Enterprise Mobility

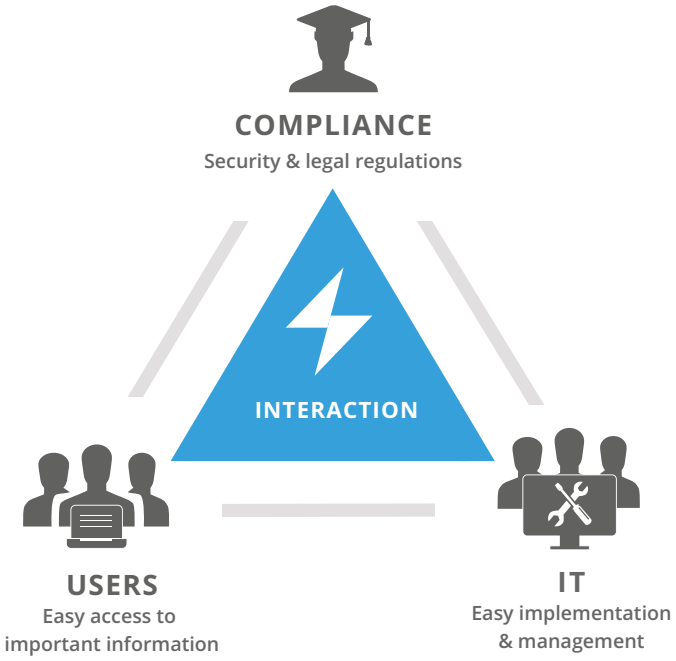
THE BEST APPROACH TO SECURE MOBILE ACCESS

Soliton®

More stringent legislation and (local) regulations as well as the increasing number of cyber-attacks force companies to investigate solutions which provide secure mobile access to corporate data. Stationary IT systems and laptops for example may often be well secured but seldom this applies to smartphones and tablets, especially if these are private owned devices (BYOD – Bring your own device).

Organisations and IT administrators face the challenge of finding a secure solution which:

- secures corporate data from internal and external threats,
- are user friendly and offer high security without limiting/restricting users in their daily work,
- are 'affordable' and offer easy implementation and low maintenance,
- guarantee secure data access and comply to internal and external data privacy policies.



Approaches to mobile working

The predominant solutions on the market can be classified into two categories:

Device-centric: Solutions include Mobile Device Management (MDM), Enterprise Mobility Management (EMM) or Unified Endpoint Management (UEM)

Data-centric: container solutions based on application or operating systems

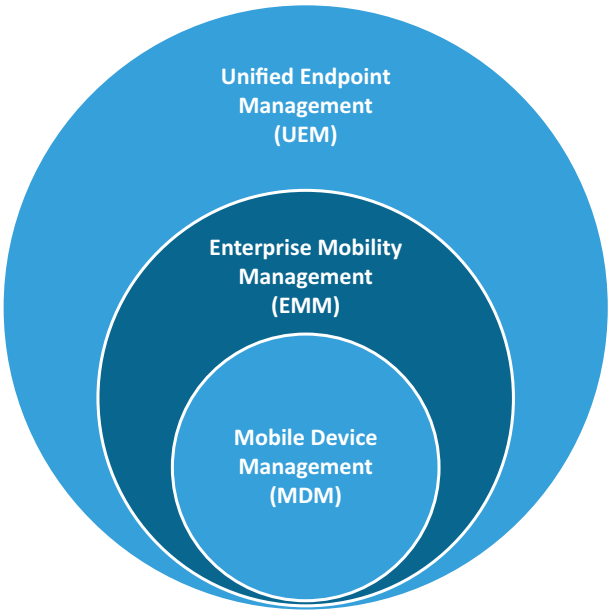
Device-centric solutions

Mobile Device Management (MDM):
At the core of this solution we find Asset Management and controlling ofthe mobile device. MDM solutions allow the IT department to specify and even enforce rules for the use of devices and apps. Apps may thus be pushed onto mobile devices without user involvement.

Enterprise Mobility Management (EMM):
Next generation of MDM solutions that include components for Mobile Application Management (MAM), Mobile Content Management (MCM) and Identity and Access Management (IAM) for a broad spectrum of mobile devices and platforms. EMM solutions often have their own app to access corporate data, such as PIM apps (Personal Information Management) for accessing e-mail, contacts or calendars.

Unified Endpoint Management (UEM):
UEM solutions contain EMM solutions plus some additional Client Management Tools for PCs, wearables, smartphones, tablets or other IoT devices.

Focus on devices



Data Centric Solutions

Data centric solutions only secure the corporate data and corporate applications, regardless the operating system or whether the device is private or corporate owned. Compared to device-centric solutions, this is a more flexible approach to securing corporate data and the privacy of the user; only corporate data is managed, not the device itself.

App containers: Container solutions create a secure and separate area on the smartphone or tablet, in which the most important business applications is kept, e.g. a Personal Information Manager (PIM) for accessing e-mails, calendars and contacts, and other applications such as file-sharing or intranet applications.

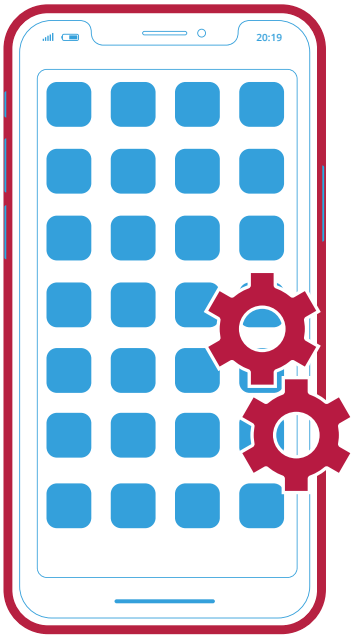
Data centric

Device centric or Data centric - which solution suits best?

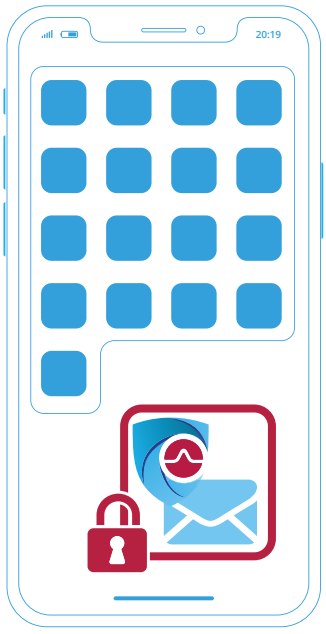
Device centric solutions offer more functionalities for managing the device. It should be clear that integrating such system involves significant configuration and setup efforts for the IT department. Furthermore, additional IT resources are required for daily management, often at significant cost.

A container will ensure that corporate data are clearly separated from any other data and applications on the mobile device. Apps such as WhatsApp can never access information in the container (e.g. contact addresses or pictures). Data in the container are encrypted both on the device and in transit, preventing unauthorised access or manipulation. Container solutions are generally controlled via their own management software. Users are created and activated through the management portal, access rules can be defined, and the container can remotely be wiped should the device be lost. This is also possible via installed MDM or EMM solutions in conjunction with the container.

A data centric approach means that the IT department provides secure data access – a solution which is easier to manage. Users can use their mobile device without any restriction or limitation, even if it is their private device. The IT department only manages the container app content, not the entire device.



Device centric:
securing the entire device



Data centric:
securing corporate data

Summary

Today, two approaches of secure access to corporate data on mobile devices exist; a) device management and b) securing company data. Based on past developments and market trends, many companies simply opted for Mobile Device Management without considering whether this is the best solution, given their specific circumstances.
Which approach is the best depends mainly on the corporate needs and priorities:

- Do I want to fully control and secure the device as such (device centric)?
- Or do I want to allow employees secure mobile access to corporate data (data centric) ?

Scenarios also exist where a combination of both solutions makes sense, e.g. the container app may be managed and pushed by an MDM system.

Important questions prior to making decisions

Who are the users?
- ◯ Internal employees only
- ◯ External co-workers, partners and/or suppliers
- ◯ Both of the above

Which devices will be used?
- ◯ Company-owned devices (personal use prohibited)
- ◯ Company-owned devices also for personal use (Corporate-Owned, Personally Enabled – COPE)
- ◯ Private owned devices (BYOD)

Which applications should be made available for the end-user?
- ◯ PIM functions (e-mail, calendar and address book)
- ◯ Access to company resources (intranet or file sharing)
- ◯ Own developed apps

What's the main objective?
- ◯ Securing company data through an easy-to-use application
- ◯ Control data and devices: asset management, company-owned devices, VPN/ WiFi setup, etc.
- ◯ Distribution of company-owned apps
- ◯ GDPR compliance

Finding the right solution

A Mobile Device Management solution may be the answer in the following cases:

- Devices must be controlled and integrated into asset management systems (company-owned devices).
- You have developed your own apps to be pushed onto the devices.
- You have your own VPN infrastructure and wish to manage policies on the end devices.
- You have a qualified IT department familiar with the setup and control of such a system and with sufficient available management resources.

A container solution is recommended when:

- Data security is more important than managing / controlling the device.
- You have internal and external users.
- Official devices are allowed for personal use (COPE) or employees can use their personal device (BYOD).
- Communication and access to corporate resources is the main scenario for mobile working.
- You have no or only a small IT department and want an easy-to-use solution that requires minimum management

Advantages of container technology

- ✓ Flexibility as no MDM is needed, for iOS and Android and for personal and company-owned devices
- ✓ One app with all the functionalities: e-mail, contacts, calendars, tasks, notes, processing and storing documents, browser and camera
- ✓ Easy setup and rollout

GDPR – Requirements for mobile working

The General Data Protection Regulation (GDPR) is a European Union regulation harmonising the rules of processing personal data by private companies and public entities. Personal data are retrieved, stored or processed also on smartphones and tablets, requiring additional security measures to prevent data leaking on these devices. The GDPR also requires companies to implement security measurements to protect personal data on private and corporate owned mobile devices. Moreover, data protection must be ensured by the right technology and privacy-friendly default settings. This requires the implementation of suitable technical and organisational measures (TOMs).

In addition to the GDPR's requirements for documenting and information sharing IT must operate according to the GDPR.

Article 5 Para. 2 demands data integrity and confidentiality, among other. This can only be assured by clear separation of business and personal data and applications on mobile devices. Only in this way can business data be reliably secured from external threats and unauthorised access, use or disclosure. Article 32 requires precautions are taken to secure data, e.g. by encryption. This can be achieved through store corporate data and applications in an encrypted container and encrypt all data in transit. This will also facilitate data protection impact assessments as required by Article 35. Unless corporate data are completely separated from personal data on the mobile device, assessments will conclude that the consequences to personal data protection are unpredictable and therefore not GDPR compliant.

Secure container with MailZen

MailZen stores e-mails, contacts, calendars, notes, tasks, documents and intranet on the smartphone or tablet (iOS and Android) in an encrypted container.

Encryption will be hybrid with RSA-4096 and AES-256.

MailZen can be used in the cloud and on-premises

The MailZen app enables sending and receiving of S/MIME-encrypted e-mails. This encryption and strict separation of personal and corporate data in the container means that MailZen meets primary GDPR requirements.

ANNEX: Market development MDM - EMM - UEM

Mobile Device Management (MDM)

Mobile Device Management originated in stationary IT which at that time had the strong focus on desktop PC management and configuration. MDM systems enable the management and updating of mobile devices.

Over time, the MDM systems became increasingly complex, offering other functionalities such as prohibiting use of specific apps, remote deletion on devices, jailbreaking or rooting detection, pushing of apps, location tracking, etc. Increasing complexity also means an increase in the daily management of an IT department.

Most common used MDM features:

- Inventory and management of devices
- Provisioning and management of apps
- Device password control (length of password, number of attempts, etc.)
- Remote deletion on the device
- Whitelisting and blacklisting, or blocking of apps
- Device encryption
- Network access configuration (e.g. WiFi or VPN)

Enterprise Mobility Management (EMM)

The "Bring your own device" (BYOD) trend and the increasing number of different business applications resulted in shifting the focus from Mobile Device management (MDM) to application security, known as Enterprise Mobility Management (EMM). Many MDM providers have extended their product range and are now supporting rudimentary BYOD also.

> ***„Most companies use less than 10% of EMM functionality and ignore the rest on the basis of cost and complexity. Second, organizations fail to identify the specific functional requirements for specific use cases.'***
>
> 'Top 10 Best Practices for EMM Deployment Success' - Gartner, November 2017

Most common used EMM features:

- MDM features as described above
- Mobile Application Management (MAM): controlling company approved apps
  - App distribution via an enterprise app store
  - App password rules
  - Remote resetting and deletion of apps
- Identity and Access Management (IAM)
- Mobile Content Management (MCM)
- Control of in-house apps

Unified Endpoint Management (UEM)

More and more different mobile devices are used to perform different tasks. This has resulted in further EMM developments such as the possibility to control different mobile devices, including stationary PCs, mobile devices, wearables and even IoT devices, through a single console. With UEM IT can control and define policies for the different devices.

Take the next step and read about the security features of MailZen >

2021 © Copyright All of the information and material inclusive of text, images, logos, product names is either the property of, or used with permission by Soliton Systems Europe N.V. The information may not be distributed, modified, displayed, reproduced – in whole or in part – without prior written permission by Soliton Systems. Trademarks Soliton® and its logo are registered trademarks. Disclaimer: All information herein was carefully gathered and examined, however, Soliton Systems cannot be held responsible for mistakes or incompleteness of content. Soliton Systems may change or modify parts at any time without notification and accepts no liability for the consequences of activities undertaken based on the contents.

Soliton®

ABOUT SOLITON SYSTEMS

Soliton Systems has a strong vision to innovate solutions to logically fulfil the needs of our customers without adding complexity. Soliton support companies with their security management challenges, including network security and remote access to the internal and cloud applications. Soliton's solutions protect the company's resources from unauthorized access and accidental data leakage.

EMEA office

Soliton Systems Europe N.V.

Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands

+31 (0)20 896 5841 | emea@solitonsystems.com | www.solitonsystems.com

SOL202104