



## BYOD (Bring-Your-Own-Device)

## About 1Mobility

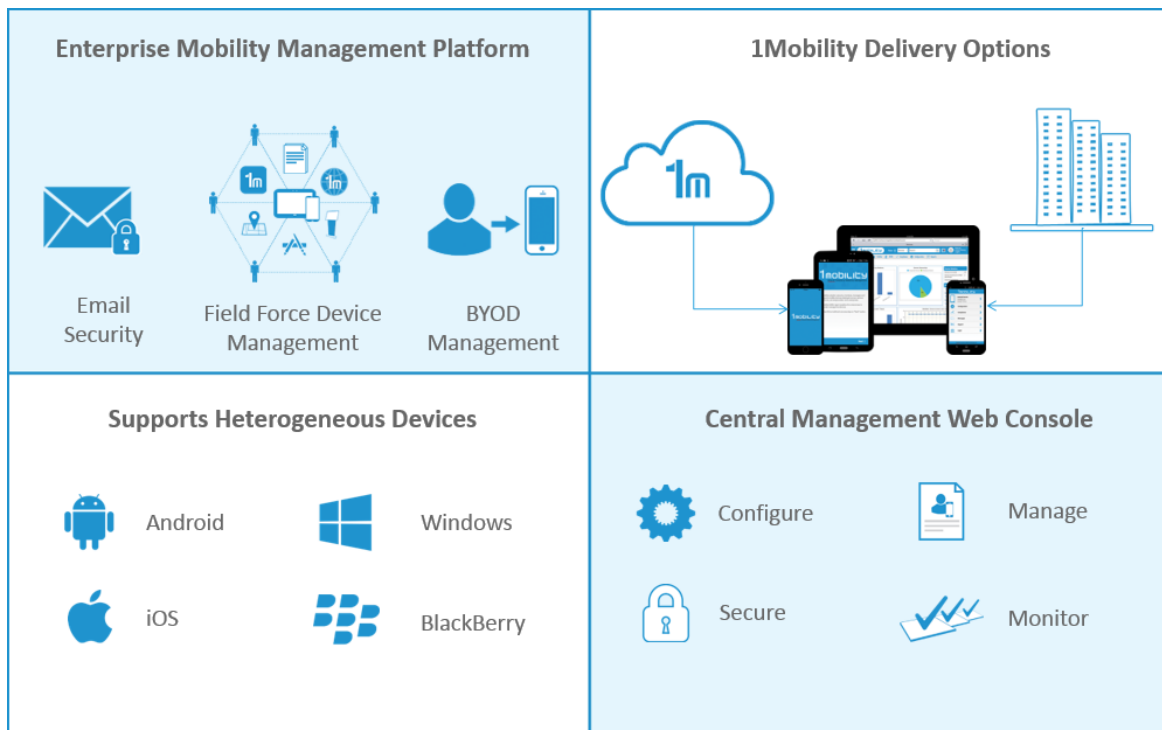
1Mobility has successfully established itself as a global company, offering cloud based, internationalized and scalable Enterprise Mobility Management (EMM) solution that monitors, manages and supports mobile devices across platforms (Android, iOS, BlackBerry, Windows), service providers and manufacturers.

1Mobility has a team of dedicated and talented professionals with over 8 years of innovative software development believes that “today, Enterprise Mobility though not mandatory, is a fact of business life for various obvious reasons like increased productivity, cost savings, competitive advantage and better customer engagement.”

Having serviced industries like Banking, Financial Services, Insurance, Technology, Education, Pharmaceutical, Communication & Media and Government and initial focus on the emerging markets, 1Mobility provides affordable solutions either cloud based or privately installed, enabling over-the-air distribution of mobile applications, configuration settings and security policies to corporate owned or employee owned (BYOD) devices through a central web console. No matter what type of organization it is, 1Mobility has affordable solutions and services for all, be it initial, advanced or matured enterprise mobility.

1Mobility offers following solutions

- Enterprise Mobility Management (EMM) through consulting, development and managed services
- Data Loss Prevention (DLP) of Mobile Data
- Compliance enforcement and monitoring
- Containerization
- BYOD Management



For further information, please visit the 1Mobility website at <http://www.1Mobility.com>

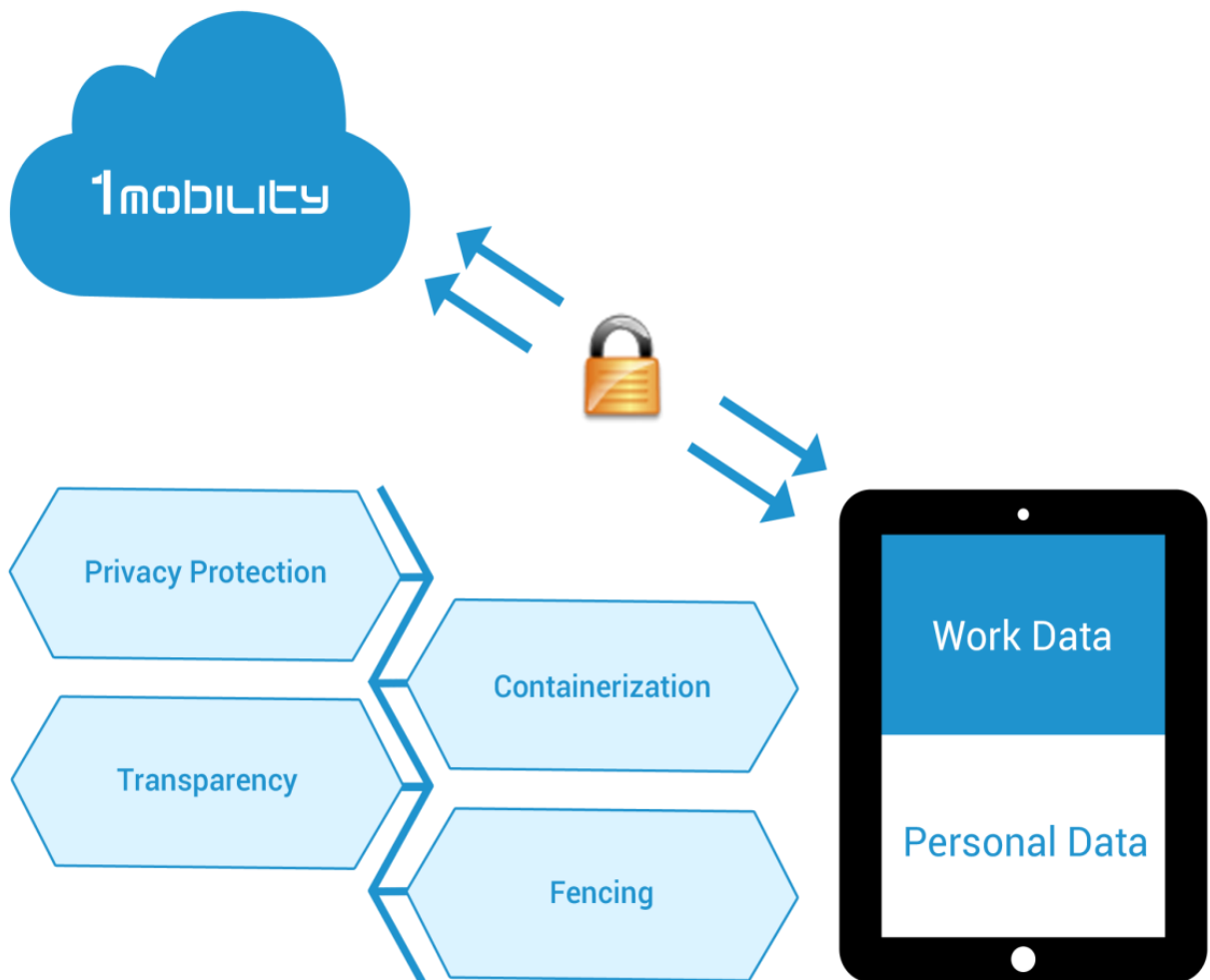
# 1Mobility for BYOD

Bring your own device (BYOD) refers to the policy of permitting employees to bring their personally owned mobile devices to workplace, and to use those devices to access privileged company information and applications.

Though BYOD brings many benefits, it creates challenges for organizations to manage and secure the corporate data on these personal devices, for example Intentional or unintentional disclosure of data or unsafe devices connecting to corporate network, etc. Organizations need to implement a solution that protects the privacy of employees without compromising security of corporate data and assets.

## Solutions

1Mobility provides BYOD Management which helps IT administrators define policies that bring a perfect balance between security of corporate assets, data and network while protecting privacy of the employees. 1Mobility fosters complete guidance to build a BYOD strategy which empowers employees to use personal devices for office use and at the same time addresses the requirements for security, simplicity and compliances. There is no change required to the existing infrastructure.



## Privacy protection for Employees

Administrators have selective rights on the BYOD devices, wherein they can manage only the corporate data. 1mobility eco-system solutions achieve this through

- ▶ No factory reset of device or wiping of personal data by administrators
- ▶ Organizations can only wipe the corporate data, enterprise Apps and configurations published on the devices by IT administrators
- ▶ Detection of blacklisted Apps without having access to list of personal Apps
- ▶ Compliance management keeping interest to keep the corporate data and network secure
- ▶ Employees are proactively informed of the changes to BYOD policies

## Containerization

- ▶ Separates corporate data from personal data
- ▶ Data Loss Prevention (DLP) for data at rest and data in motion for corporate data; including encryption, isolation of corporate data
- ▶ Seamless implementation of corporate security policies and enforce compliances, example Single Sign-on, creating secure tunnel for data in motion, integration with LDAP authentication.

## Transparency: DIY (Do-It-Yourself)

Organizations can grant access to DIY (Do-It-Yourself) portal, which allows employees to access. Employees can get access to logs and have visibility into the policies published, restrictions applied as well as audit logs of actions performed on the devices through Do-it-Yourself (DIY) portal.

- ▶ Based on Organization's polices, end users can perform various actions on their devices for example; reset passcode, clear passcode, factory reset passcode and etc.
- ▶ End user can view device information, audit Logs for actions performed by administrators on their device.

This creates a complete transparency! It empowers end users and gets better adoption of management of the devices and data by them.

## Conditional Policies

1Mobility provides a complete solution that extends a Geo-location, Wi-Fi and Time based fencing solution for BYOD. This allows organizations to define and apply policies on the devices and check compliances when the Devices connect to corporate Wi-Fi or during the work hours. These policies will be automatically removed when the devices are disconnected from the corporate Wi-Fi or during the off-hours. This brings the best balance and benefits to both:

- ▶ Employees: Privacy and unrestricted benefits of the mobile devices
- ▶ Organization: Security for organizations data without any compromise.