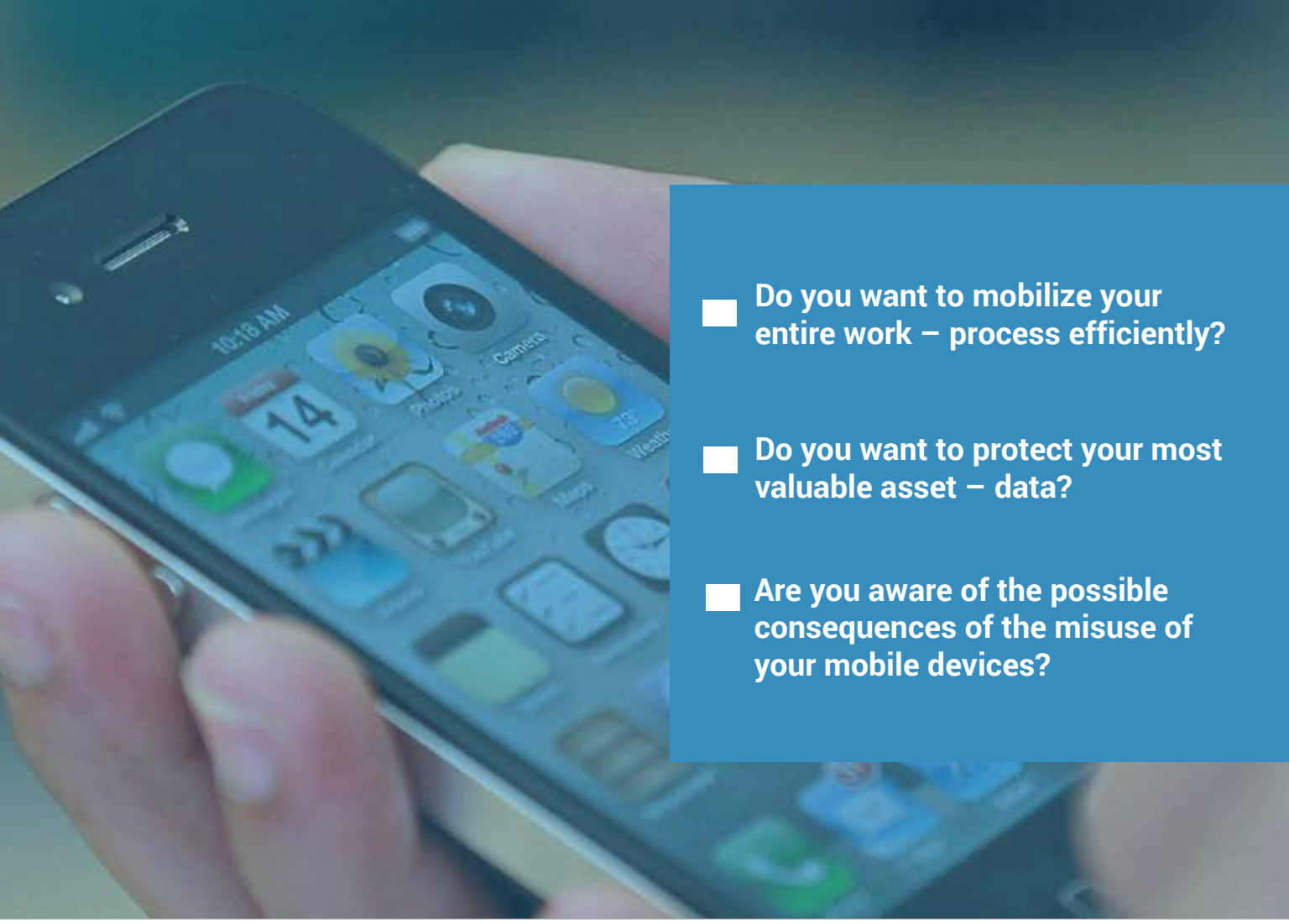


- Do you want to mobilize your entire work – process efficiently?
- Do you want to protect your most valuable asset – data?
- Are you aware of the possible consequences of the misuse of your mobile devices?

ENTERPRISE MOBILITY MANAGEMENT

IT'S NOT THE LENGTH OF THE FEATURE LIST WHAT MAKES THE DIFFERENCE BETWEEN A GOOD PRODUCT AND A BETTER ONE. MANY CAN PROGRAM SOFTWARE. IT IS ESSENTIAL ADDING EXPERTISE AND KNOWLEDGE OF THE USERS' SITUATION AND TARGETS.

DC Solutions AppSec

ENTERPRISE MOBILITY MANAGEMENT (EMM)

DO MUCH. DO EVERYTHING. DO THE RIGHT THINGS.

FACT

We are witnesses of a new digital revolution - mobile devices revolution.
Your company works in this surrounding.
It is necessary integrating and managing your mobilized work-processes and the mobile hardware utilized - from smartphone to tablet PCs - in an optimal way.
Enterprise mobility Management (EMM) is the solution you need.

ONE SOFTWARE - ALL PLATFORMS

Android
iOS
Windows Phone
Windows Mobile
Symbian

ALL IS POSSIBLE

- Device management (inventory, lock, wipe, etc.)
- System management (backup, update, etc.)
- Reporting (log relevant processes)

RAISE PRODUCTIVITY

- Configure, update & handle any number of devices with some mouse clicks saves time.
- Automate processes
- Simply integrate corporate processes via Web APIs

SIMPLER NICER BETTER

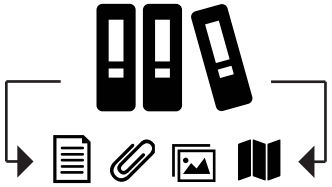
- The easy to use graphical user interface is more than just nice.
- Customizing is very simple.
- Every user group owns its optimized working environment.
- The end user different from the administrator.

AS FLEXIBLE AS YOUR DEMAND

- Flexible development of the models with mobility management services in order to increase web and mobile applications performanses.

SAFE FOR SURE

- TÜV certified
- Security audited
- You configure suitable actions on policy breaches



MOBILE
CONTENT
MANAGEMENT

MOBILE
DEVICE
MANAGEMENT

ENTERPRISE
MOBILITY
MANAGEMENT

MOBILE APP
MANAGEMENT

MOBILE APPLICATION MANAGEMENT (MAM)

MAM is a component for your Enterprise Mobility Management (EMM), that automatically responds to potential app risks. It helps you manage your applications, their installation, update, possible reconfiguration and their removal.

Your black- & whitelist for apps tested by professionals and always updated.

THE CHALLENGE

Although there are security controls that an app has to pass before the launch of the app at the various application stores, tests from various security providers show that every 2.nd app leaks non-approved data. Every day new apps are added to the various application stores and provides a new potential security risk within the company.

> Do YOU have the time for testing all the apps at the various application stores, that your employees access, for any potential risks?

THE SOLUTION

MAS — MOBILE APP SECURITY BASED ON EUROPEAN STANDARD

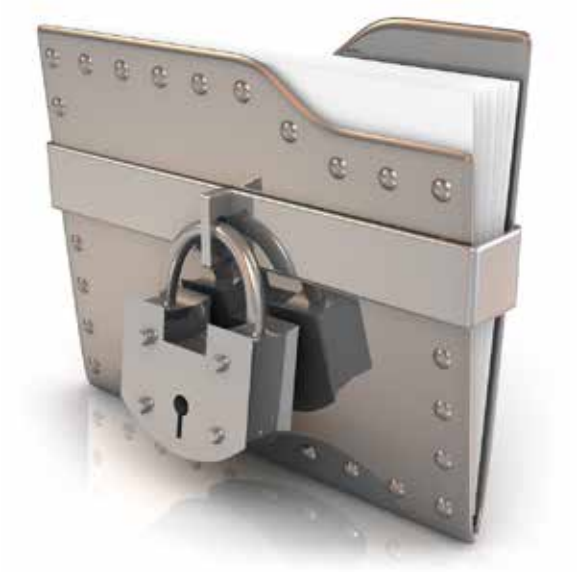
MAS offers you an access to an application directory (TAD), where you can find results and ratings of tested apps from all the various application stores for mobile operating system platforms.
Then you have a proven basis to decide yourself if you find the app secure or if you find it insecure and would add the app to a Blacklist.
The creation of Black- & Whitelists for your company apps is either done automatically or via your MDM admin control using simple clicks creating your own customized lists.

MOBILE CONTENT MANAGEMENT (MCM)

MCM is a component for your Enterprise Mobility Management (EMM), that allows protection of your most valuable asset – data.

Losing a hardware is retrievable, but losing data will hurt your company directly.
Your reputation will be seriously compromised.

In order to prevent these situations, you can use MCM that offers you data security functions, partial or complete removal of data in the case your mobile device gets lost.
Identity Management (IM) enables you to define the actions that are allowed for mobile device users, as well as keeping track of their activity.



MOBILE DEVICE MANAGEMENT (MDM)

INTELLIGENT MOBILE DEVICE MANAGEMENT THAT UNDERSTANDS YOUR NEEDS.

MDM is the component that integrates enterprise mobility into your business systems: Not only does
it provide all the functions you need – its architecture, the services that accompany it and our security requirement reflect the demands of leading European enterprises perfectly.

WHY DO YOU NEED MDM?

- Enables efficient call cost control (roaming)
- Protects your company data against loss through mislaid mobile devices
- Supports your business processes
- Gives your employees secure mobile access to data protection regulations and rules on conduct of your IT infrastructure
- Controls mobile devices via actions and rules of usage

MDM CHARACTERISTICS?

MDM solution offers functions that can be used on smartphones with the following operating systems: iOS, Android, Windows Phone

Available in english and german

Easy installation
An integrated viewer makes it possible to view and to process standard office files and images, as well as media files

Strictly separates the business data from the private area of the device user

Keeps data costs and call costs in home and/or roaming networks under control

MDM TOOLS

SECURE ACCESS GATEWAY (MAG)

COST GUARD

FILES2GO

SECURE PIM

MOBILE APP SECURITY (MAP)

SECURE ACCESS GATEWAY (SAG)

YOU DECIDE WHO ACCESSES YOUR COMPANY DATA!

The fact that tablet PC and smartphones are now very widespread means that employees are also increasingly checking their email while on the go.
Now it must be ensured that this infrastructure is protected from damage by being accessed from outside, irrespective of the operating system of the end device and the type of access.

SAG and your firewall together protect your IT infrastructure from misuse and damage.

If users want to access the Exchange server by means of a mobile end device, they must be authenticated to get through the firewall. This is done on the basis of a "unique identifier" (IMEI, serial number, ActivesyncID, AppID). The firewall checks the Secure Access gateway, a MDM option on the MDM server to see whether the identifier belongs to an end device that is registered in the MDM. If this is the case, data access is permitted. Otherwise, the device is rejected by the firewall.
This is how you can protect your data and information from unauthorized use and abuse.

COST GUARD

NOW, PHONE COSTS CAN BE PLANNED, CONTROLLED AND REMAINED WITHIN THE BOUNDS OF THEIR CONTRACTED TARIFFS.

This app allows you to control phone call costs, especially roaming costs.

THE APP HAS 3 MAJOR FEATURES

- Whitelisting of phone numbers (phone numbers that are not on the list can't be dialed)
- Control of the voice call duration
- Control of the data volume usage

CostGuard app can either be enrolled and configured automatically to all Android devices in the company, or installed locally, and manually configured. Besides, app can control phone costs, roaming costs, the amount of data transfer and which number you can call, it also gives alert to the user if it comes to determined limit. When the actual limit has been reached, or exceeded, the user will only be able to dial previously defined numbers (e.g. director, manager, admin etc.), these limits can be temporarily extended. Emergency numbers are always available!

FILES2GO

PROTECTING DATA AND SAFE ACCESS ARE IMPORTANT, BUT AVAILABILITY OF DATA IS ALSO VERY IMPORTANT.
YOU WANT YOUR EMPLOYEE AVAILABLE TO THE CUSTOMERS AT ANY TIME.

We offer a solution for iOS terminals, which makes it possible to access data from the company network that have been approved for mobile access. An integrated Viewer allows it to view and edit standard Office files and images, as well as media files. Files2Go makes it possible to synchronize locally modified data with the company's IT infrastructure.
Communication takes place via a certificate-based SSL connection between mobile end device and IT infrastructure. All data are exchanged in a cloudless manner - direct and encoded - between the app and the server in the company.

SECURE PIM

BUSINESS DATA OF YOUR COMPANY NOW CAN BE USED WITHOUT ANY RESTRICTION, PROTECTED BY PASSWORD AND SELECTIVELY DELETED – IF IT'S NECESSARY.

Popularity of mobile devices endanger privacy and safety of company's documents and data.
Mobile devices, as we all know, are often used by busy users in unsecured surroundings, such as public hotspots, coffee houses, and shops – and pose a significant risk of loss – and of course theft!
MDM gives you one more tool – Secure PIM (Personal Information manager).
This tool on a mobile device separates user's private and business zone.
This tool is available for iOS devices, soon for Android.

MOBILE APP SECURITY (MAS)

DO YOU HAVE TIME FOR TESTING ALL THE APPS AT THE VARIOUS APPLICATION STORES, THAT YOUR EMPLOYEES ACCESS?

Every day new apps are added to the various application stores and provide a new potential security risk within the company and tests from various security providers show that every 2nd app leaks non-approved data.
MAS offers you an access to an application directory (TAD), where you can find results and ratings of tested apps from all the various application stores for mobile operating system platforms.
Then you have a proven basis to decide yourself if you find the app secure or if you find it insecure and want to block that app.

This tool enable creating lists for approving certain apps and also list for blocking those apps that threatens your data safety. For those apps that do not violate your company safety you can create „Whitelists“, and for those apps which do violate your company safety you can create „Blacklist“ and block them. This tool is available for Android and IOS devices.

DVC Solutions

A [Dr Mladena Stojanovića 4
78 000 Banja Luka

T [00387 51 340 616
F [00387 51 340 617

W [www.dvcsolutions.com
E [info@dvcsolutions.com

www.dvcsolutions.com