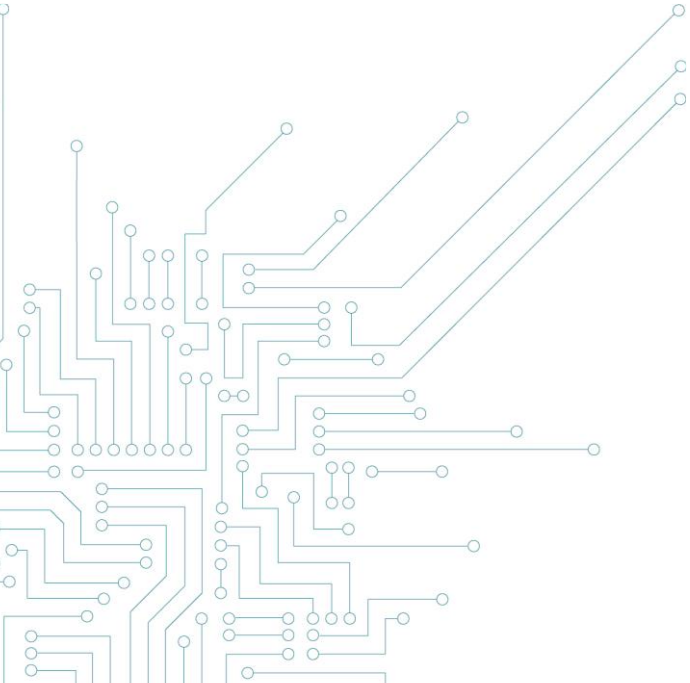
CENTRE FOR CYBER SECURITY BELGIUM

UNDER THE AUTHORITY OF THE PRIME MINISTER

.be

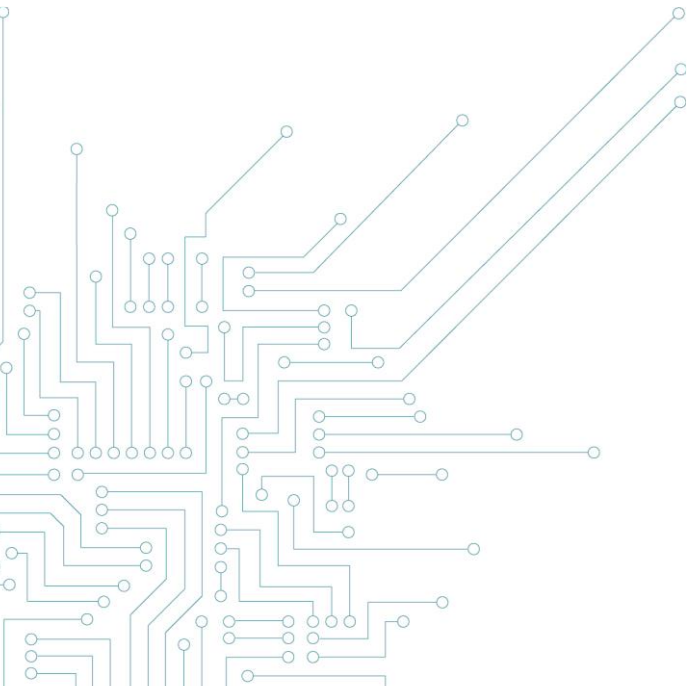
# How to keep control of your mobile devices



April 2023

# Table of Contents





# 1 Introduction

The corporate environment and data are more easily protected on-site but end-users also access data, and eventually keep copies on their mobile -or sometimes personal- devices.

The scope of mobile devices covers any asset that is allowed to access the organization's network and resources from outside the office, and thus both laptops and smartphones. However, laptops are more generally provided by the company and included in the security strategy, set up and hardened by the IT department before being delivered to the employee.

Therefore, this paper will mainly focus on smartphones, corporate or personal, that are used by employees. Such devices and their linked connected devices (watches, etc.) are open to the world among others via social networks. They are the hub of important personal, professional, or confidential data.

Whether you are a private citizen, a worker in a critical sector, a minister, a military officer, or anyone else, the data collected need to be carefully protected. The data in question are your location, biometric health, and habits. They are valuable and at risk for unintentional leaks or espionage, no matter whether it comes from private companies, competitors, foreign countries, or criminals.

The data security problem is not only technical or dependent on the user directly. It can also come from the legislation of the country where the data is hosted. Because some foreign countries have in their law the authorization for the government to consult the exchanged and stored data for user accounts. This could be as much the case for a cloud solution that will automatically synchronize data as for what users transmit via social networks.

If you are a person of public authority or if you can personally represent a risk because of your position or your knowledge, your protection even in a private context is to be taken into account and, at least, to completely separate your personal and professional digital life. More than that, it would be interesting to limit in a general way the personal data you share on social networks. They could be used against you or against your entourage in order to reach you.

In this paper, we will talk about the best practices and technologies involved with Mobile Device Management (MDM) technologies on mobile devices. They aim to protect data that leaves the security of the corporate network as well as personal data.
Today, most MDM solutions include DLP. That's why we are going to discuss the integration of mobile devices with MDM solutions.

# 2 Device management policy

The first step will be for the organization to define what are the risks. As detailed in the introduction, the situation will be different depending on yourself, the size of the company, the criticality of the sector, the capacities of the competitors, in short: your value, and the value of the data you protect.

Organization policy for device provisioning will in most cases be one of the following:

- Corporate-owned device: the device is bought and configured by the organization.
- Bring Your Own Device (BYOD): the organization's tools and access are set up on the employee's device.

The best approach will be a choice between security and work comfort for employees. A completely restricted access is more secure but will make employees' life complicated and maybe unproductive. If employees are authorized to use their personal devices (maybe for a financial reason for the organization), it is normal that they remain owners of their hardware and keep sufficient permissions on it.

In a BYOD situation, the user owns the device, not the organization. This makes security somewhat trickier for IT to establish and maintain.

In a corporate-owner situation, the situation is clearer. The IT department can put in place all the restrictions it wants like removing administrative access to the device, choosing the applications that are installed, restricting resource access depending on location, blocking synchronizations with external providers, and all necessary policies to prevent unwanted actions.
But is it possible to apply such "enterprise" security on personal devices? Elements of an answer are below.

## 3 Minimum security configuration

When you are dealing with data, you will always want to be sure that the person who accesses them is identified and has sufficient privileges. You will also want that the channel through which the data transit is not readable by someone else. You will also want to be sure that the data won't be read by someone else while stored. These are the three principles that guarantee integrity, confidentiality, and authenticity.

According to that, at a minimum, any mobile device that accesses or stores business information:

- should be configured for user identification and strong authentication (strong password, MFA),
- must be encrypted,
- should run current anti-malware software (or better an EDR which will also detect abnormal behaviors rather than just known signatures),
- and must use virtual private networking (VPN) links to access the corporate network.

For a corporate Microsoft environment, which is more frequently the case, Intune already gives a lot of possibilities. The solution can also manage IOS devices if employees have both Android and IOS devices.

## 4 Mobile device hardening

The following measures should be taken for better security of the devices and data:

- The device is enrolled via an MDM solution,
- Back-ups are done regularly,
- User education about Data Loss Prevention and best practices in that matter,
- Data classification is in place (labeling is different than classification),
- Policies about data management, classification, and usage are made and explained at the organization's level (data classification standard must be incorporated into your organization's overall security policy),
- A mobile DLP software is watching mobile users, but nowadays this is more often included with MDM.

## 5 Anti-malware solutions

Today, the main mobile OS Android provides sandboxing for applications. That means that by default, applications can't interact with each other and have limited access to the OS.
Corporate applications can cohabit with personal ones but respect a strict separation. For example, you can have two versions of your favorite messaging application, one professional and one personal with separate contact lists, message history, etc.

The isolation with IOS is even more strong and will greatly limit the inter-application interactions without the user's consent. Therefore, antivirus software in an IOS environment cannot run efficiently, as it cannot analyze the actions of other applications.

More than that, today many threats that third-party anti-malware protected against are now handled by default when the correct configuration is set up at the OS level. This is the case for both laptops and smartphones. But even if the built-in anti-malware security is performant, don't forget that this needs to be kept up to date. Apps and OS-level updates could be automatic, but manufacturer ones can require manual intervention.

# 6 Mobile Device Management

A proper and clearly defined device management policy is the first step to success.
After that, you will get help from tools to achieve your goals and keep control of your mobile devices.
Also, keep in mind that adding an additional layer will require time and people to manage it (eg. Applying security fixes, updates, testing new brands, etc).

Mobile Device Management (MDM) solutions are available from many vendors on the market.
Every asset is enrolled in the MDM appliance prior to being delivered to the employee.
The device is now remotely manageable for the IT department and significantly improves the onboarding process and maintenance time.

These solutions allow you to have an up-to-date inventory of your assets, manage applications on them, monitor them, wipe them, locate them, and enforce policies like password strength, MFA, encryption, an obligation to connect to the corporate environment via VPN, detect data exfiltration, etc. These are the main features and a must-have for a well-managed mobile devices fleet.

There are two big ways to manage mobile devices with an MDM solution. The first one is to completely isolate the device. The second is to create two separate and isolated environments on the same device. The latter is the hard way and is sometimes heavy for the hardware.

The security flaw will come mainly through the installation of malicious applications to which the user will give access rights to the storage, or through legitimate applications whose data management in the background is not controlled.
In both cases, the MDM solution will give the IT department the right to select the approved applications with more capabilities regarding to device security and data management. The selection criteria will be based on both business needs and tests of the application's safety.

Here are some of the most common MDM solutions:

- Ivanti MobileIron
- VMWare Workspace ONE
- BlackBerry Unified Endpoint Management
- Microsoft Intune
- Citrix Endpoint Management
- IBM MaaS360
- Cisco Meraki
- Kandji (for IOS)
- etc.

# 7 What do you need to effectively manage mobile devices (Checklist)

## 7.1 To gain Control on mobile devices you need…

- An acceptable list of mobile devices and platforms authorized to connect to the enterprise network(s) is defined.
- A mobile security standard defines requirements and configuration baselines for mobile devices and platforms.
- Lost or stolen devices are reported, tracked, and managed through a standard process and via an implemented MDM solution.
- A centralized mobile device management platform is deployed and used to monitor and track device usage, configurations etc. and performs integrity checks (e.g., jail break detection) prior to allowing access to internal resources.
- A basic set of access permissions and configuration baselines are defined for BYOD devices and integrated with MDM solution.
- Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container.
- Mobile devices implement basic DLP (Data loss prevention) use cases such as monitoring and alerting and are integrated with enterprise SIEM infrastructure for monitoring purposes.
- BYOD devices implement the same or improved levels of restrictions and security controls than firm-owned mobile devices.

## 7.2 Device encryption needs to be implemented

- All devices implement strong encryption capabilities during storage and transmission.
- Full disk encryption technologies are implemented (i.e. BitLocker in Windows, Filevault in MacOS) with pre-boot authentication implemented.
- FIPS (U.S. Federal Information Processing Standards) approved algorithms such AES, or equivalent industry standards, are implemented.
- Encryption standards are customized and adjusted based on the criticality of device and data stored in the device.

## 7.3 Mobile devices need to be correctly configured & hardened

- Controls implemented to prevent unauthorized changes to configurations and baseline builds.
- Secure configuration or hardening standards are established and published for all technology platforms including mobile platforms such as iOS, Android etc, and are required for any device before it can be connected to the network.
- End users do not have administrator privileges on their endpoint.
- Patching of device operating systems or applications takes place regularly.
- Devices without the latest security patches are quarantined and patched before network connection.
- Baseline / build images and standards are periodically reviewed and updated.
- Automated tools are used to detect deviations from security configuration standards, and timely corrective actions are taken to close deviations.

## 7.4 You need to implement Host-based detection like anti-malware

You will find useful and complete information in our related paper: https://cert.be/en/paper/recommendations-anti-virus-edr-and-xdr-security-solutions

### 7.5 You need to track Mobile devices and software tracking

- Centralized inventory of all authorized and unauthorized software and devices exists and captures appropriate details regarding assets (e.g., owner, criticality etc.).
- The asset inventory is reviewed and updated at least annually.

### 7.6 You need to implement mobile devices ownership & lifecycle monitoring

- Critical devices are monitored throughout the organization and have a defined owner.
- Devices, including hardware and software, are monitored throughout the asset lifecycle from procurement to retirement, and all ownership changes are tracked.
- Change management process is in place to request and approve changes to devices throughout device lifecycle.
- Automated monitoring of assets through asset inventory.

### 7.7 You need to label and review your mobile devices

- Devices are labelled with appropriate security classification.
- Devices are periodically reviewed and re-labelled during asset changes.

Sources:


- Lindros, E. T. K. (2023, February 4). *5 Ways to Prevent Data Loss in Mobile Environments*. CIO. https://www.cio.com/article/288235/mobile-security-5-ways-to-prevent-data-loss-in-mobile-environments.html
- Geekflare. (2021, September 25). *8 meilleures solutions de prévention des pertes de données qui pourraient vous faire économiser des millions*. https://geekflare.com/fr/data-loss-prevention-solutions/
- Desai, P. (2023, March 7). *Step-by-Step New Windows Autopilot Setup Guide [2023]*. Prajwal Desai. https://www.prajwaldesai.com/new-windows-autopilot-setup-guide/
- *Antivirus and other security software. (n.d.).* https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software