# MOBILEKEEPER

Korea's No.1 MDM Solution: Integrated Mobile Security and Management Solution

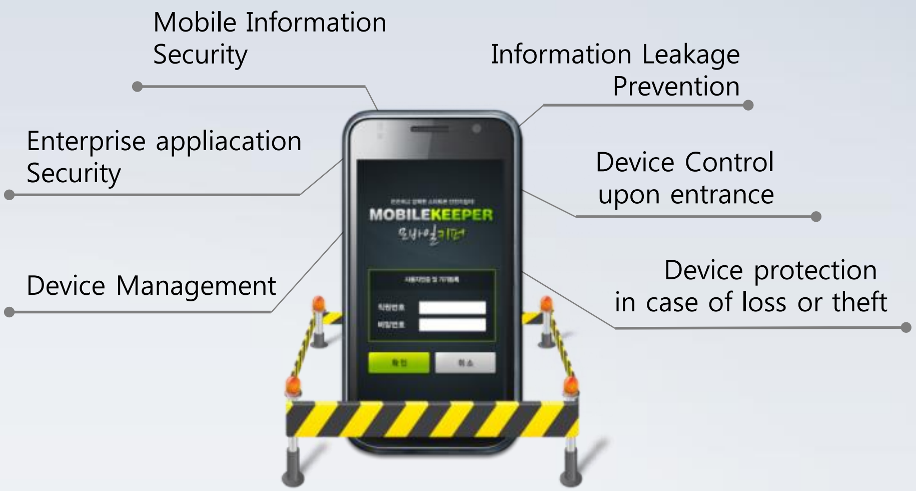
지란지교시큐리티

# Product Overview

MOBILEKEEPER

# Product Concept

## Mobile Security & Management Solution


Mobile Information Security

Information Leakage Prevention

Enterprise appliacation Security

Device Control upon entrance

Device Management

Device protection in case of loss or theft

**MOBILEKEEPER**

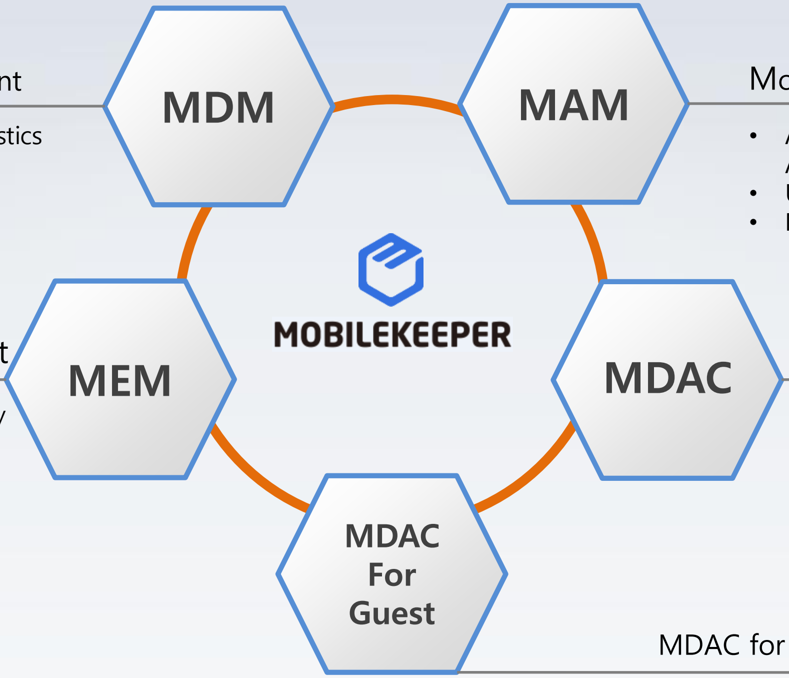
## Integrated Mobile Security and Management Solution

MOBILEKEEPER is an MDM (Mobile Device Management) solution that manages mobile devices within a company and provides **remote locking and data deleting services in case mobile devices are lost/stolen** to prevent information leaks.

In addition, MOBILEKEEPER protects company and personal information through **Mobile Application Management (MAM)** and **Mobile Application Security (MAS)**, functions designed for the work environment. MOBILEKEEPER also **automatically blocks and regulates diverse smartphone functions upon entrance** into a security area to prevent internal information from leaking due to smart devices (camera, recording, etc.).

Jiran Security's MOBILEKEEPER is the **best solution for preventing information leaks from mobile devices**.

# Product Coverage



MOBILEKEEPER

MDM

Mobile Device Management

- Mobile device management and statistics
- Loss and theft response

MAM

Mobile Application Management

- App distribution and management
  App Operation support
- User/group management and statistics
- Meet mobile security compliance

MEM

Mobile E-mail Management

- Mobile email management & security
- User authorization control
- Download of attachment prohibited

MDAC

Mobile Device Access Control

- Automatic mobile device access control
- Blocking the device access carried into the security areas of the company

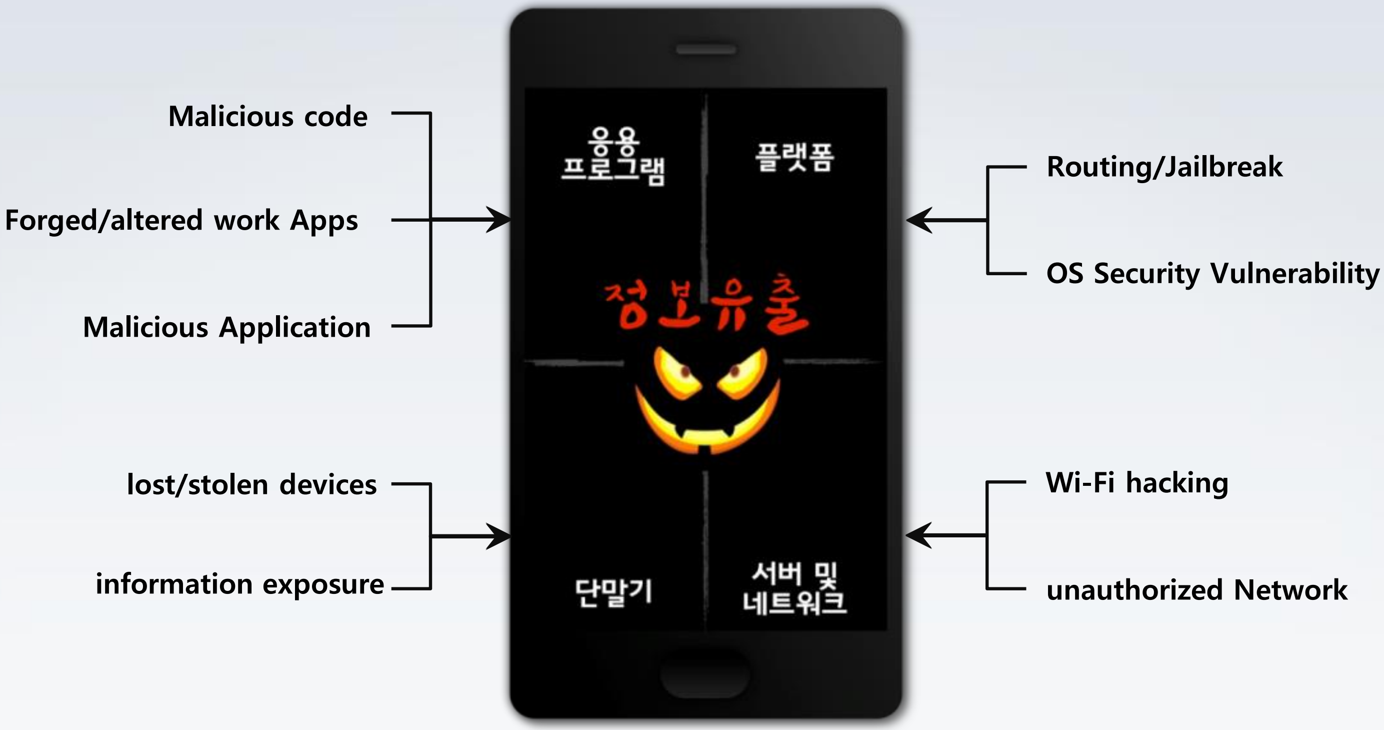
MDAC For Guest

MDAC for visitors

Mobile device access control for guest without system setup

# Mobile Security Threats

As mobile work environments become more commonplace, **cases and threats of diverse information leaks from smart devices are increasing**. Mobile security is essential for protecting **vital personal and company information**.



Malicious code

Forged/altered work Apps

Malicious Application

Routing/Jailbreak

OS Security Vulnerability

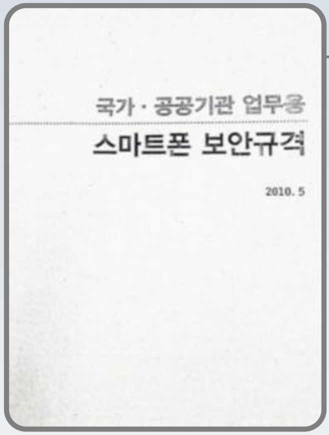
lost/stolen devices

information exposure

Wi-Fi hacking

unauthorized Network

# Mobile Device Compliance


국가 · 공공기관 업무용

스마트폰 보안규격

2010. 5

## National Intelligence Service [Smartphone Security Regulations]

Permit only registered devices access to work systems
Prohibit wireless, tethering, and screenshots to prevent work related materials from leaking
Periodically inspect and take measures for operation system integrity (routing/jailbreaking)
Deny corrupt devices access through integrity checks
Prepare security alternatives by using Mobile Device Management (MDM), preventing screen shots, storing data in case of lost/stolen devices, S/W remote wiping
In case of administrative services, restrict Wi-Fi functions and allow 3G only

## Financial Supervisory Service [Smart Work Information Security Guidelines]

Restrict access and conduct integrity inspections at crucial times in case of failure to update work Apps
Force termination in case of abnormal access and connection
Block access for routing/jailbreak devices
Prohibit widespread distribution through an official Appstore
Apply password combination characters and implement periodical password changes
Block unregistered devices from access to smart work
Block screen capture functions when using work related Apps

금융권 스마트워크 정보보호 가이드라인

(금융감독원 IT감독국, '11.6월)

I. 개 요

1. 목적 및 범위

- (목적) [illegible]
- (적용대상) [illegible]

2. 용어 정의

- (스마트워크) [illegible]
- (이용자) [illegible]
- (중요정보) [illegible]
- (무선통신망) [illegible]
- (단말기) [illegible]

3. 법규 준수

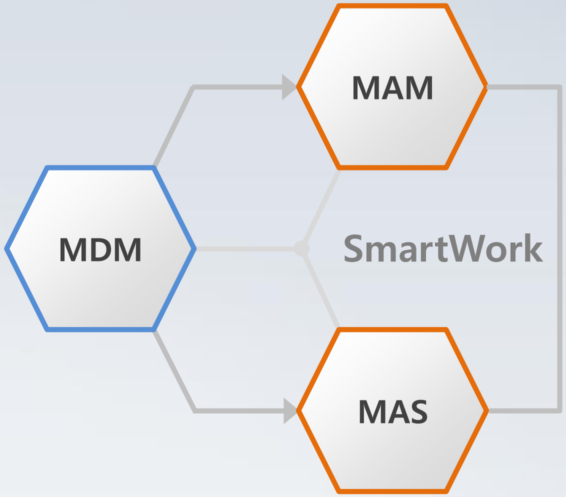
- [illegible]

- 1 -

# The Development of MDM in Korea

## Main Solution Functions for Compliance

- Check for forged/altered work Apps and restrict access
- Restrict functions (screen shots, Wi-Fi, etc.) when using work Apps
- Authenticate device when installing mobile security, and restrict access/encourage installation
- Compulsory use of locked screens and passwords when using work Apps
- Prepare remote data deletion functions in case of lost devices with work Apps
- Restrict access in case of failure to update work Apps and mobile security programs
- Restrict access to work systems through Wi-Fi and block Wi-Fi
- Restrict routing/jailbreak devices from accessing work Apps
- Encode exchange to exchange (E2E) data



# Mobile Security Needs

☑ Can we protect internal company information from leaking through mobile devices?

☑ Can we strengthen security for work related Apps?

☑ Can we easily distribute and manage work related Apps?

☑ Can we automatically restrict mobile devices upon entrance?

☑ Can we prevent information leaks in case of lost mobile devices?

☑ Can we minimize user dissatisfaction when applying security to BYOD (bring your own device) policies?

# Solution benefits

Recently, mobile work environments are implementing BYOD policies, where employees use their own personal devices. As such, the key to security is to **guarantee the rights of the user and minimize dissatisfaction while applying effective security measures**. MOBILEKEEPER enables efficient and effective security measures in the BYOD work environment, and provides **measures and cases for successful change management**.

.

## User Satisfaction

Minimize user dissatisfaction
Protect personal life/ personal information
Successful change management

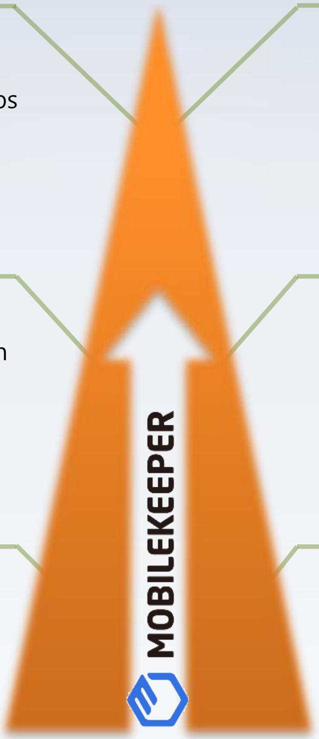
Security & Management for

BYOD

## Effective Security

Strong security policies
Apply necessary security measures only
Adhere to security regulations

# Key effect of Solution



### Strengthen Security of Mobile Office Work Apps

Authenticate work App use and strengthen access stability
Restrict smart device functions when using work Apps

### Effective Distribution and Management of Work Related Apps

Conveniently distribute Apps through push services
Understand installation conditions and usage situation

by version
Manage user Apps and work-related Apps

### Protect and Manage Company and Personal Assets

Improve recoverability of lost devices
Understand usage situation of mobiles within the company and reflect related information into policies

### Prevent Information Leaks from Smart Devices

Restrict information exposure through remote control in case of lost/stolen devices
Restrict smart device functions upon entrance into security area

### Security Inspections and Compliance Measures

Prepare a response system for mobile security inspections
Adhere to compliance regulations as dictated by the Financial Supervisory Service, National Intelligence Service, etc.

### Prepare a Basis for Smart Work Environment

Take measures for user change management and establish an efficient work environment
Establish a basis for expanding mobile work environment

# Strength & Reference

MOBILEKEEPER

# Strengths

700,000 user

시장점유율
기술력

Leader in Number of Clients
: Product developed by using client feedback as a basis

No. 1 in all benchmarking tests (BMT), verifying our technology and stability

Provide optimal operation/establishment guidelines in accordance with each purpose

Provides user change management measures based on experience

# Strengths

## Pioneer of MDM Technology

## Case of System Establishment for the Largest Number of Users

### Reliability

### Stability

- **First domestic company to receive CC certification (2014.7)**
- Passed Financial Supervisory Service security inspections: Shinhan Bank, Shinhan Life Insurance
- Passed National Intelligence Service security compliance inspections: Korea Water Resources Corporation (SL-3), National Security Research Institute (SL-4)
- First domestic company to receive GS certification (2012.10)
- Partnership with 3 device manufacturers: Samsung Electronics, LG Electronics, Apple MDM SDK

- Currently operating for **over 700,000 users** within the company

: Provide for diverse devices,

solve diverse issues

- No. 1 in all BMT (refer to client company situation)
- Have diverse cases according to operational purposes/business groups/targets

### Project Implementation Capability

- **Incorporated a project implementation time responsible for establishing MDM**
- Specialize mobile OS update support systems

- Provide optimal measures according to operational purposes/environments/policies
- Implementing systematic projects based on experience

### User Change Management

- **Consulting for minimizing user dissatisfaction**
- Consulting for optimal operating policies and processes

- **Provide user change management cases of other companies**
- Provide user PR videos
- Provide training materials, persuasion materials, legal evidence

# Competitiveness

| Category | Company Products | Domestic Products | Overseas Products |
|---|---|---|---|
| **Technology** | • No. 1 in all BMT, No. 1 in technology superiority<br>• Received grand prize in mobile<br>• Completed numerous mobile related national projects | • Inadequate fulfillment of MDM CC standards<br>• Falls short of BMT internal security standards<br>• Benchmarks our products as second developers | • MDM functions are stable but lacks app security technology |
| **Security** | • First domestic company to acquire CC certification (2014.7)<br>• First domestic company to acquire GS certification<br>• Passed Financial Supervisory Service security inspections<br>• Passed National Intelligence Service security compliance inspections | • Only some products have acquired the GS certification<br>• Passed only some of the National Intelligence Service security compliance inspections | • Have not satisfied domestic security criteria |
| **Stability** | • One server provides for 700,000 active users<br>• Has cases of operational experience, etc Has numerous large-scale references | • Do not have many references and therefore lacks stability | • Has cases of stable operation related to MDM functions in the overseas market |
| **Availability** | • Accommodates a large number of users and data<br>• Provides independent domains for each company affiliation<br>• Future expansion and high levels of compatibility alongside acceleration | • Lacks capability related to accommodating a large number of users<br>• No experience in expansion<br>• Lacks availability and compatibility as only experienced with establishing systems for individual companies | • High levels of availability but no domestic references |
| **Customization** | • Able to customize based on client company policies (based on separate negotiations) | • Able to customize | • Cannot customize, and therefore at a client win back stage |
| **Partnership** | • Established partnerships with 3 domestic manufacturers (Samsung, LG, Pantech, SDK)<br>• Contracted as a KNOX reseller<br>• Established a partnership with Apple | • Only some products have entered into partnerships. Have not entered into partnerships with all manufacturers | • Only some products have entered into partnerships with Samsung, etc. |
| **Reference** | • Large group corporations, financial institutions, companies, public institutions, etc.<br>• No. 1 in domestic references | • Extremely limited references<br>• Many false references | • Some overseas and global cases<br>• Applied group wide in Korean branches |
| **Economic Feasibility** | • Reasonable pricing system based on domestic security product criteria and maintenance of stable relations | • Low pricing policies to secure references | • Burdensome to introduce with very high prices compared to functions |

# Major Customers

## Groups

| 코오롱 | E·LAND 이랜드 | 금호아시아나 | 신한금융그룹 | JW 중외그룹 |
|---|---|---|---|---|
| Chemicals, bio, materials, R&D, distribution, fashion, construction, leisure, etc. | Food, distribution, fashion, construction, accommodations, leisure, etc. | Airline, transport, tire, construction, terminals, accommodations, IT, etc. | 13 affiliates in the finance sector | Pharmaceuticals, LED lamps for medical devices, products for cars, etc. |

## Finance

| | | |
|---|---|---|
| NH농협은행 | 신한생명 | 신한은행 |
| 신한금융지주회사 | 신한금융투자 | 신한데이타시스템 |
| 신한데이터센터 | 동양생명보험(주) | 현대해상 |
| 롯데카드 LOTTE CARD | LIG 손해보험 | 하나캐피탈 |
| 아주캐피탈 | JB우리캐피탈 | ACE 생명 |
| 비씨카드 | MIRAE ASSET 미래에셋생명 | 금융결제원 |
| KB국민카드 | and many other | |

## Research Ins. & Manufacturing., etc.

| | | |
|---|---|---|
| LG하우시스 | LG생명과학 | 현대삼호중공업 |
| HANMI Semiconductor | DONGJIN 주식회사 동진쎄미켐 | LS엠트론 |
| AGC | 오비맥주(주) Oriental Brewery Company | LOTTERIA |
| KCC | 대우건설 | t-broad |
| 'TORAY' 도레이첨단소재 | DK 동국산업 | and many others |
| LG화학 Research Park | ETRI Security Technology Research Institute | 코오롱 Technology Center |
| DGIST 대구경북과학기술원 | and many others | |

## Public Institutions

| | | |
|---|---|---|
| K water | TP 사학연금 | 한국산업단지공단 |
| IIAC Incheon International Airport | Dongdaemun Design Plaza & Park 동대문디자인플라자&파크 | ncia |
| 국군복지단 | 문화체육관광부 | 금융결제원 |

Recorded the largest num. of customers/users in Korea mobile security market

**Over 700,000**

JIRANSECURITY

# Case Study

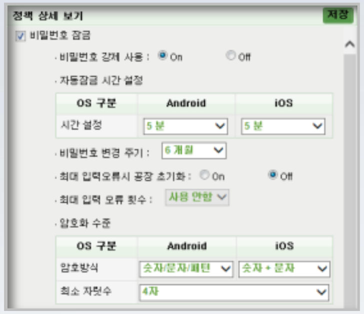
MOBILEKEEPER

# Case #1. Device Security and Measures for Lost Devices: MDM

Device security policies are applied in a variety of ways depending on company operation policies. Device restriction policies are applied when using business or work apps, and during access control. Remote control functions to manage lost devices (such as location confirmation, data deletion, etc.) are authorized only to the user in order to protect personal information.

## Device Security Set Up

Password policies



정책 상세 보기 [저장]

☑ 비밀번호 잠금

· 비밀번호 강제 사용 : ● On ○ Off

· 자동잠금 시간 설정

| OS 구분 | Android | iOS |
|---|---|---|
| 시간 설정 | 5 분 | 5 분 |

· 비밀번호 변경 주기 : 6 개월

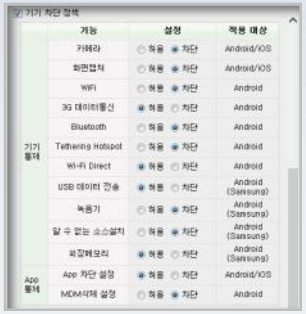
· 최대 입력오류시 공장 초기화 : ○ On ● Off

· 최대 입력 오류 횟수 : 사용 안함

· 암호화 수준

| OS 구분 | Android | iOS |
|---|---|---|
| 암호방식 | 숫자/문자/패턴 | 숫자 + 문자 |
| 최소 자릿수 | 4자 | |

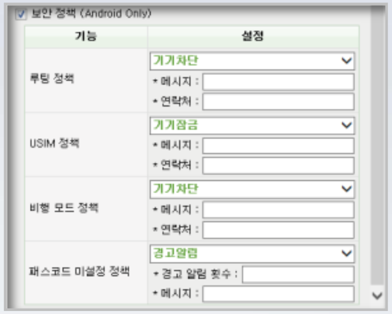
Device regulation policies



☑ 기기 차단 정책

| | 기능 | 설정 | 적용 대상 |
|---|---|---|---|
| 기기 통제 | 카메라 | ○ 허용 ● 차단 | Android/IOS |
| | 화면캡처 | ○ 허용 ● 차단 | Android/IOS |
| | WIFI | ○ 허용 ● 차단 | Android |
| | 3G 데이터통신 | ● 허용 ○ 차단 | Android |
| | Bluetooth | ○ 허용 ● 차단 | Android |
| | Tethering Hotspot | ○ 허용 ● 차단 | Android |
| | Wi-Fi Direct | ● 허용 ○ 차단 | Android |
| | USB 데이터 전송 | ● 허용 ○ 차단 | Android (Samsung) |
| | 녹음기 | ○ 허용 ● 차단 | Android (Samsung) |
| | 알 수 없는 소스설치 | ○ 허용 ● 차단 | Android (Samsung) |
| | 외장메모리 | ● 허용 ○ 차단 | Android (Samsung) |
| App 통제 | App 차단 설정 | ● 허용 ○ 차단 | Android/IOS |
| | MDM삭제 설정 | ○ 허용 ● 차단 | Android |

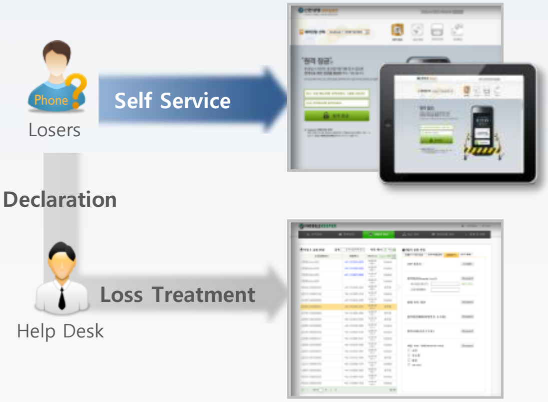
Device security policies



☑ 보안 정책 (Android Only)

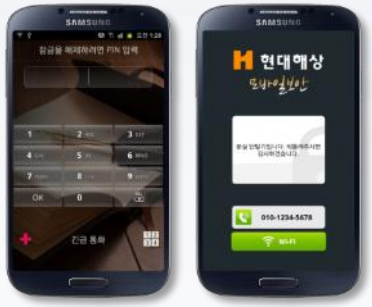
| 기능 | 설정 |
|---|---|
| 루팅 정책 | 기기차단<br>* 메시지 :<br>* 연락처 : |
| USIM 정책 | 기기잠금<br>* 메시지 :<br>* 연락처 : |
| 비행 모드 정책 | 기기차단<br>* 메시지 :<br>* 연락처 : |
| 패스코드 미설정 정책 | 경고알림<br>* 경고 알림 횟수 :<br>* 메시지 : |

## Measures for Lost/Stolen Devices



Remote lock

Request return



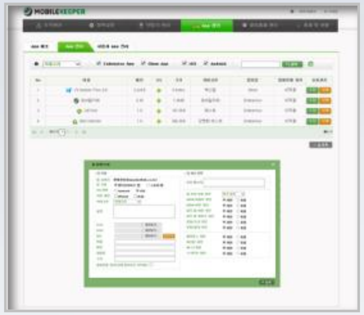
Confirm current location

# Case #2. Distribution/Management of Work Apps: MAM

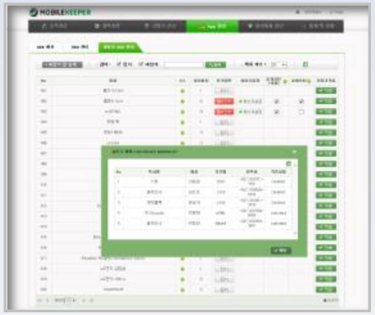
As mobile offices become more commonplace, MAM makes registering/distributing/updating work apps easier. This system is able to collect current information related to user and group installation/update, and more. MOBILEKEEPER's internal company App Store and management tools enable effective distribution and management of work apps and user apps.

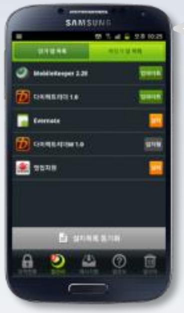
## App Distribution and Management

Set up App distribution policies



Manage user apps

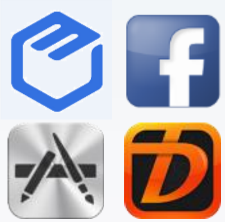




App Store

Download
Install
Update

## App Distribution Management Process



App Enrollment

Distribution target/set up security

App Management Center

Redistribute(Push)

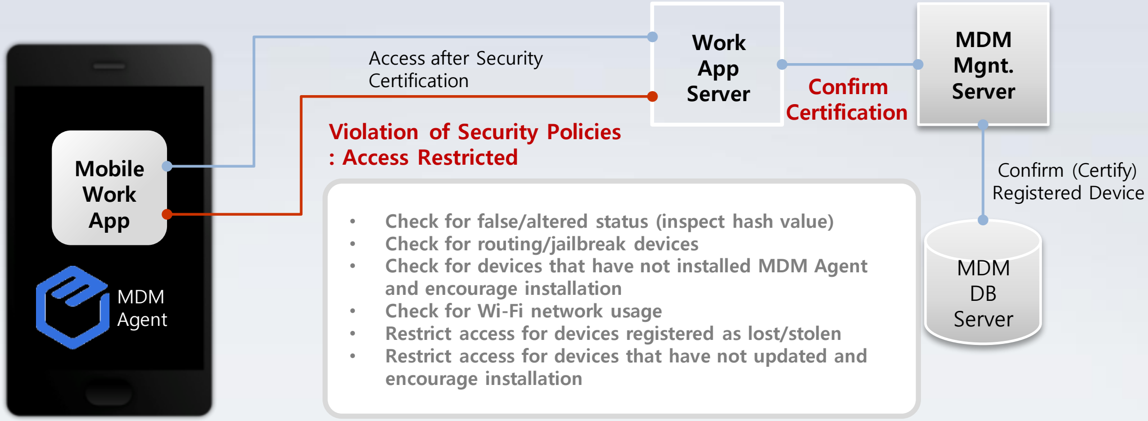
installation situation

redistribute/update

# Case #3. Work App Security: MAS

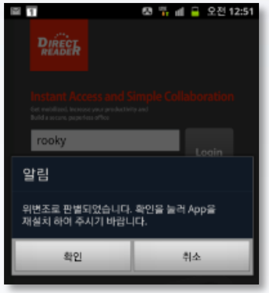
The mobile office system emphasizes work efficiency but is very vulnerable to security threats. As such, information leaks can occur in various ways and simple authorization methods (ID/PW) are lacking in security strength. MOBILEKEEPER (MDM), increases user security of mobile offices and minimizes user dissatisfaction through App certification, device certification, screen capture restrictions, and more.

## 업무 App 인증 및 보안


Mobile Work App
MDM Agent
Access after Security Certification
Violation of Security Policies : Access Restricted
Work App Server
Confirm Certification
MDM Mgnt. Server
Confirm (Certify) Registered Device
MDM DB Server

- Check for false/altered status (inspect hash value)
- Check for routing/jailbreak devices
- Check for devices that have not installed MDM Agent and encourage installation
- Check for Wi-Fi network usage
- Restrict access for devices registered as lost/stolen
- Restrict access for devices that have not updated and encourage installation

Restrict for false/altered status



Instant Access and Simple Collaboration

Get mobilized, Increase your productivity and
Build a secure, paperless office

rooky

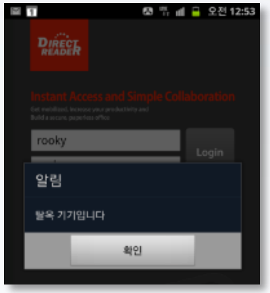
Login

알림

위변조로 판별되었습니다. 확인을 눌러 App을
재설치 하여 주시기 바랍니다.

확인 취소

Restrict access for
routing/jailbreak devices



Instant Access and Simple Collaboration

Get mobilized, Increase your productivity and
Build a secure, paperless office

rooky

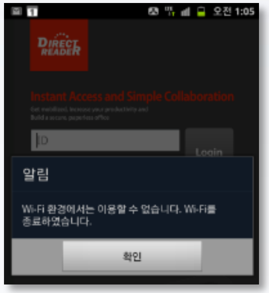
Login

알림

탈옥 기기입니다

확인

Restrict access for Wi-Fi



Instant Access and Simple Collaboration

Get mobilized, Increase your productivity and
Build a secure, paperless office

ID

Login

알림

Wi-Fi 환경에서는 이용할 수 없습니다. Wi-Fi를
종료하였습니다.

확인

# Case #4. Mobile Device Access Control: MDAC

To prevent vital work data from being exposed, restricting camera/recording/Bluetooth functions and unauthorized app usage is necessary within the company. MDAC reduces the hassle of the existing sticker method, and automatically blocks a variety of smartphone functions and apps to prevent information leaks within a security area. Operational scenarios include GPS based/wireless network based/linking to physical security systems and more, with linking to a physical security system being the most general.

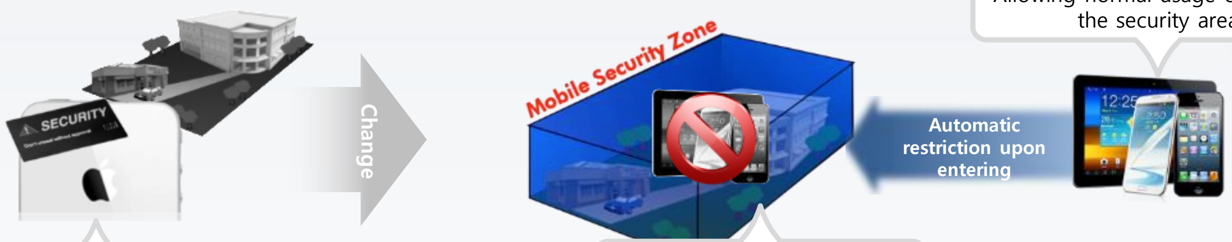
## Access Control Management

Security area/set up policies

access control records/regulation

confirming restriction status

## Access Control Concept

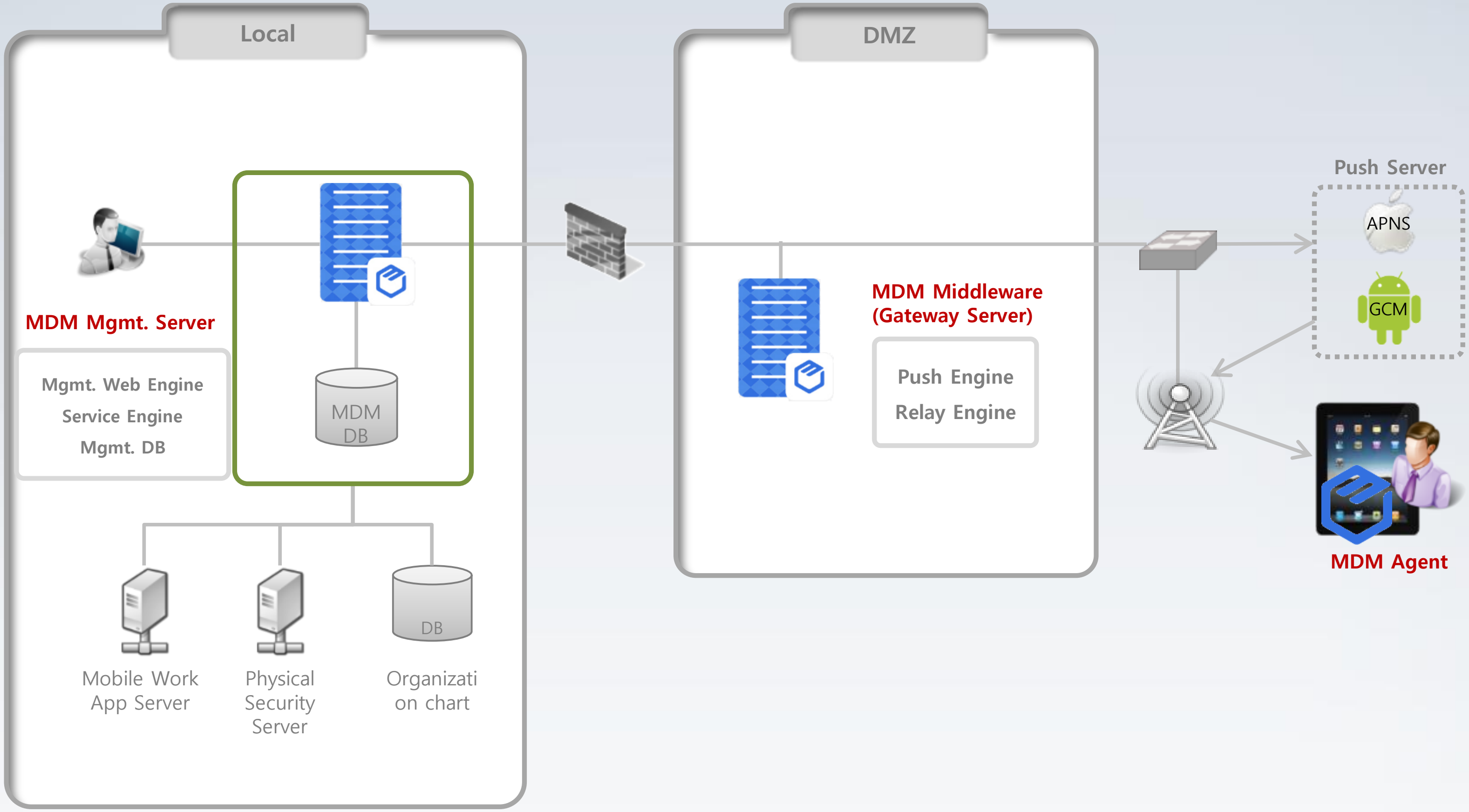


Applying stickers

Restricting devices within a security area

Allowing normal usage outside of the security area

# Standard System Architecture



# Company Overview

MOBILEKEEPER

# Company Overview

## Korea No1. Security Vendor

JiranSecurity has grown its business for 20 years as the Security Div. of Jiransoft, a leading security solution vendor in Korea, and has been separated from the parent company in January 2014. JiranSecurity is making efforts for research and development of more specialized security products in order to be a 100-year-lasting security company based on trust and communications with customers.

| | |
|---|---|
| **Company** | JiranSecurity Co., Ltd. |
| **Foundation** | January 1, 2014<br>(separated from parent company Jiransoft Security Division) |
| **Represen-tative & CEO** | Doo Shik, Yoon |
| **Business Area** | Security solution development |
| **Major Product & Service** | Mail security, Document security  and Mobile security |
| **No. of Employees** | 115 employees (As of January 2016) |
| **Capital** | ₩ 1.1 billion |
| **Sales** | ₩ 15.5 billion (as of 2015) |
| **Location** | (Seoul) (5th Floor, Shinsa S&G) 542, Yeoksam-ro, Gangnam-gu, Seoul<br>(Daejeon) 604, Hanshin S Mecca 1359, Gwanpyeong-dong, Yuseong-gu, Daejeon |
| **Webpages** | http://www.jiransecurity.com |

JIRANSECURITY

# Company History

## Product Launch

| | |
|---|---|
| 2016 | MAILSAFER |
| 2015 | JVAULT+<br>OfficeHARDPRIVACY<br>SPAMSNIPER APT<br>OfficeHARDCLOUD |
| 2014 | Founded JiranSecurity Co., Ltd.<br>**(separated from Jiransoft Security Div.)** |
| 2013 | DocStream |
| 2011 | DirectReader<br>MOBILEKEEPER |
| 2010 | J-VAULT |
| 2009 | MAILSCREEN |
| 2004 | OfficeHARD |
| 2002 | SPAMSNIPER |
| 1996 | Founded Jiransoft Co., Ltd. |

## Certification by Line-up Product

2015 **Jun : launched J-VAULT+**

**Apr : launched SpamSniper APT**

Jan : formed a partnership with FireEye Korea

2011 Jun : acquired GS certificate for J-VAULT, MailScreen

2010 **Sep : launched J-VAULT**

2009 Dec : acquired CC certificate for SpamSniper CC

**Apr : launched MailScreen**

2007 Jun : SpamSniper won grand prize for the New SW product Award (Ministry of Information and Communication)

2002 **Oct : launched SpamSniper**

2015 **Jun : launched OfficeHard PRIVACY**

**Jan : launched OfficeHard CLOUD**

2014 Apr : acquired GS certificate for DirectReader

2013 Dec : OfficeHard won excellent prize for TTA Test Certification Award

**Sep : launched DocStream for corporate use**

Aug : acquired GS certificate for OfficeHard VEX

**Apr : launched OfficeHard VEX**

2011 **May : launched DirectReader**

2009 Aug : OfficeHard won grand prize for the Japan Monotsukuri Award

2004 **Nov : launched OfficeHard**

2016 Jan : launched MailSafer

2014 Nov : MobileKeeper won the Ministry of Trade, Industry & Energy's prize for the Korea Technology Awards

Jul : acquired first CC certificate for MobileKeeper as MDM

2013 Nov : MobileKeeper won the Korea Economic Daily Representative's Prize for the 13th Mobile Technology Award

Jul : MobileKeeper passed Security Conformance of the National Intelligence Service

**2012** Oct : acquired the first GS certificate for MobileKeeper MDM Solution

**2011** **Sep : launched MobileKeeper 2.0**