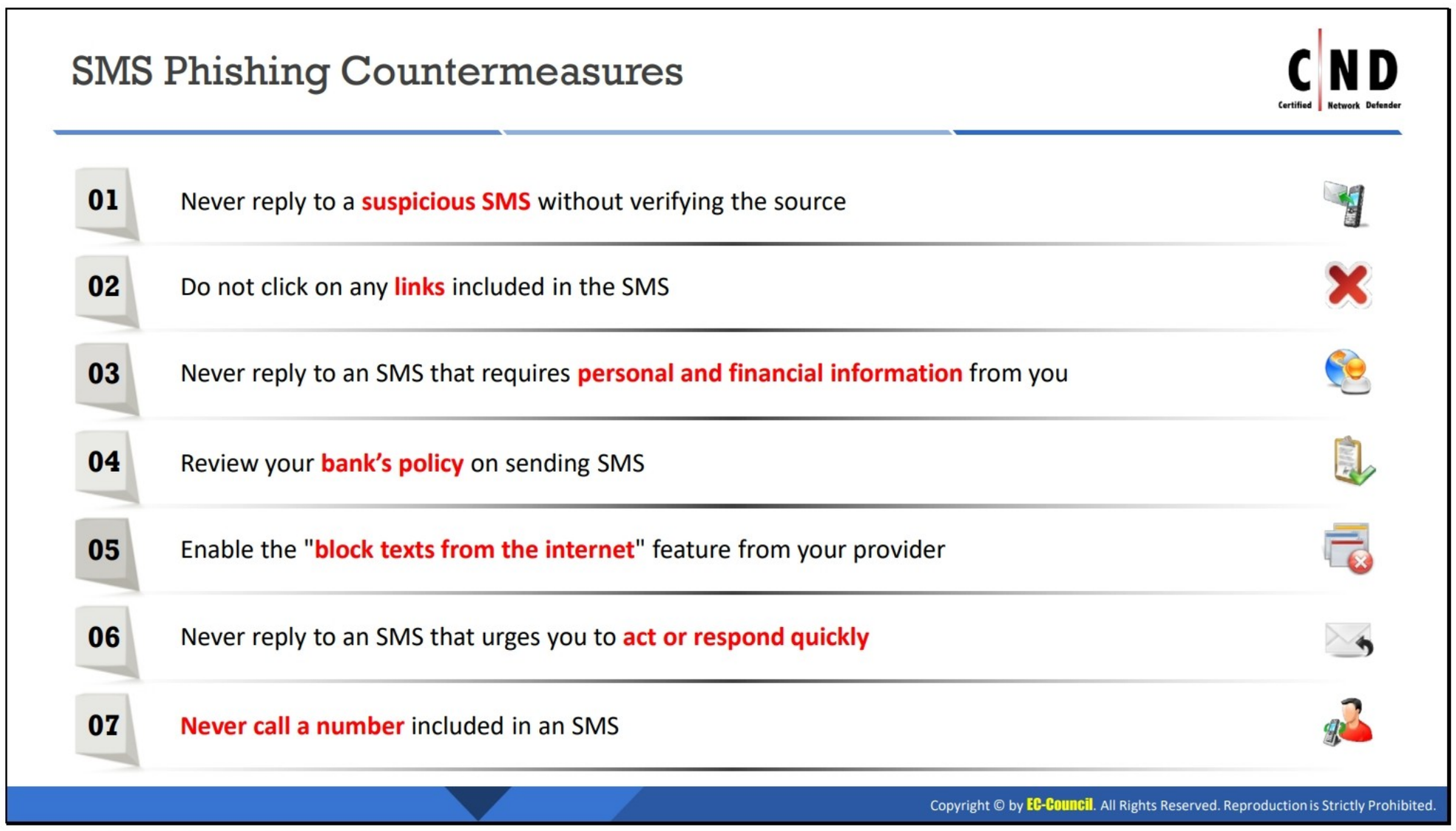
Mobile Device Security Guidelines for Administrators

Given below are some administrator guidelines to maintain corporate mobile device security:

- Publish an enterprise policy that specifies the acceptable usage of consumer-grade devices and BYOD in the enterprise.
- Publish an enterprise policy for the cloud.
- Enable security measures such as antivirus to protect the data in data centers.
- Implement policies that specify the allowed levels of application and data access on consumer-grade devices and those that are prohibited.
- Specify a session timeout through the access gateway.
- Specify whether the domain password can be cached on the device or if users must enter it every time they request access.
- Determine the allowed access gateway authentication methods from the following:
  - No authentication
  - Domain only

- SMS authentication
- RSA SecurID only
- Domain + RSA SecurID

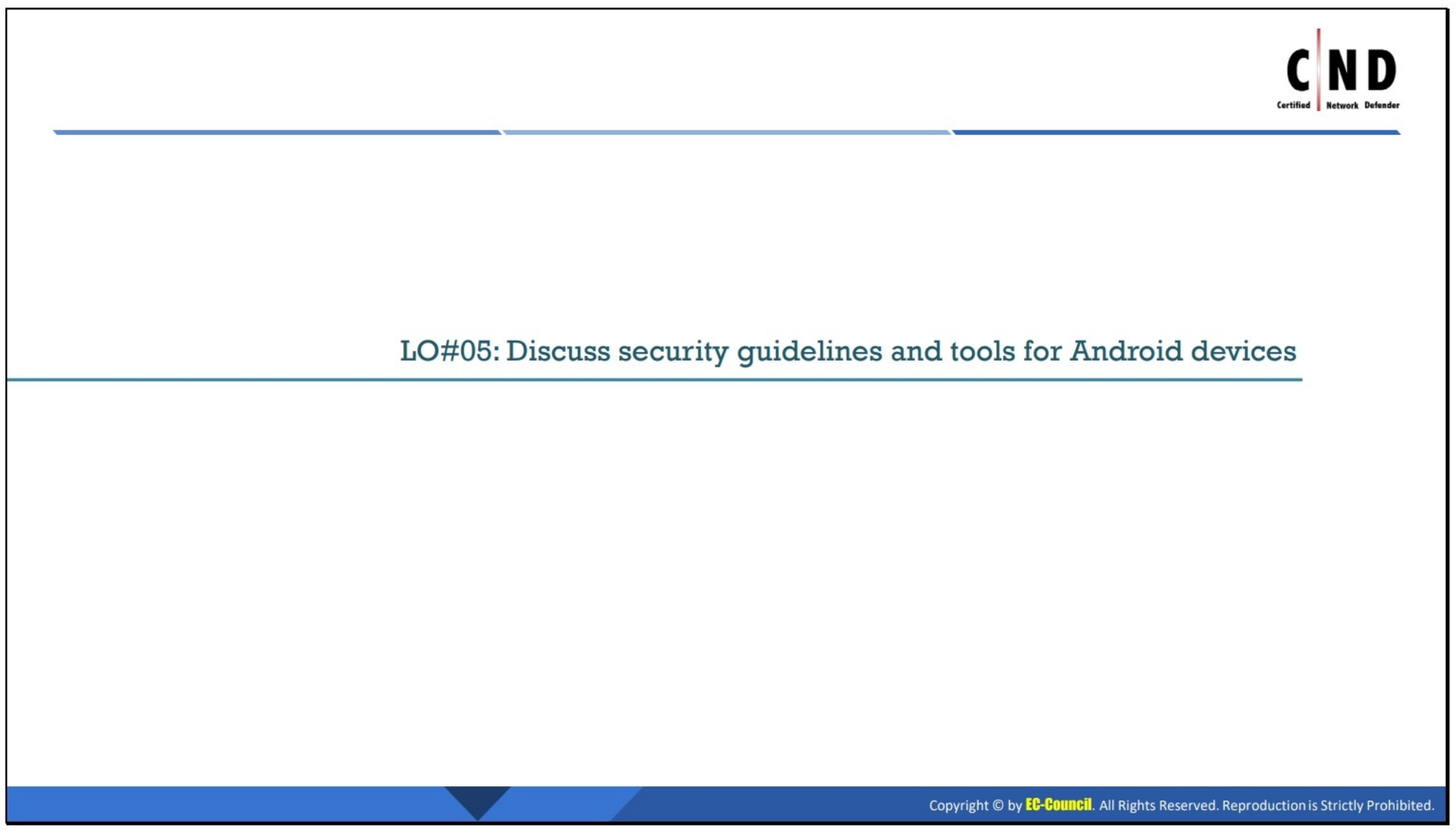
- Develop and maintain a mobile device security policy that specifies the organizational resources to access via mobiles, types of mobiles allowed, and access privileges, among others.
- Develop system threat models for mobile devices and the resources accessed using them, which enables an organization to design security solutions.
- Enable the required security settings for mobile devices before issuing them to users
- Regularly maintain mobile device security, including updated OS and apps, ensuring that mobile clocks are synchronized to a common time source, reconfiguring access privileges, and identifying and documenting abnormalities within device infrastructures.
- Regularly monitor whether users properly follow the policies and procedures framed for device security.
- Consider the best services provided by various service providers, determine the services suitable for the respective organization environments, then design and attain one or more solutions to meet these and any other requirements.
- Test the solutions before sending them into production. Evaluate various aspects of solutions such as authentication, app functionality, security, connectivity, and performance.



SMS Phishing Countermeasures

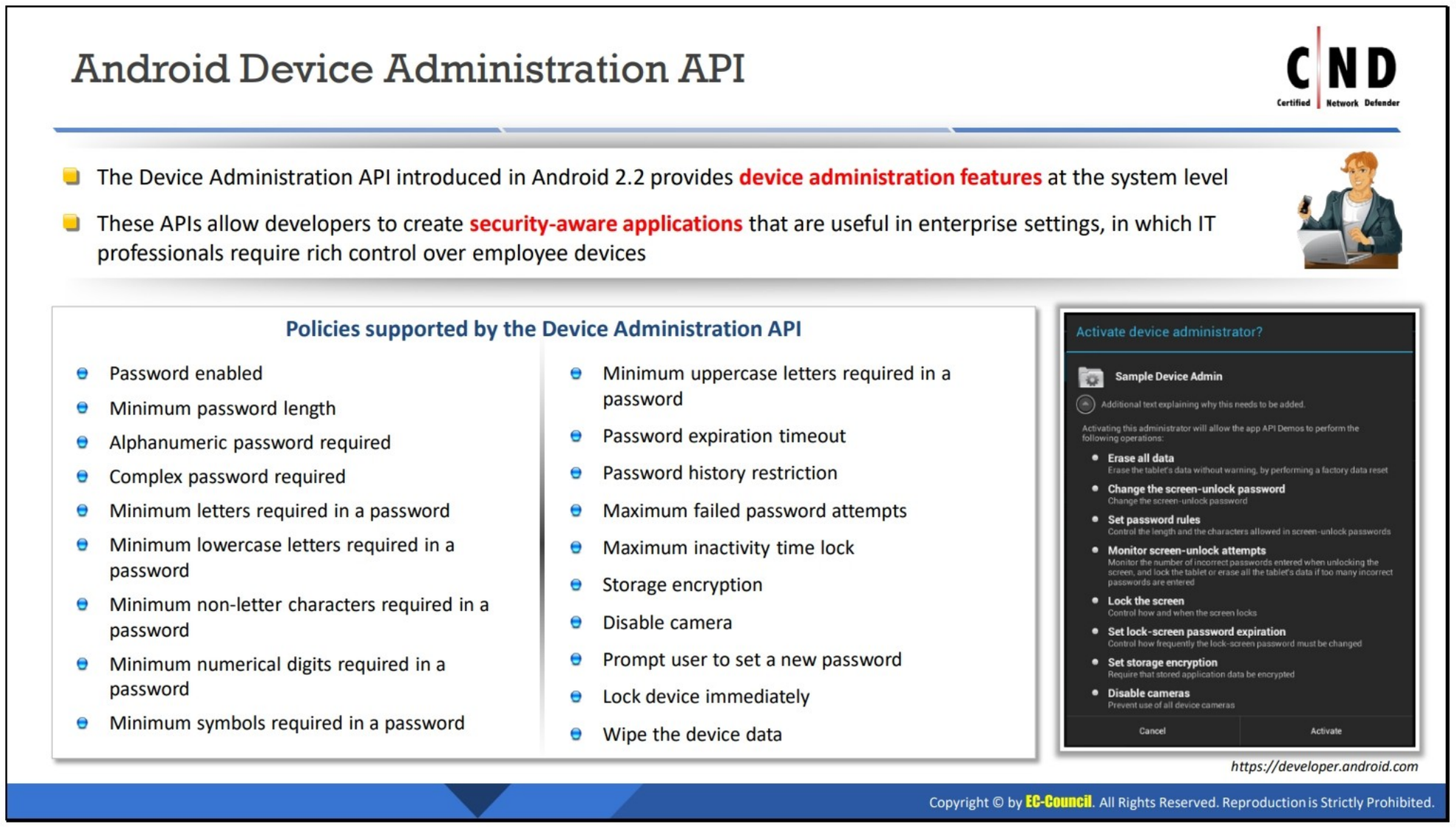
Below is a list of countermeasures to defend against SMS phishing attacks:

- Never reply to a suspicious SMS without verifying the source.
- Do not click on any links included in the SMS.
- Never reply to an SMS that requires personal and financial information from you.
- Review your bank's policy on sending SMS.
- Enable the "block texts from the internet" feature from your provider.
- Never reply to an SMS that urges you to act or respond quickly.
- Never call a number included in an SMS.
- Do not fall prey to scams, gifts, and offers that seem to be unexpected.
- Attackers might send text messages through an internet text relay service to conceal their identity; thus, it is best to avoid messages from nontelephonic numbers.
- Check for spelling mistakes, grammatical errors, or language inconsistency in text messages.



LO#05: Security Guidelines and Tools for Android Devices

Android devices have some built-in security features that should be enabled or configured properly. The objective of this section is to explain the security guidelines and tools used to secure Android devices.



Android Device Administration API

Source: https://developer.android.com

The Device Administration API introduced in Android 2.2 provides device administration features at the system level. These APIs allow developers to create security-aware applications that are useful in enterprise settings, in which IT professionals require rich control over employee devices. A device administration ("admin") API can be used to write device admin applications that can be installed by users on devices. The device admin applications enforce the desired policies.

Following are some examples of the types of applications that might use the device administration API:

- Email clients
- Security applications that perform remote wipe
- Device management services and applications

The following table lists the policies supported by the Android Device Administration API:

Policy	Description
Password enabled	Requires devices to ask for PIN or passwords
Minimum password length	Set the required number of characters for the password. For example, a PIN or password can be configured to have at least six characters.
Alphanumeric password required	Requires password to have a combination of letters and numbers and may include symbolic characters.

Complex password required	Requires passwords to contain at least a letter, numerical digit, and special symbol (introduced in Android 3.0).
Minimum letters required in a password	The minimum number of letters required in the password for all admins or a particular one 9(introduced in Android 3.0).
Minimum lowercase letters required in a password	The minimum number of lowercase letters required in the password for all admins or a particular one (introduced in Android 3.0).
Minimum nonletter characters required in a password	The minimum number of nonletter characters required in the password for all admins or a particular one (introduced in Android 3.0).
Minimum numerical digits required in a password	The minimum number of numerical digits required in the password for all admins or a particular one(introduced in Android 3.0).
Minimum symbols required in a password	The minimum number of symbols required in the password for all admins or a particular one (introduced in Android 3.0).
Minimum uppercase letters required in a password	The minimum number of uppercase letters required in the password for all admins or a particular one (introduced in Android 3.0).
Password expiration timeout	When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration timeout (introduced in Android 3.0).
Password history restriction	This policy prevents users from reusing the last *n* unique passwords. Typically, this policy can be used in conjunction with setPasswordExpirationTimeout(), which forces users to update their passwords after a specified amount of time has elapsed(introduced in Android 3.0).
Maximum failed password attempts	Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.
Maximum inactivity time lock	Sets the time elapsed since the user last touched the screen or pressed a button before the device locks its screen. When this happens, users must re-enter their PIN or passwords before they can use their devices and access data. This value can be between 1 and 60 min.
Require storage encryption	Specifies if a device supports storage encryption (introduced in Android 3.0).

Disable camera	Specifies the camera-disabling feature. Note that this does not have to imply permanent disabling. The camera can be enabled/disabled dynamically based on the context or time (introduced in Android 4.0).

Table 7.1: List of Policies Supported by the Android Device Administration API

In addition to supporting the aforementioned policies, the device administration API enables the following:

- Prompt user to set a new password
- Lock device immediately
- Wipe the device data (i.e., restore the device to its factory defaults)

Following is an example of an Android Device Administrator page in an Android device:

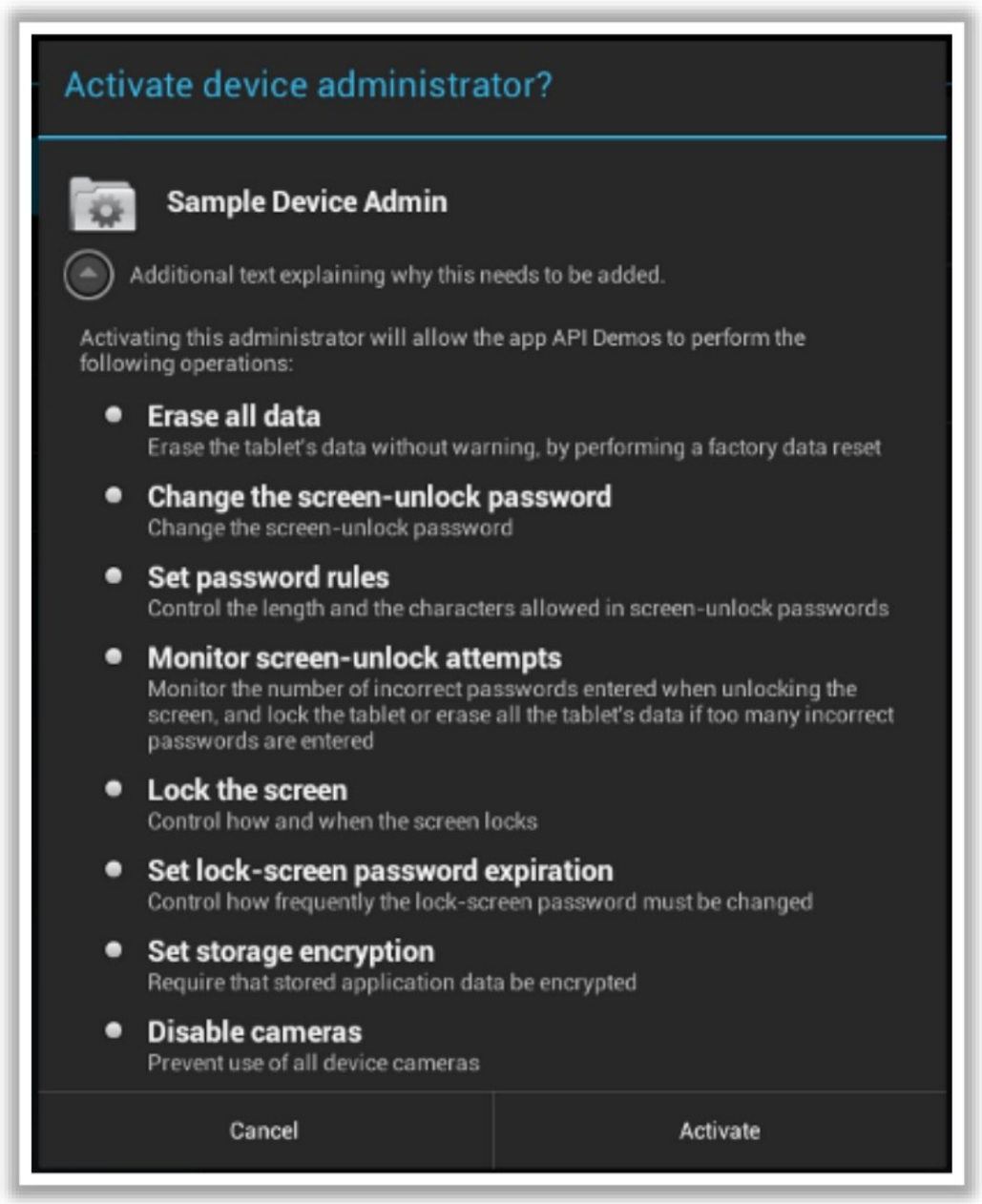
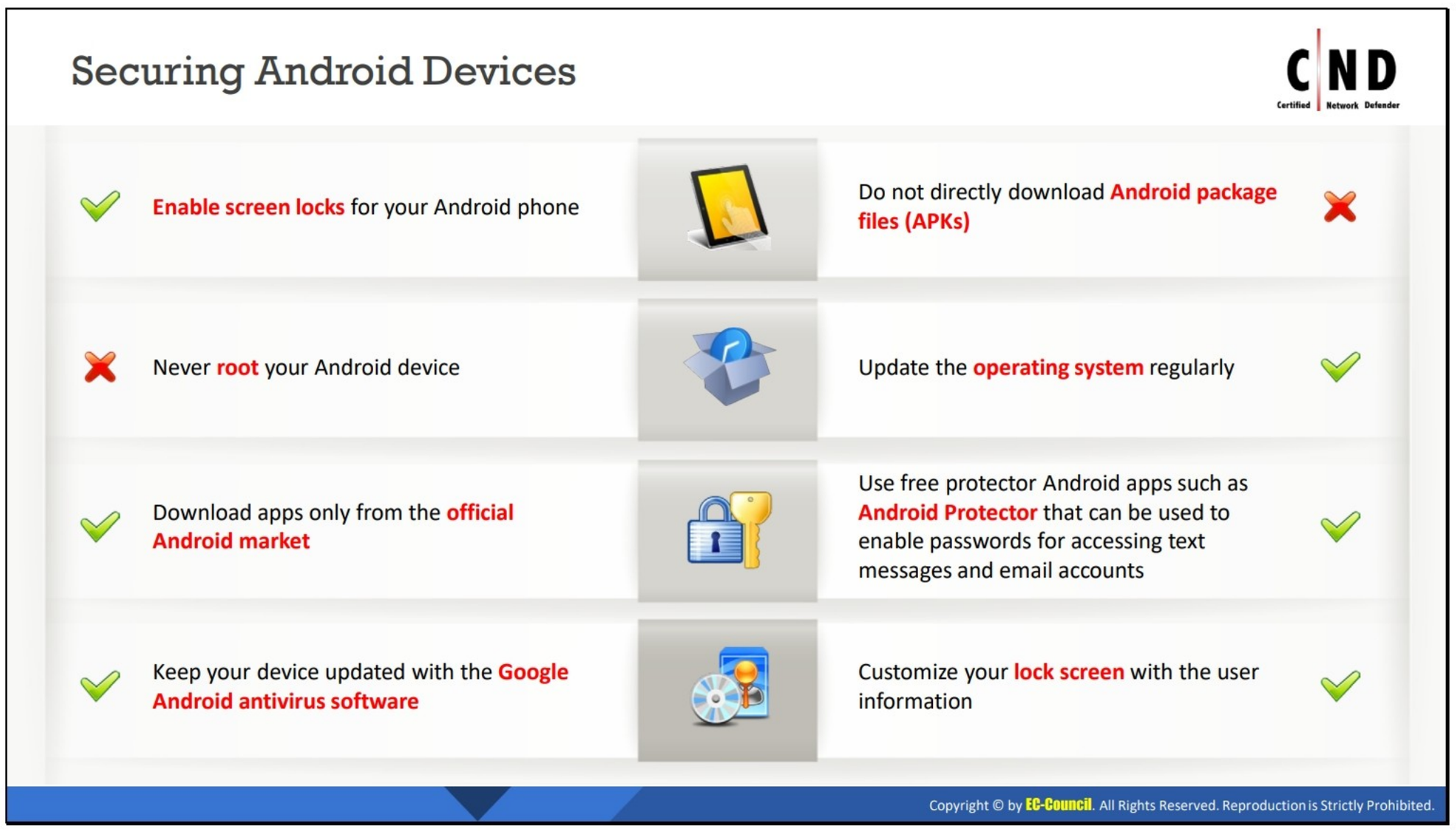


Figure 7.2: Screenshot of Android Device Administrator



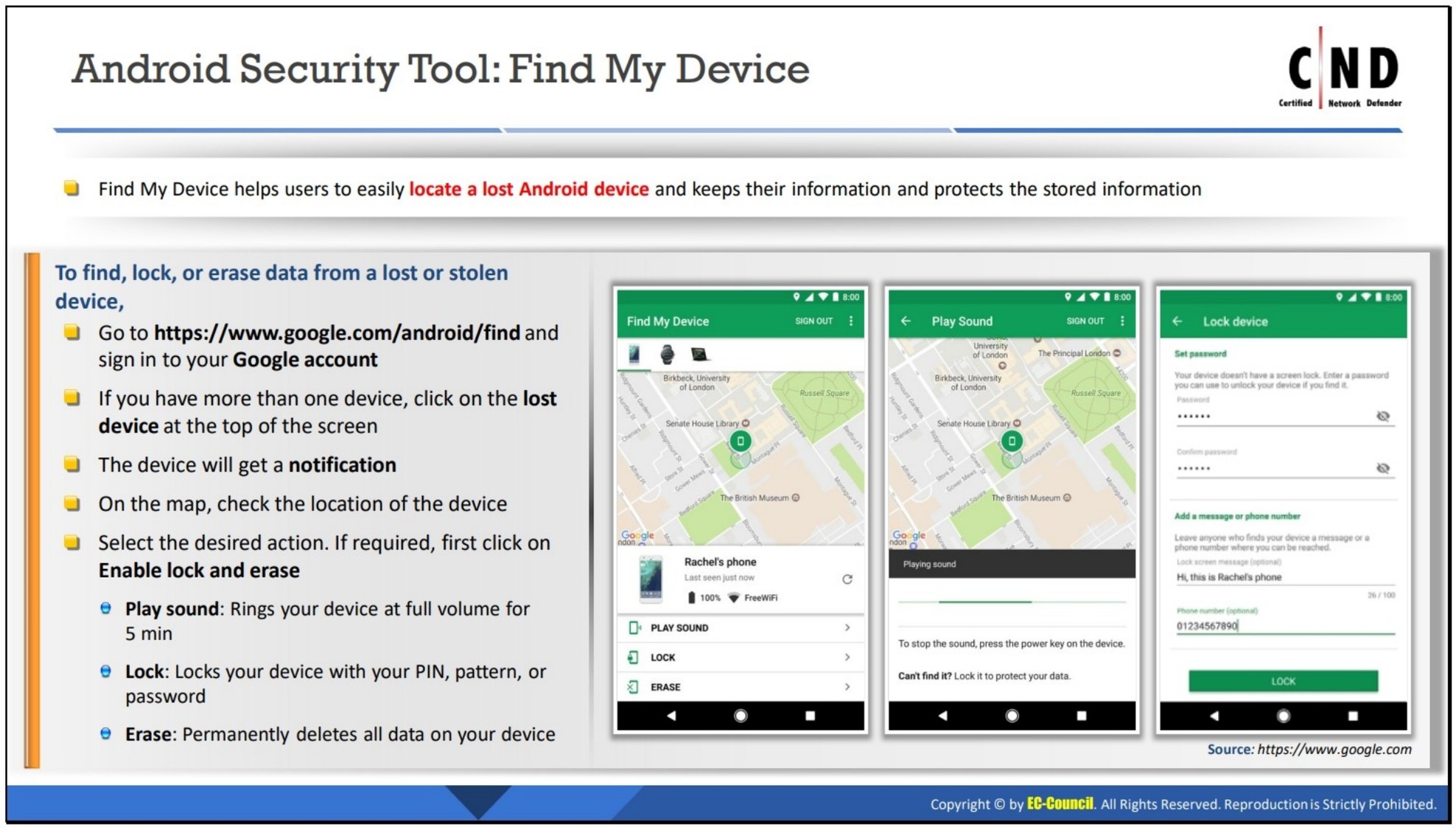
Securing Android Devices

Security in Android devices is a major concern because they are widely attacked. Given below are some of the countermeasures that can help in securing Android devices and their data from malicious users:

- Enable screen locks on Android phones for increased security
- Never root an Android device
- Download apps only from the official Android market
- Keep the device updated with the Google Android antivirus software
- Do not directly download Android package files (APKs)
- Update the OS regularly
- Use free protector Android apps such as Android Protector that can be used to enable passwords for accessing text messages and email accounts
- Customize the lock screen with the user information
- Enable encryption in Android devices to enhance their security
- Use apps such as AppLock to lock apps that contain private information
- Before installing an app from Google Play, read the required permissions and ensure that it corresponds to the app functionalities; additionally, browse through the ratings and reviews of the app.
- Create multiple accounts if an Android device must be shared between multiple users to ensure privacy.

- Enable GPS on Android devices so that they can be tracked when lost or stolen.
- Use third-party applications such as Lookout Mobile Security, 3CX Mobile Device Manager, or SeekDroid AntiTheft to remotely erase the confidential data when the Android device is lost or stolen.
- Turn off the following features:
  - **Visible passwords**- prevents displaying passwords on screen
  - **Use secure credentials**- prevents applications from accessing secure certificates and credentials
  - **Wi-Fi**- to ensure that a device does not accidentally get connected to a wireless network

Note: The aforementioned features can be found in **Settings → Connections** or **Settings → More → Security** on most Android devices.



Android Security Tool: Find My Device

Android Security Tools

- **Find My Device**

  Source: https://www.google.com

  Find My Device helps users to easily locate their lost Android device and protects the stored information. It allows users 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 the data on the lost Android device.

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

  To use Find My Device, the 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 its location enabled
  - Have Find My Device turned on

  To find, lock, or erase the data of 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 on the lost device at the top of the screen.
- The device will get a notification.
- On the map, check the location of the device.
  - The location is approximate and might not be accurate.
  - If the device cannot be found, then its last known location can be obtained, if available.

- Select the desired action. If needed, first click on **Enable lock and erase**.
  - **Play sound**: Rings the device at full volume for 5 min even if it is set to silent or vibrate.
  - **Lock**: Locks the device with its PIN, pattern, or password. If there are no locks on the device, you can set one. To help someone return your device to you, you can add a message or phone number to the lock screen.
  - **Erase**: Permanently deletes all data on your device (but might not delete the SD card content). After this step, Find My Device will not work on the device.

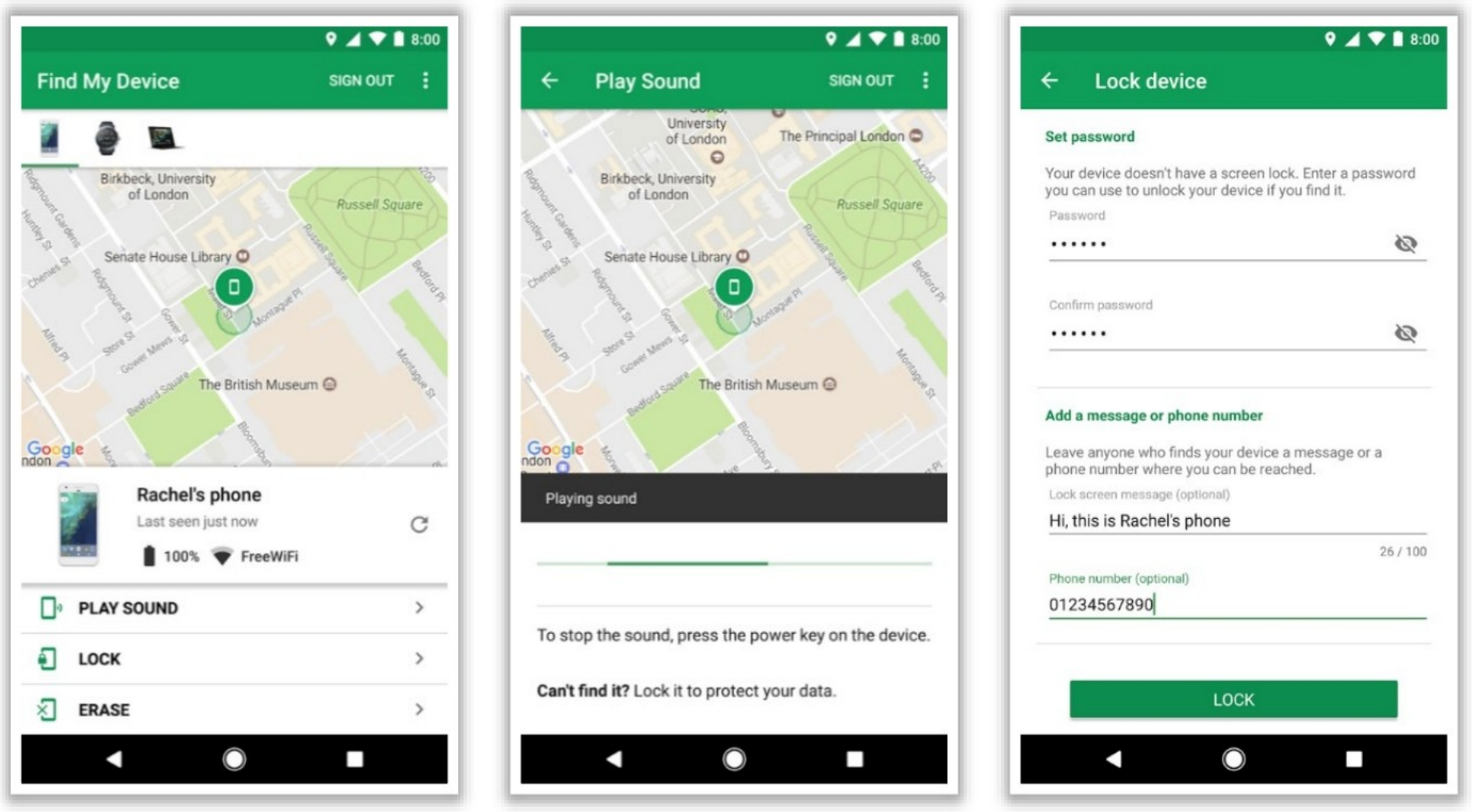
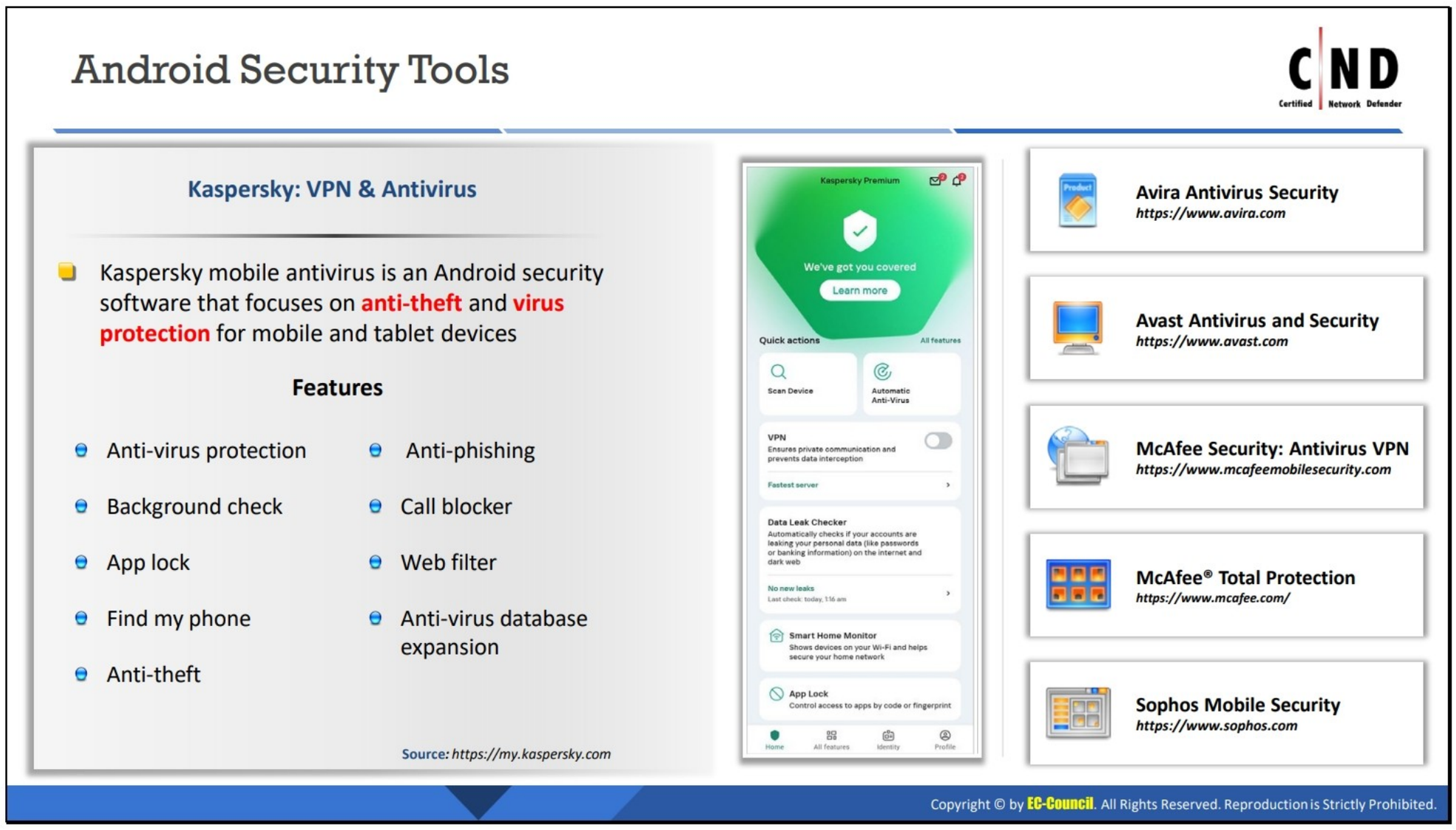


Figure 7.3: Screenshot of Find My Device service



Android Security Tools

- **Kaspersky: VPN & Antivirus**

  Source: https://my.kaspersky.com

  Kaspersky: VPN & Antivirus mobile antivirus is an Android security app that focuses on anti-theft and virus protection for mobile and tablet devices. It is designed to help users find their device, step-by-step, if it is lost or stolen. It also protects the device against virus or malware attacks.

  Features:

  - **Antivirus protection**- Acts as a virus cleaner and automatically blocks malware from phones and tablets.
  - **Background check**- Scans for viruses, spyware, and trojans.
  - **App lock**- Allows users to add a secret code to access their private messages or photos, among others.
  - **Find my phone**- Tracks and finds an Android phone or tablet if it is lost or stolen.
  - **Anti-theft**- Protects vulnerable personal information from prying eyes.
  - **Anti-phishing-** Keeps the financial information secure while shopping and banking online.
  - **Call blocker**- Blacklists unwanted phone calls and text/spam messages.
  - **Web filter**- Filters dangerous links and sites while surfing the internet.
  - **Android 8 Support**- This allows users to maximize the protection of their device.

- **Antivirus database expansion**- To improve protection against sophisticated threats.

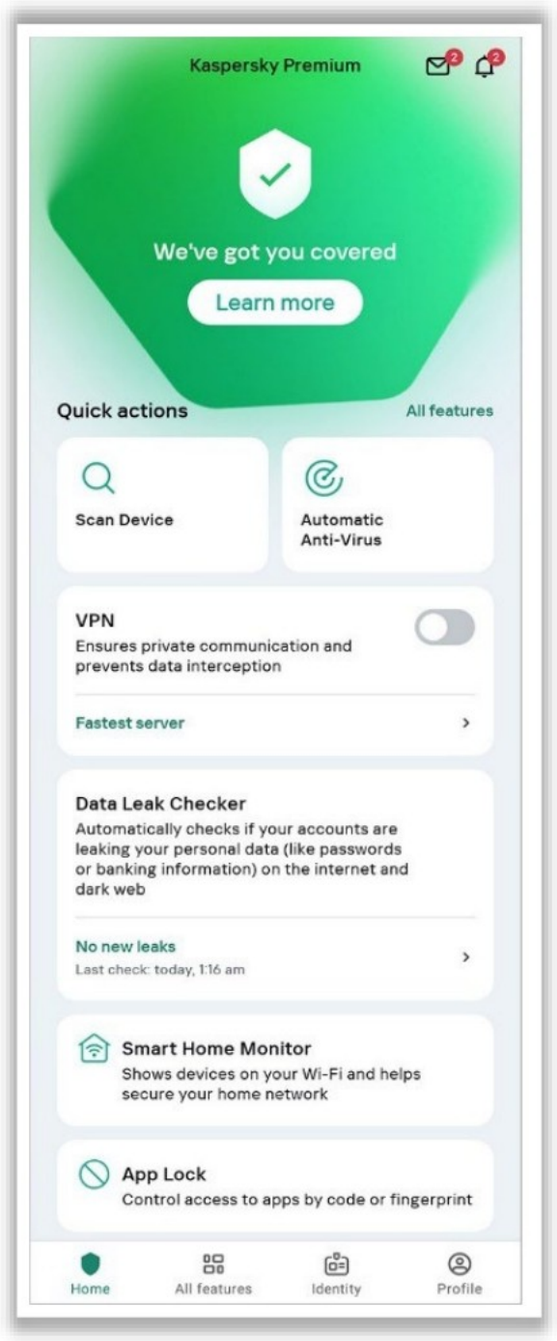
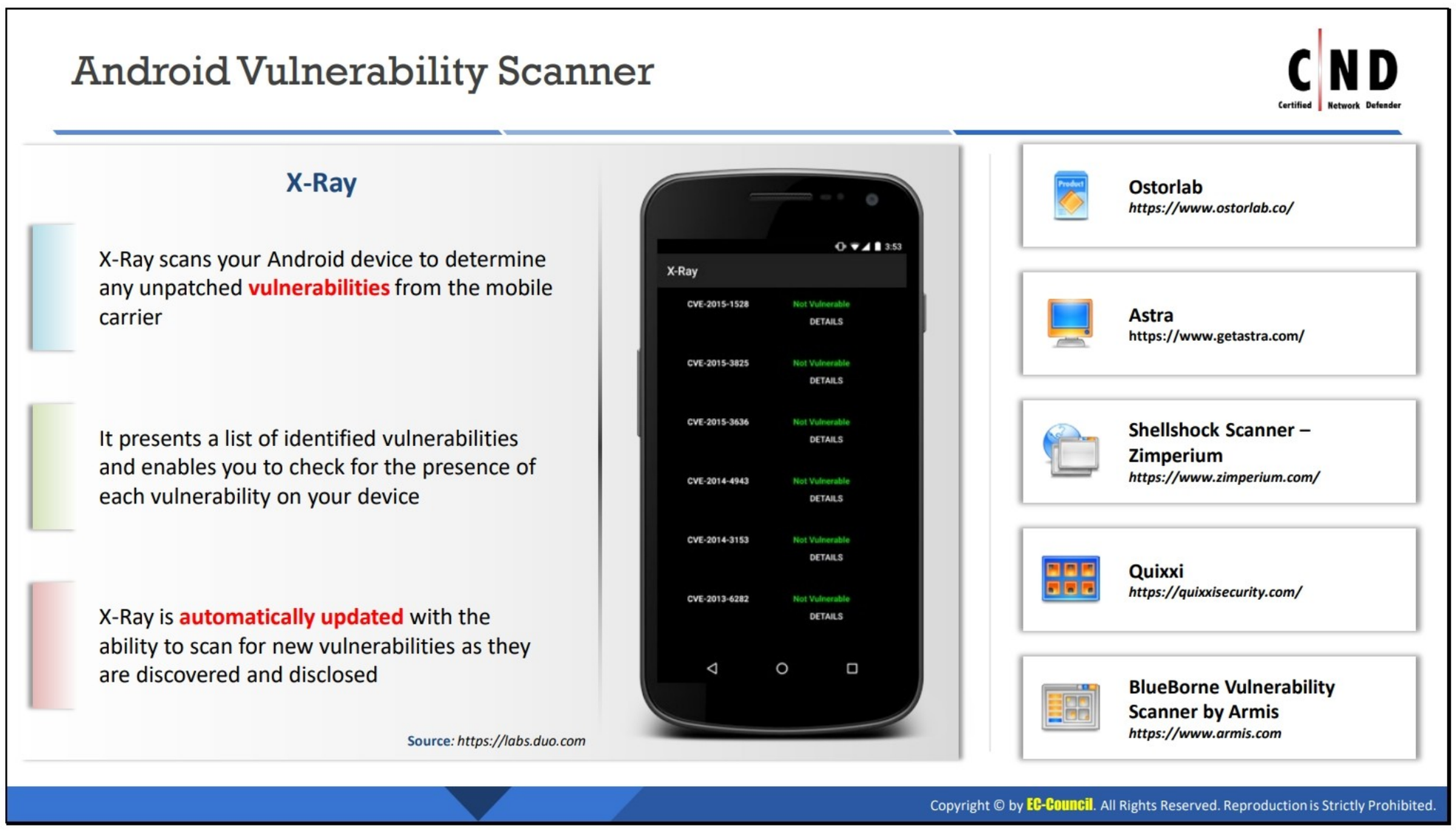


Figure 7.4: Screenshot of Kaspersky Mobile Antivirus

Following are some additional Android security tools:

- Avira Antivirus Security (https://www.avira.com)
- Avast Antivirus (https://www.avast.com)
- McAfee Security: Antivirus VPN (https://www.mcafeemobilesecurity.com)
- McAfee® Total Protection (https://www.mcafee.com)
- Sophos Mobile Security (https://www.sophos.com)
- Malwarebytes for Android (https://www.malwarebytes.com)
- AVG AntiVirus 2020 for Android Security Free (https://www.avg.com)
- Safe Security - Antivirus, Booster, Phone Cleaner (http://www.safesecurityapps.com/)
- Trend Micro Mobile Security and Antivirus (https://www.trendmicro.co.in)
- BullGuard Mobile Security and Antivirus (https://www.bullguard.com)



Android Vulnerability Scanner

- **X-Ray**

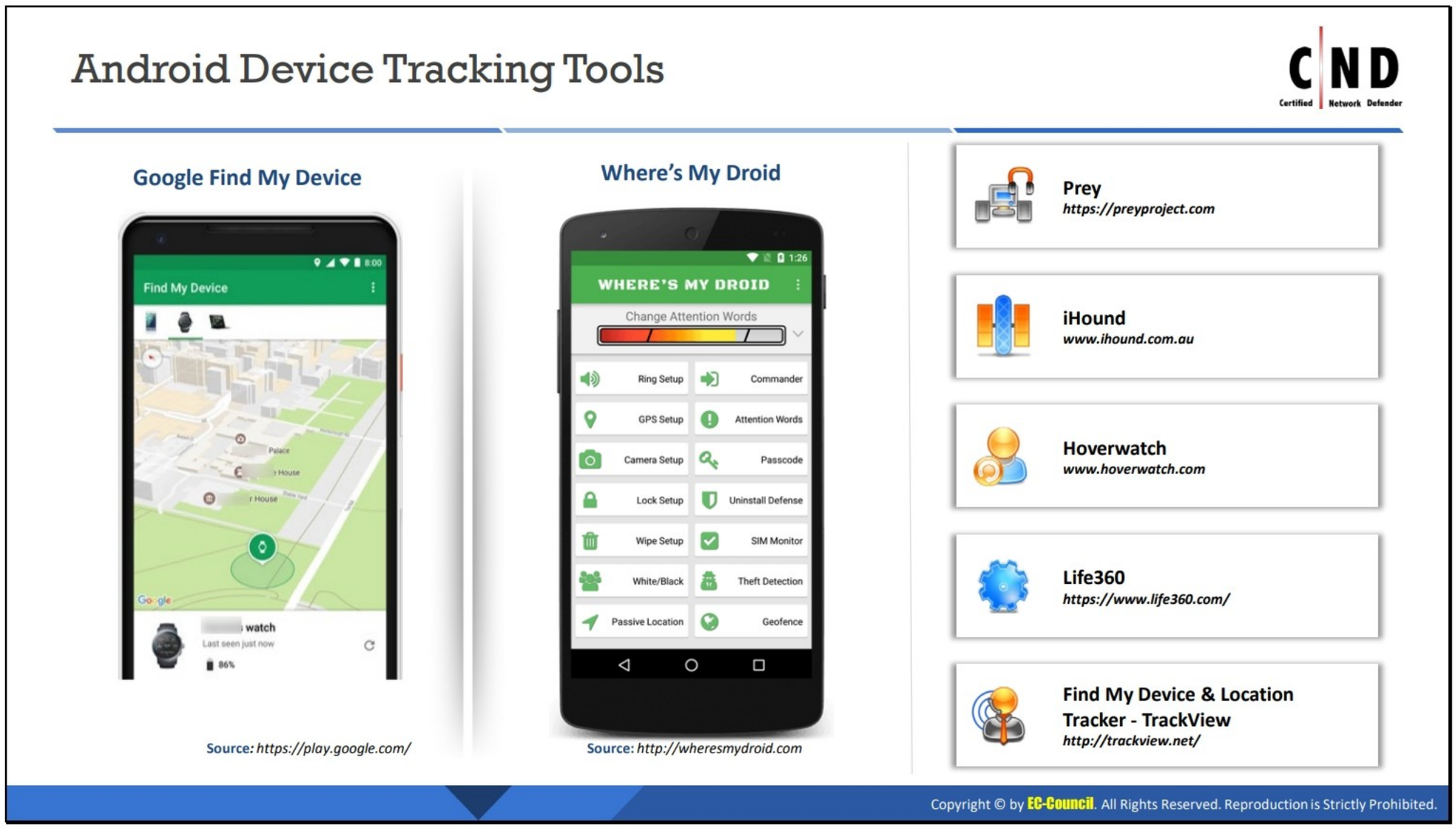
  Source: https://labs.duo.com

  X-Ray enables users to scan their Android device for security vulnerabilities that may expose it to risks. It scans to determine the presence of vulnerabilities that remain unpatched by your carrier. It presents a list of identified vulnerabilities and allows users to check for each vulnerability in their device. X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered and disclosed.

Figure 7.5: Screenshot of X-Ray Android Vulnerability Scanner

Following are some additional android vulnerability scanners:

- Threat Scan (http://free.kaspersky.com)
- Astra (https://www.getastra.com/)
- Shellshock Scanner – Zimperium (https://www.zimperium.com)
- Quixxi - https://quixxisecurity.com/
- BlueBorne Vulnerability Scanner by Armis (https://www.armis.com)
- EternalBlue Vulnerability Scanner (https://ebvscanner.firebaseapp.com)



Android Device Tracking Tools

Android device tracking tools help users to track and find the location of an Android device if it is lost or stolen. Below is a list of the widely used Android device tracking tools.

- **Google Find My Device**

  Source: https://play.google.com/

  Google Find My Device is an anti-theft device recovery app for Android that helps users to find their lost or stolen mobile phone or tablet.

  Features:

  - If your phone is lost, send a text message to it and Find My Device will reply to you with its current address and a Google Maps link to its location.
  - After sending a text message, it makes a device ring at the maximum volume (even if it is on silent) to manually locate it.
  - Helps in determining the remaining battery.
  - Notifies the owner if someone changes the device SIM card
  - Remotely erases the phone data

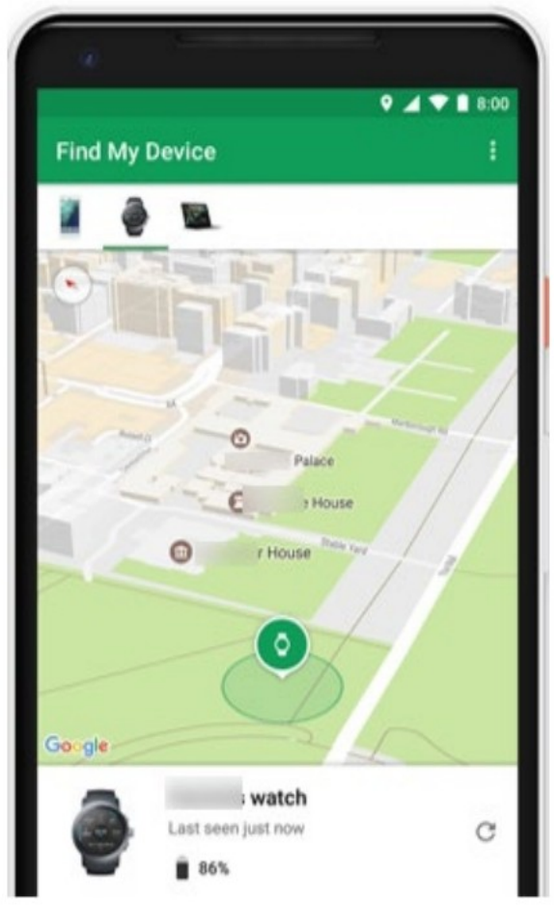


Figure 7.6: Screenshot of Find My Phone

- **Where's My Droid**

  Source: http://wheresmydroid.com

  Where's My Droid is an Android device tracking tool that allows users to track their phone from anywhere with a text message attention word or through the online control center known as Commander.

  Features:

  - Finds the phone by making it ring/vibrate
  - Finds the phone using the GPS location
  - GPS Flare—Location alert on low battery
  - Passcode protection to prevent unauthorized app changes
  - Notification of changed SIM card or phone number
  - Stealth mode hides the incoming texts with attention word

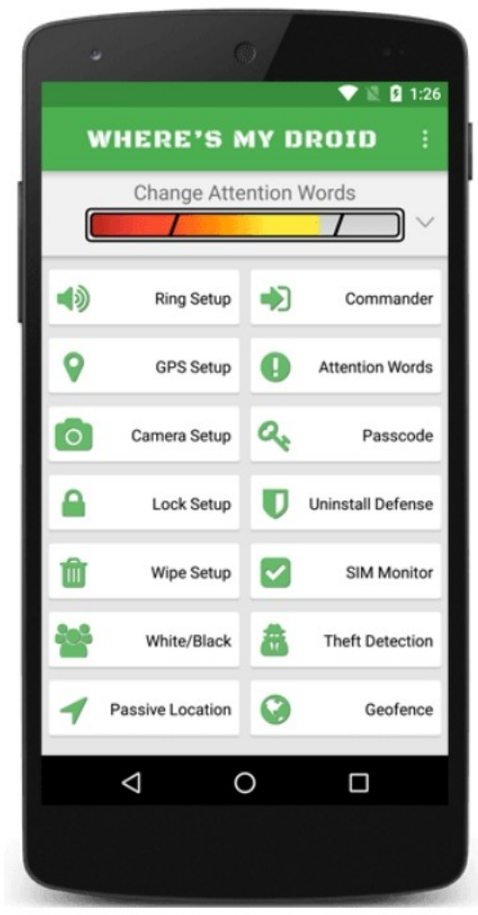
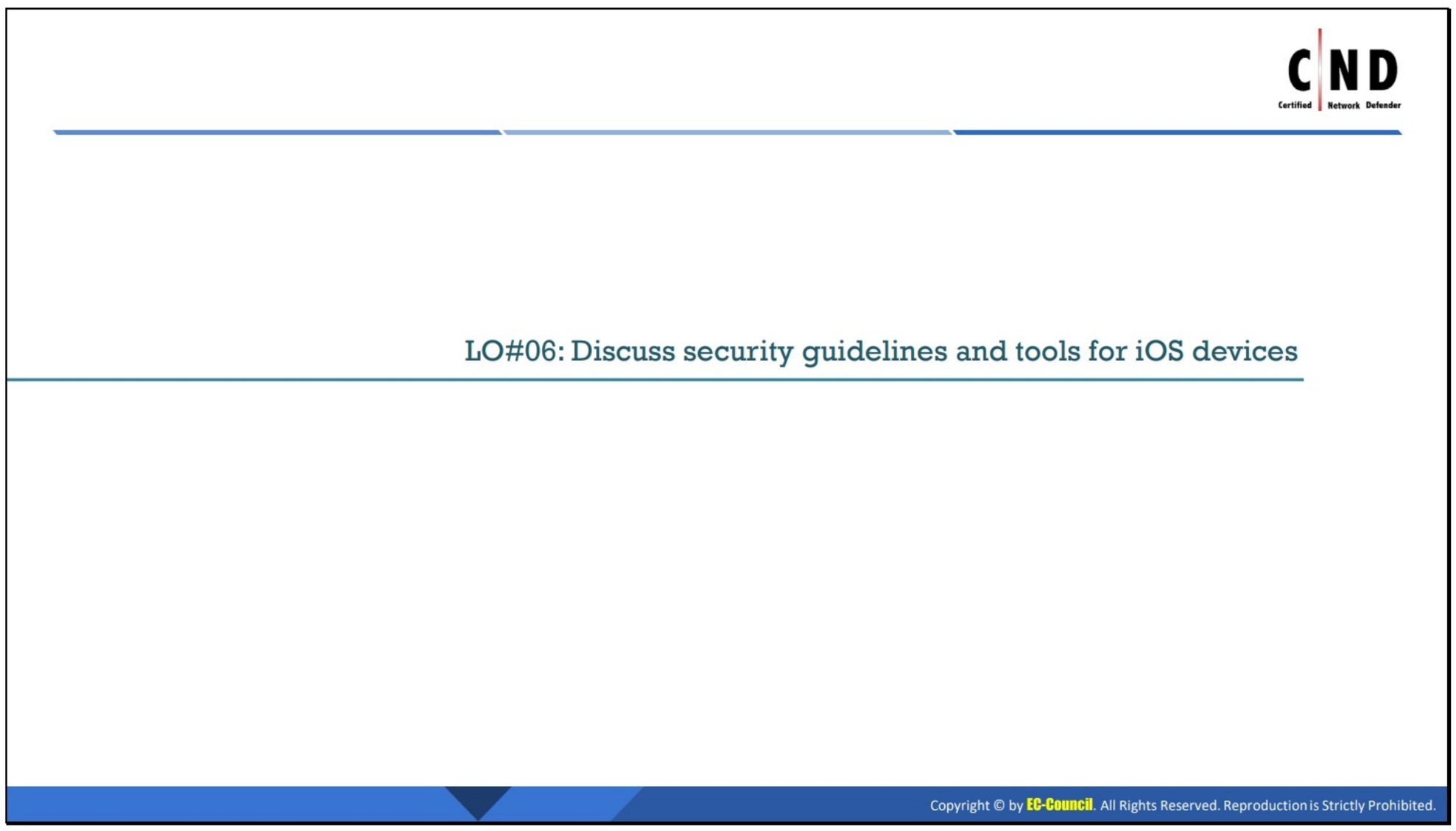


Figure 7.7: Screenshot of Where's My Droid

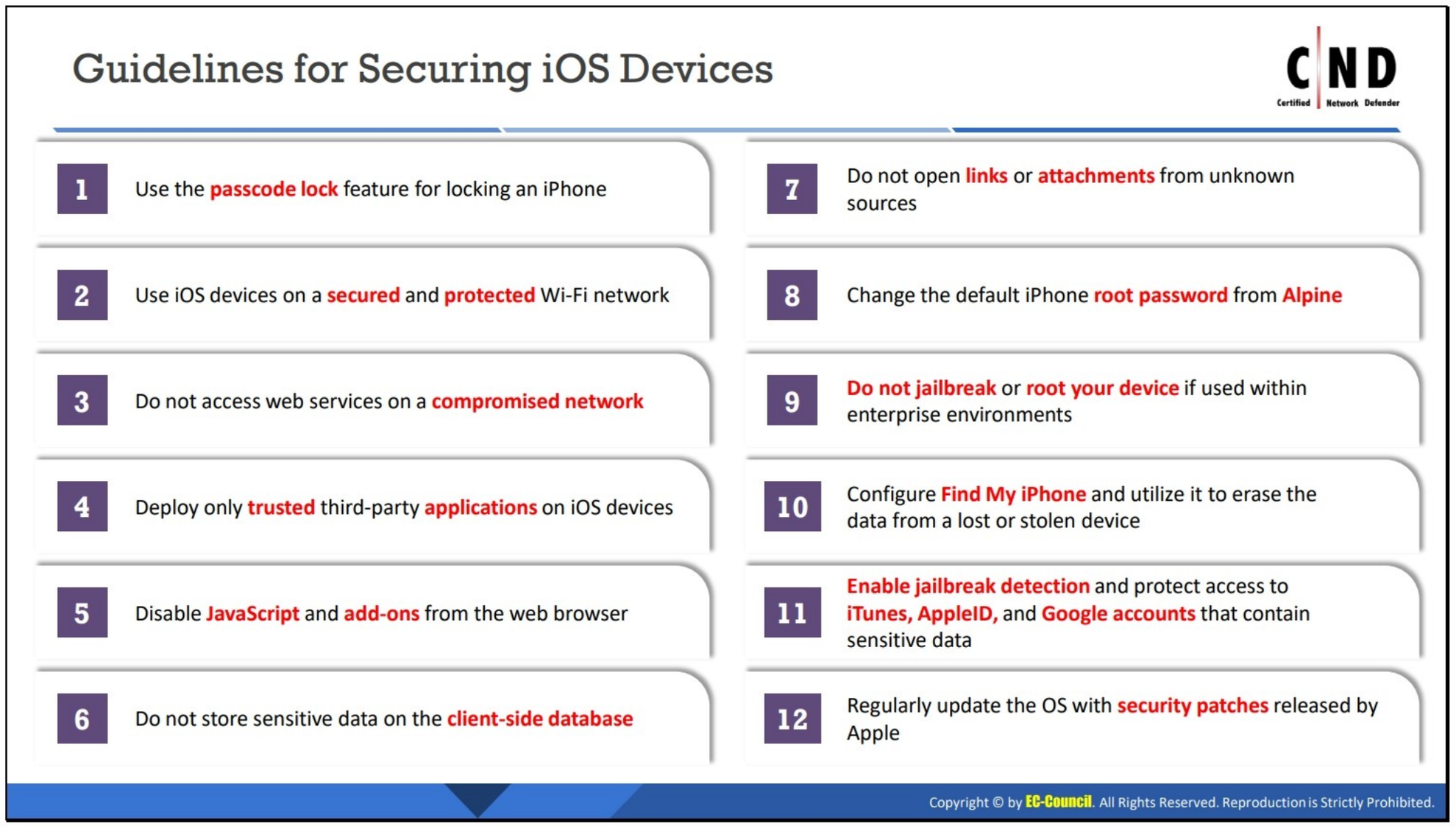
Following are some additional Android device tracking tools:

- Prey (https://preyproject.com)
- iHound (http://ihoundgps.com)
- Hoverwatch - www.hoverwatch.com
- Life360 - https://www.life360.com/
- GadgetTrak Mobile Security (http://www.gadgettrak.com)
- Find My Device and Location Tracker - TrackView - http://trackview.net/
- Lost Android (http://www.androidlost.com)



LO#06: Security Guidelines and Tools for iOS Devices

iOS devices have some built-in security features that should be enabled or appropriately configured. The objective of this section is to explain the security guidelines and tools used to secure iOS devices.



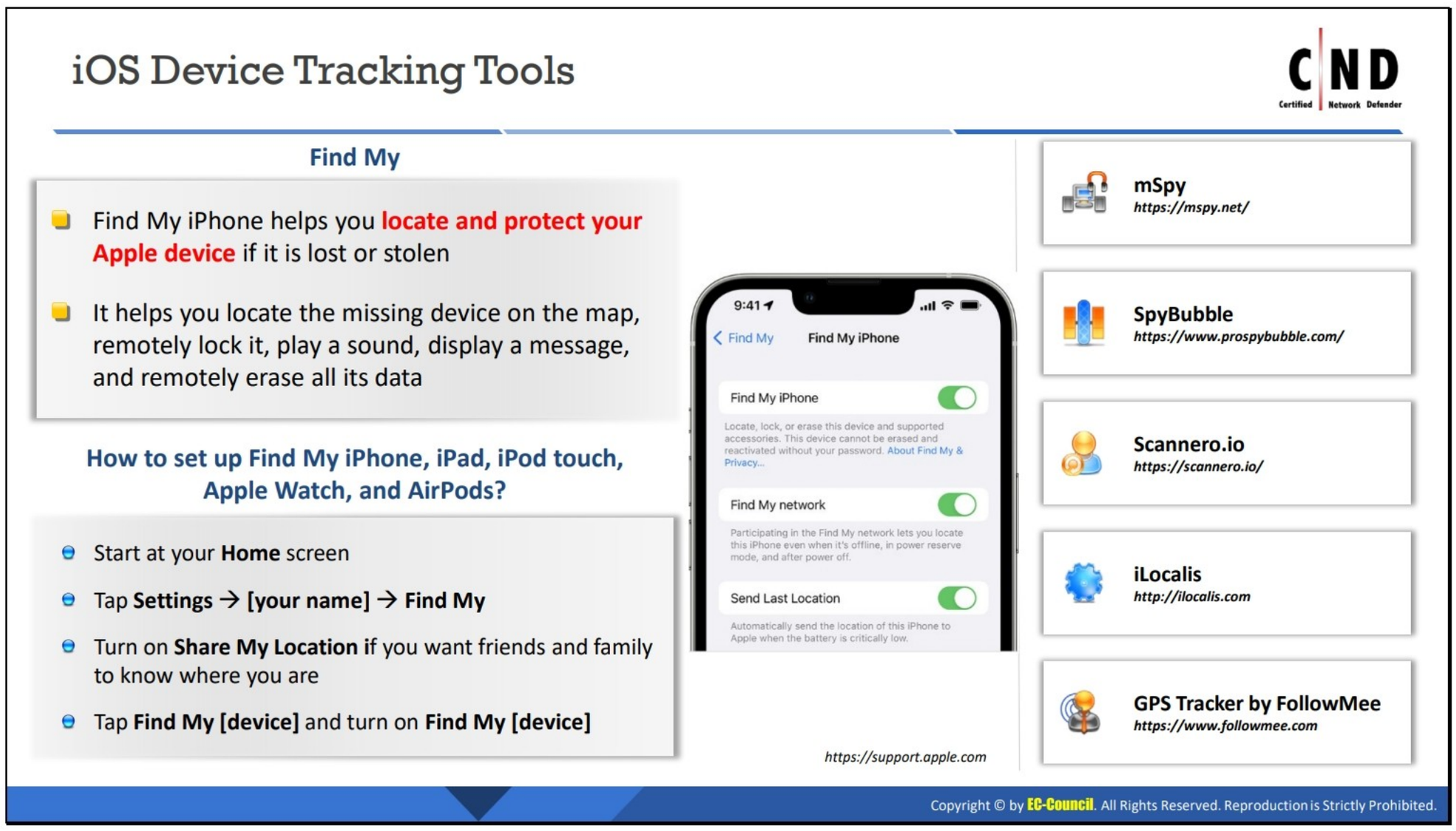
Guidelines for Securing iOS Devices

Listed below are some guidelines that help in securing iOS devices and their data from attackers:

- Enable the **Passcode Lock** feature on the iPhone. Go to **Settings → Touch ID and Passcode Lock**, and then tap **Turn Passcode On.**
- Set separate passcodes for applications containing sensitive data.
- Disable JavaScript and add-ons from the web browser.
- Always download applications from the **Apple App Store.**
- Set **Auto-Lock Timeout** to enter a passcode after a set time. Go to **Settings → General → Auto-Lock.**
- Use iOS devices on a secured and protected Wi-Fi network.
- Do not store sensitive data on the client-side database.
- Do not access web services on a compromised network.
- Do not open links or attachments from unknown sources.
- Deploy only trusted third-party applications on iOS devices.
- Change the default iPhone root password from Alpine.
- Do not jailbreak or root a device if used within enterprise environments.
- Configure Find My iPhone and utilize it to wipe a lost or stolen device.
- Enable jailbreak detection and protect access to iTunes, AppleID, and Google accounts that contain sensitive data.

- Disable iCloud services so that sensitive enterprise data are not backed up to the cloud (note that cloud services can backup documents, account information, settings, and messages).
- Enable the **Ask to Join Networks** function; this prevents a device from randomly connecting to the available Wi-Fi networks. Go to **Settings → Wi-Fi → Ask to Join Networks.**
- Regularly update the device OS with the security patches released by Apple. To receive updates, connect to iTunes. For iOS5 and above, updates can be received via **Settings → General → Software Updates.**
- Enable the **Erase Data** feature on iPhone to erase all data and settings after specified failed attempts (for example 10) to unlock the device. Go to **Settings → Touch ID and Passcode → Erase Data.**
- Disable the **Voice Dial** feature on the iPhone to prevent attackers from accessing it without entering a passcode. Go to **Settings → Touch ID and Passcode**, and then **Turn Voice Dial** to **OFF.**
- Delete the **Keyboard Cache** on the iPhone to remove all recorded keystrokes. Go to **General → Reset**, tap on **Reset Keyboard Dictionary**, and then **Confirm** on the warning screen.
- Disable **Geotagging** (storage of location-based data in images) on the iPhone. Go to **Settings → Privacy → Location Services**, and then toggle the **Camera** to **OFF.**
- Enable **Safari's Privacy and Security Settings** on the iPhone. Go to **Settings → Safari**. Here, users can block pop-ups, disable passwords and AutoFill, enable fraudulent website warning, block cookies, clear history and website data, etc.
- Enable the **Do Not Track** feature to keep web browsing information private. Go to **Settings → Safari →** and enable the **Do Not Track** option.
- Disable Bluetooth when not in use. Go to **Settings → Bluetooth**, and then toggle it to **OFF.**
- Disable Wi-Fi when not in use. Go to **Settings → Wi-Fi**, and then toggle it to **OFF.**

Note: The aforementioned paths for enabling/disabling respective features may change based on the iOS version or device used.



iOS Device Tracking Tools

Given below is a list of few iOS device tracking tools:

- **Find My**

  Source: https://support.apple.com

  Find My iPhone device tracking tool allows users to use another iOS device to track a lost or misplaced mobile, iPhone, iPad, iPod touch, or Mac and protects its data. To use this app, it must be installed on another iOS device and signed in with the Apple ID of the lost device. It helps in locating the missing device on the map, remotely lock it, play a sound, display a message, and erase all data.

  If the missing iDevice operates on iOS 6 or later versions, then Find My iPhone also includes a Lost Mode; it locks the missing device with a passcode and displays a custom message such as a contact phone number on the lock screen. In the Lost Mode, the whereabouts of the device are also tracked so that its recent location history can be viewed from the Find My iPhone app.

  How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods?

  1. Start at your **Home** screen.
  2. Tap **Settings → [your name] → iCloud**. If you are using iOS 10.2 or earlier versions, go to **Settings → iCloud.**
  3. Scroll to the bottom and tap on **Find My iPhone.**
  4. Slide to turn on **Find My iPhone** and **Send Last Location.**

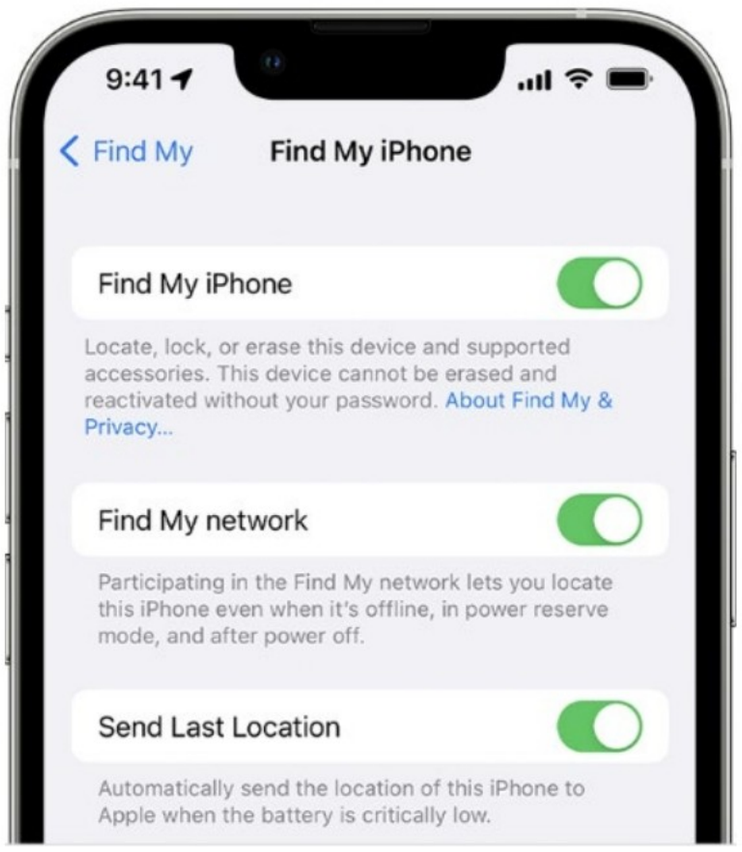
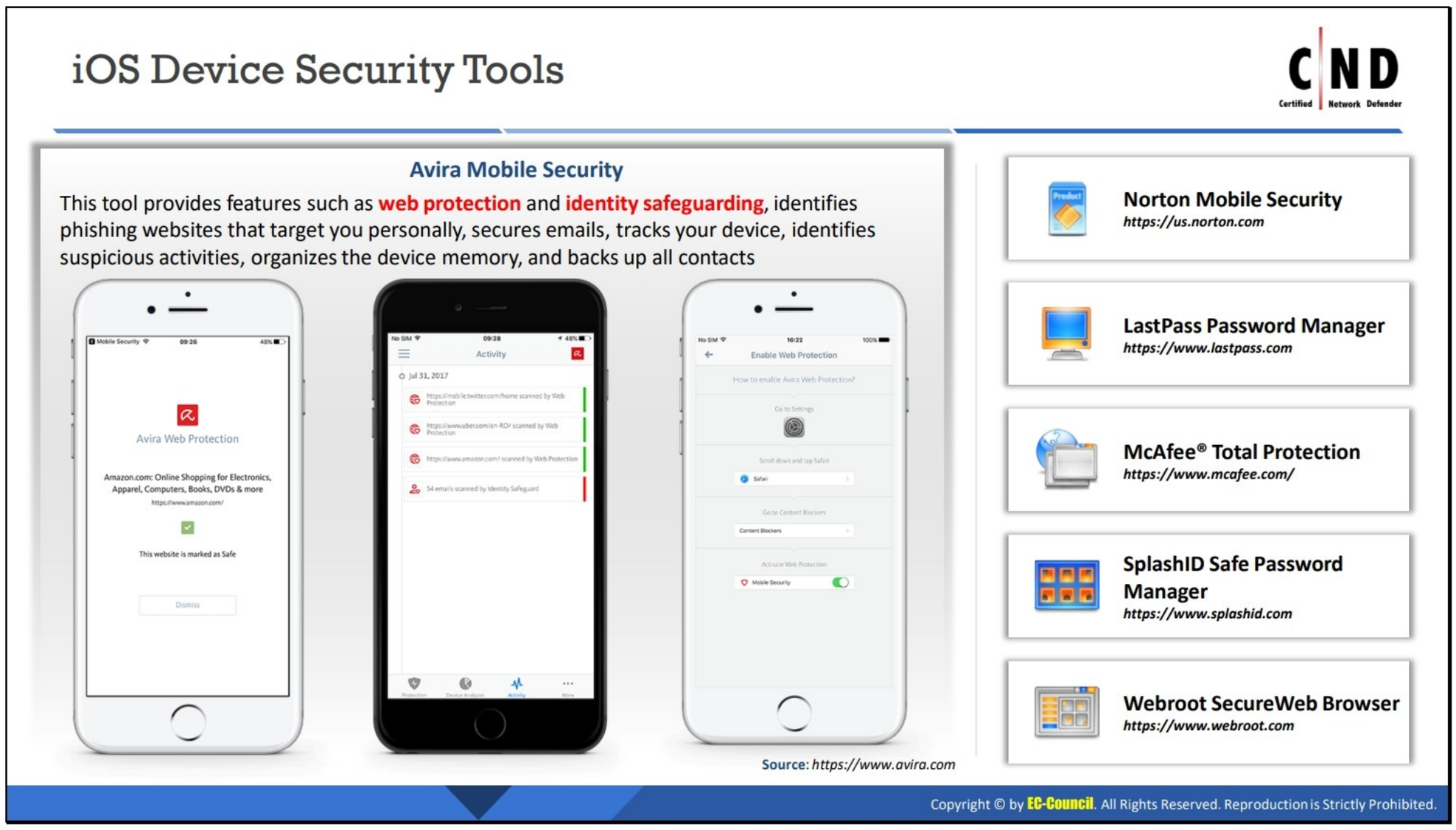


Figure 7.8: Screenshot of Find My iPhone

Following are some additional iOS device tracking tools:

- mSpy (https://mspy.com)
- SpyBubble (https://www.prospybubble.com/)
- Scennario.io – (https://scennario.net/)
- iLocalis (http://ilocalis.com)
- GPS Tracker by FollowMee (https://www.followmee.com)
- iHound (https://apps.apple.com/)



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.

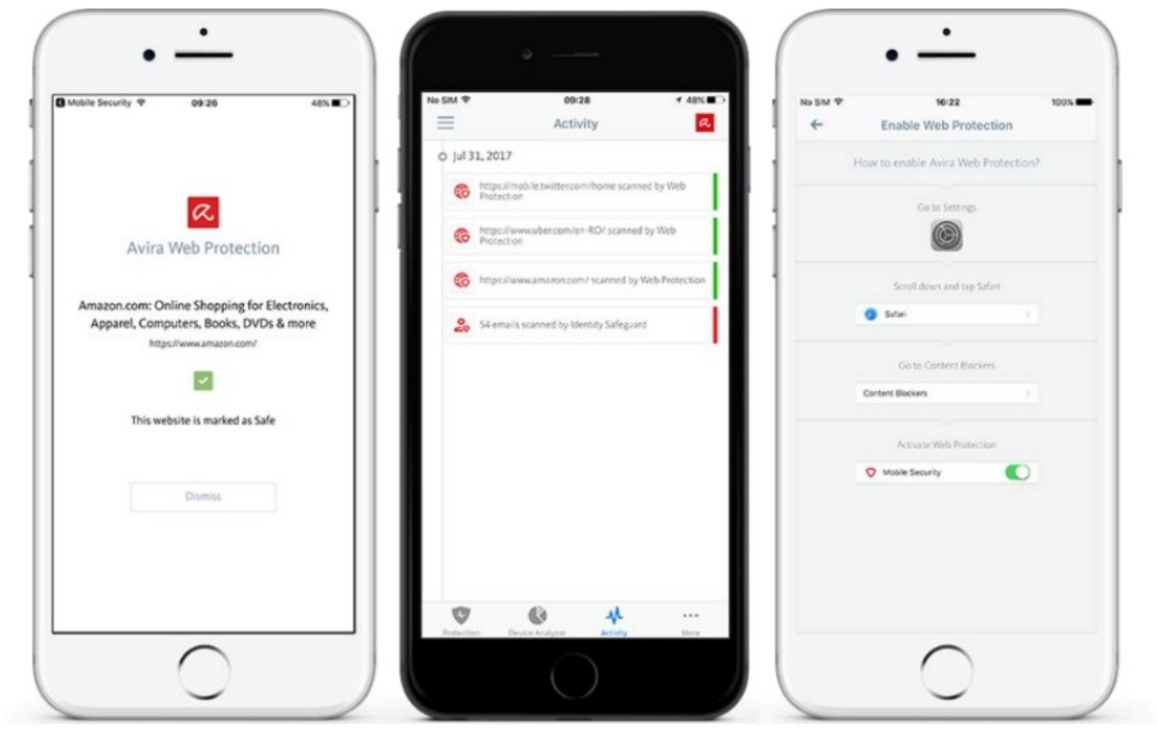
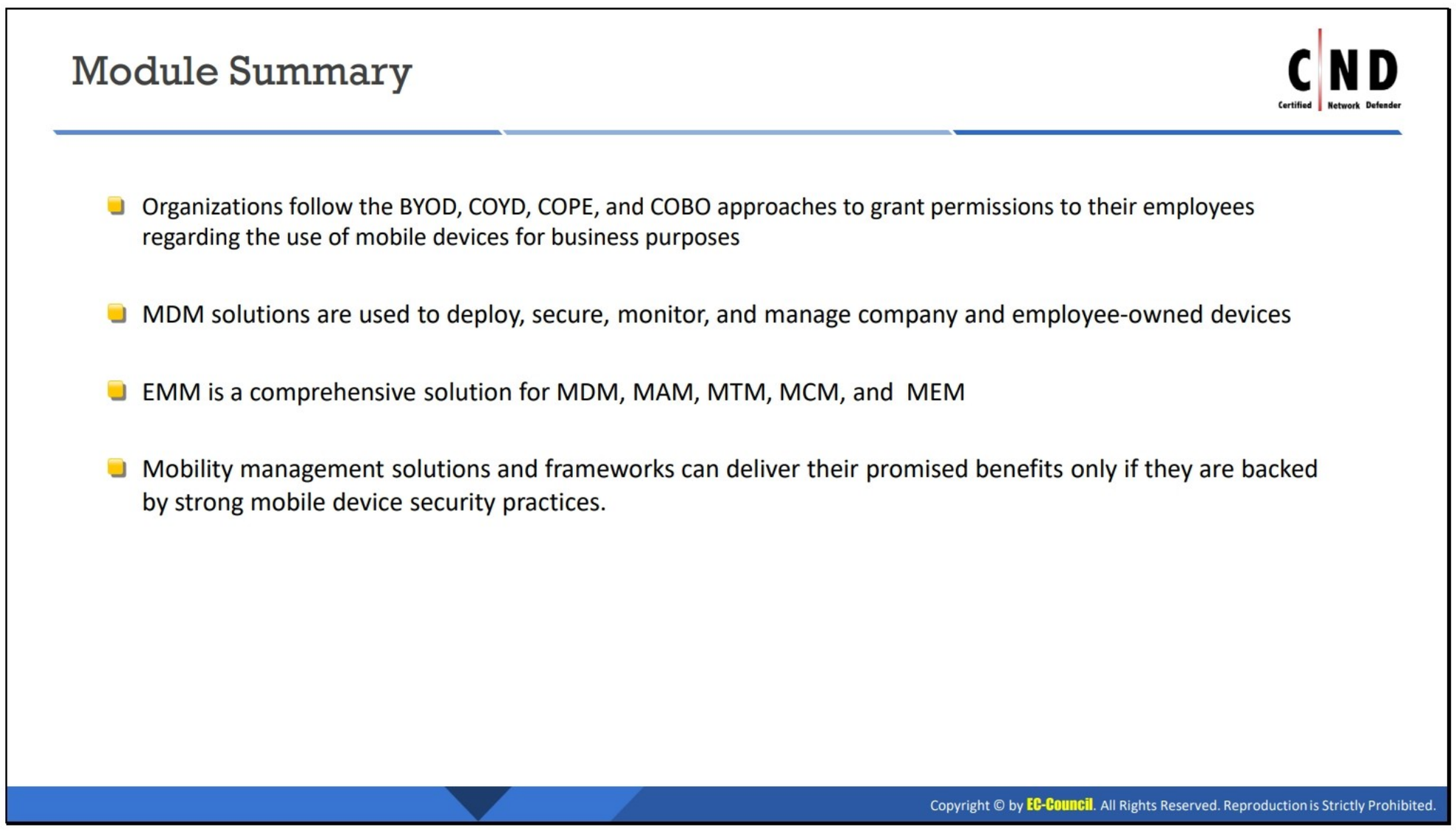


Figure 7.9: Screenshots of Avira Mobile Security

Following are some additional iOS device security tools:

- Norton Mobile Security (https://us.norton.com)
- LastPass Password Manager (https://www.lastpass.com)

- McAfee® Total Protection (https://www.mcafee.com)
- SplashID Safe Password Manager (https://www.splashid.com)
- Webroot SecureWeb Browser (https://www.webroot.com)
- Wickr Me - Private Messenger (https://www.wickr.com)
- 1Password (https://1password.com)
- GadgetTrak (http://www.gadgettrak.com)
- iLocalis (http://ilocalis.com)
- GPS Tracker by FollowMee (https://www.followmee.com)



Module Summary

This module described mobile security at the enterprise level. This module also identified the security risks and challenges associated with enterprise mobile usage policies. The key points highlighted in this module are:

- Organizations follow the BYOD, COYD, COPE, and COBO approaches to grant permissions to their employees to use mobile devices for business purposes.
- MDM solutions are used to deploy, secure, monitor, and manage company and employee-owned devices.
- EMM is a comprehensive solution for MDM, MAM, MTM, MCM, and MEM.
- Mobility management solutions and frameworks can only deliver their promised benefits if they are supported by strong mobile device security practices.

This page is intentionally left blank.