

모바일 기기 홍수로부터 귀사의 정보를 지키는 방안

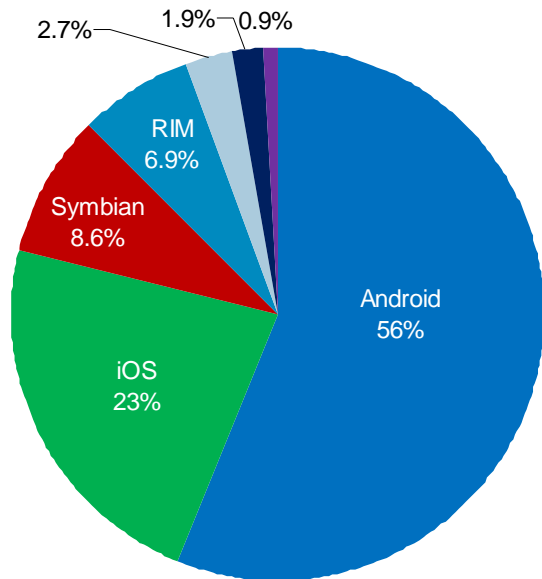
IBM Endpoint Manager for Mobile Devices

정종훈 부장
티볼리 사업부, 한국IBM



Google, Apple 및 기업 직원들이 업계의 성공 주역이 된 반면 Nokia, RIM 및 기타 IT 분야들은 여러 도전 과제에 직면해 있습니다

2012년 1사분기의 OS별 최종 사용자를 대상으로 한 스마트폰 판매 세계 점유율



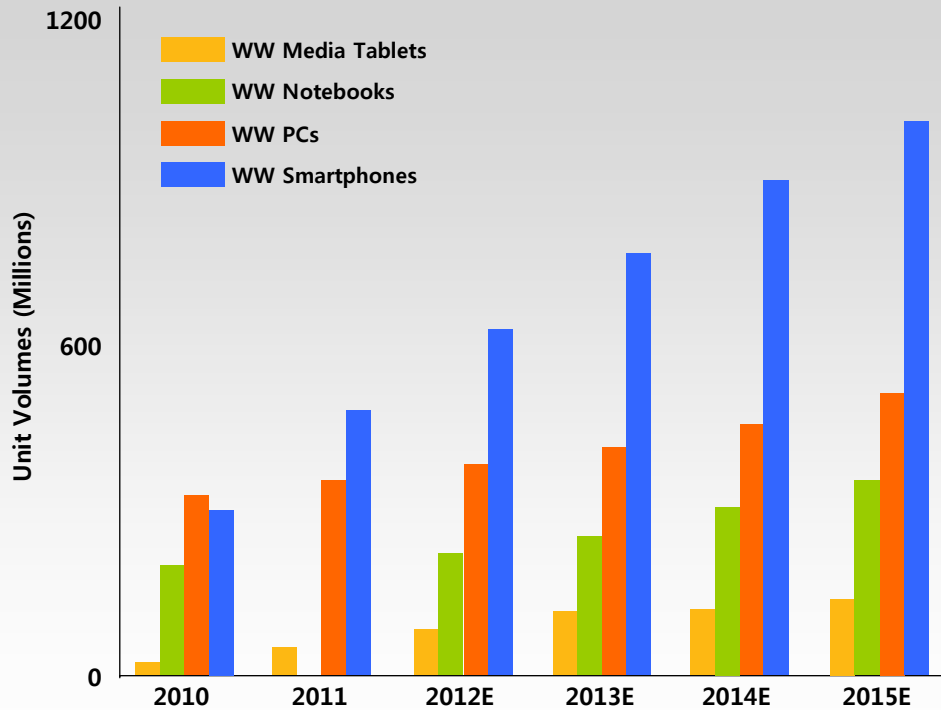
■ Android ■ iOS ■ Symbian ■ RIM ■ Bada ■ Microsoft ■ Others

- Android의 점유율은 1.5년 만에 25%에서 56%로 2배 이상 증가
- Apple과 Google의 소비자 지향적 디바이스들은 빠르게 기업 시장에 진출했지만, 대부분은 관리되지 못하고 있음

출처: Gartner 2012년, 미디어 태블릿은 포함되지 않음

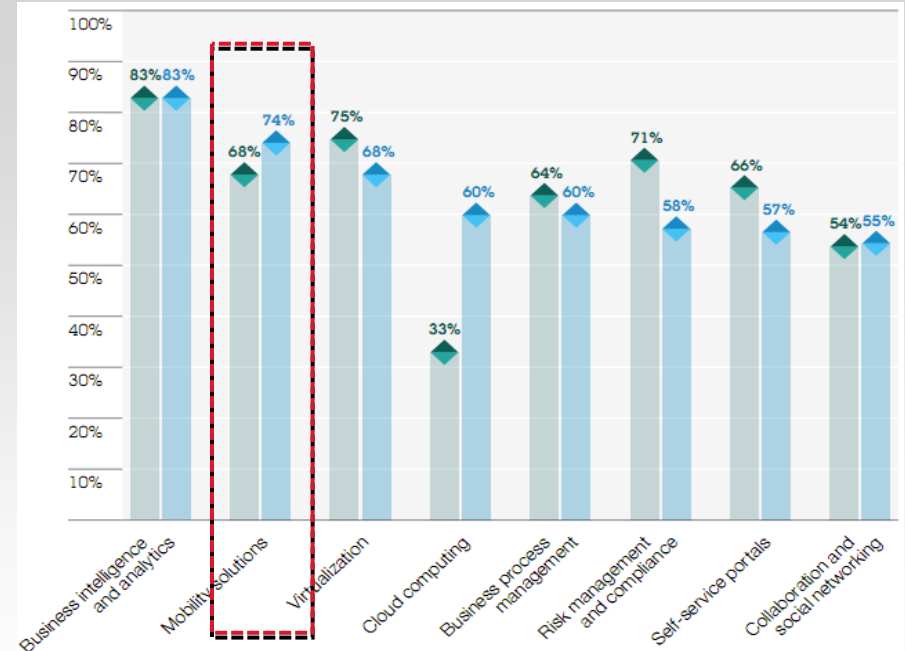
기업의 투자우선순위

인터넷 연결 디바이스의 증가 트렌드



Source: Wells Fargo Securities, January 23, 2012
 "Fostering the People: The Shift to Engagement Apps"

모바일 및 클라우드가 최우선순위



¹ 2011 IBM Global CIO Study
² Wireless Industry News, August 26, 2010
³ 2011 Economist

90%의 기업들이 2014년까지 개인이 소유한 모바일 디바이스에서 기업용 애플리케이션을 지원할 예정입니다 (BYOD)

모바일 환경의 라이프사이클

- 최종 사용자 중심의 다양한 요구
- 모바일 애플리케이션에 대한 사용자의 높은 기대 수준
- 모바일 애플리케이션에 대한 베스트 프랙티스 부재
- 디자인 단계에서부터 사용자 및 관련자 중심의 직접적인 참여
- 모바일 디바이스 별 상이한 구조로 인한 애플리케이션 포팅의 어려움
- 모바일 디바이스와 플랫폼에 대한 긴밀한 협력 관계
- 대상 장비, 플랫폼, 통신사 등의 다양성으로 인한 관리의 어려움
- 빠른 속도로 진화하는 모바일 관련 기술
- 애플리케이션 업데이트에 대한 신속한 반영



모바일 환경에서 고려해야 할 새로운 도전 과제들

모바일 디바이스들은 기존 도전과제의 범위를 확장하며, 기존의 관리 패러다임 전반을 흔드는 독특한 것들을 요구합니다

도전과제	고려사항
직원이 소유한 모바일 디바이스의 성장 범위를 지원 및 보호하기 위한 직원 및 고위 경영진의 압박	<ul style="list-style-type: none"> • 이러한 디바이스를 누가 관리하는가? PC 팀? 메시징 팀? 보안 팀? • 직원 소유의 디바이스로부터 기업 데이터만 삭제하려면 어떻게 해야 하는가? • 너무 많은 디바이스 플랫폼들을 다룰 때 발생하는 급격한 비용 폭증
기존의 시스템 관리 패러다임을 혼란스럽게 만드는 "폐쇄적 구조"의 모바일 OS	<ul style="list-style-type: none"> • iOS는 Android와는 다르게 처리되며, 이는 BlackBerry와 다르다 • 그러면 애플리케이션을 어떻게 배포할 것인가?
급변하는 디바이스/OS/애플리케이션/사용자 태도를 어떻게 다룰 것인가?	<ul style="list-style-type: none"> • 어떤 디바이스들이 탈옥되거나 루팅되었는가? • 어떠한 버전의 Android가 기업 환경에 최적화(Enterprise-Ready)되어 있는가?
회사에서 관리할 디바이스가 증가하고 있는데 관리 포인트가 많아져 솔루션 유지에 대한 비용 압박	<ul style="list-style-type: none"> • PC, 서버, 모바일 등 다양한 디바이스에 대한 관리가 각각 필요할 뿐만 아니라 에너지 비용 상승에 따른 에너지 관리, 소프트웨어 관리, 보안 관리가 필요 • 모든 걸 갖추기 위해서는 몇 개의 관리 솔루션이 필요한가?

모바일 디바이스 관리(MDM) 솔루션 구축을 위한 사전 고려사항

모바일 기능적인 고려사항

도전과제	고려사항
직원 소유의 자산과 기업 소유의 자산을 어떻게 관리할 것인가?	<ul style="list-style-type: none"> • 기업에 이메일 기반의 관리(소극적 개입) 또는 정교한 에이전트 기반의 관리를 사용할 수 있는 유연성 제공
분실하거나 도난 당한 디바이스를 어떻게 처리할 것인가?	<ul style="list-style-type: none"> • 비밀번호 정책 제어(PIN 길이, 타임아웃, 로그인 실패 후 삭제 등) 및 원격 삭제
디바이스 내 민감한 기업 데이터를 어떻게 처리할 것인가?	<ul style="list-style-type: none"> • 직원이 퇴사할 경우, 디바이스 암호화 및 기업 데이터의 선택적 삭제 지원
디바이스/OS/애플리케이션/사용자 태도의 급격한 변화를 어떻게 처리할 것인가?	<ul style="list-style-type: none"> • 신속한 업데이트 및 새로운 솔루션 제공을 위해 클라우드 기반의 기술 모델과 결합된 유연한 Endpoint Manager 플랫폼
외부 방문자의 모바일 기기를 통제할 수 없을까?	<ul style="list-style-type: none"> • 외부 방문자 모바일 기기의 카메라, 음성녹음, 메일 등을 원격에서 통제

모바일 디바이스 관리(MDM) 솔루션 구축을 위한 사전 고려사항

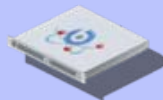
비용 및 관리적인 고려사항

도전과제	고려사항
<p>여러 디바이스를 처리할 경우 발생하는 IT 비용 폭증을 어떻게 억제할 것인가?</p>	<ul style="list-style-type: none"> 공유 인프라를 통해 서버/데스크톱/노트북/ 모바일 디바이스 등의 모든 디바이스를 관리하기 위한 단일 플랫폼
<p>분산환경으로 구성 시 관리 서버가 많아져 IT 비용 증가</p>	<ul style="list-style-type: none"> 분산 환경인 경우라도 단일 서버에서 관리할 수 있는 아키텍처 고려
<p>관리 대상이 많아져 관리 서버가 증가 되는 문제점</p>	<ul style="list-style-type: none"> 관리 대상이 많아지더라도 단일 서버에서 관리할 수 있는 아키텍처 고려
<p>PC에 여러 에이전트가 설치되어 PC 성능이 저하되는데 단일 에이전트로 통합할 수 있을까?</p>	<ul style="list-style-type: none"> TEM은 PC 라이프사이클 관리, 보안 관리, 소프트웨어 관리 등 단일 에이전트로 동작하여 PC 부하를 줄일 수 아키텍처
<p>필요한 정책의 구현 비용이 지속적으로 발생하여 유지보수 비용의 증가를 줄일 수 있을까?</p>	<ul style="list-style-type: none"> 필요한 정책의 구현을 위해서 도입된 제품의 기능 수정이나 추가 개발이 발생하지 않고 추가 정책을 반영할 수 있는 아키텍처 고려

PC와 모바일 디바이스들은 동일한 관리 요건들이 많습니다

기존 엔드포인트 관리

- OS 프로비저닝
- 패치
- 전원 관리
- 바이러스 예방 관리



모바일 디바이스 관리

- 디바이스 제거
- 위치 정보
- 탈옥/루팅 감지
- 기업 앱스토어
- 셀프 서비스 포털



- 디바이스 인벤토리
- 보안 정책 관리
- 애플리케이션 관리
- 디바이스 구성 (VPN/이메일/Wi-Fi)
- 암호화 관리
- 로밍 디바이스 지원
- 내부 시스템과 통합
- 확장성/보안 솔루션
- 손쉬운 배치
- 다양한 OS 지원
- 통합된 인프라

IBM Endpoint Manager는 모든 기업 디바이스를 위한 통합 시스템과 보안 관리 솔루션을 제공합니다



유닉스/리눅스 서버	Android/iOS/Symbian/ 윈도우 폰 디바이스
윈도우 및 Mac 데스크탑/노트북	윈도우 모바일/ 키오스크/POS 디바이스

보다 많은 수의 디바이스를

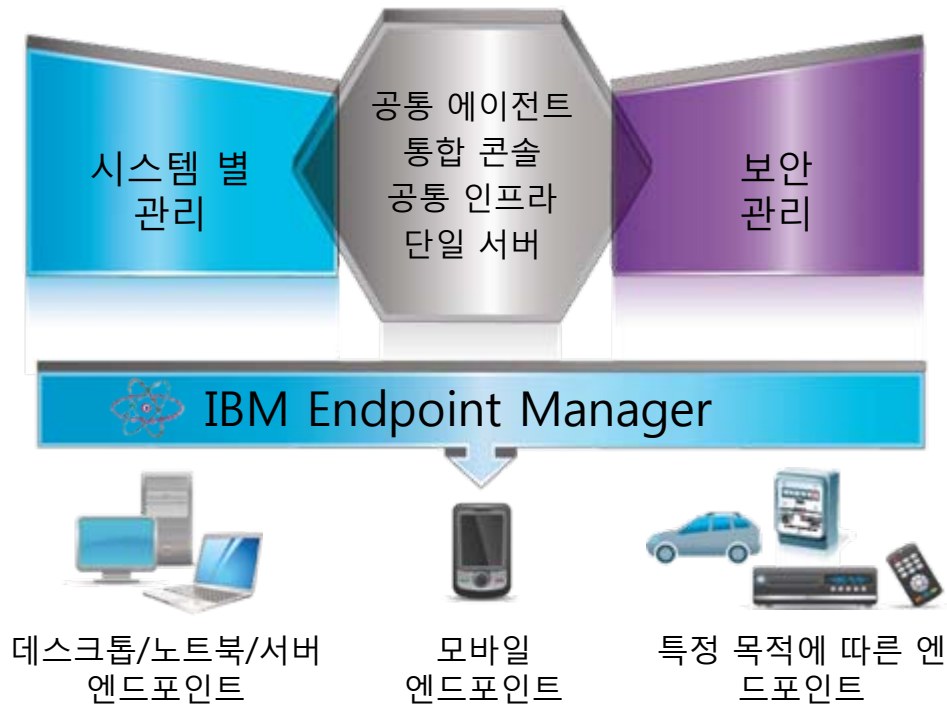
그리고 보다 많은 기능을 지원합니다

디바이스 인벤토리	엔드포인트 보호	소프트웨어 사용 분석
패치 관리	전원 관리	보안 구성 관리
구성 관리	원격 제어	OS 배포
		모바일 디바이스 관리

IBM Endpoint Manager는 모든 기업 디바이스를 위한 통합 시스템과 보안 관리 솔루션을 제공합니다

디바이스의 유형, 운영체제에 구애 받지 않는 일원화된 관리/보안 능력을 제공하는 일원화된 Total Endpoint 솔루션

Managed = Secure



TEM 제품의 특징점

- 모든 종류의 엔터프라이즈 디바이스에 대한 일원화된 시스템/애플리케이션, 파워, 보안 관리 솔루션
- 고객 환경으로의 실시간에 가까운 기능 업데이트와 보고
- 모바일 디바이스 용 정보 수집 시스템(CMDB, SIEM 등)과의 연동을 통한 확장 플랫폼
- iOS, Android, Symbian, Windows Phone 등을 위한 진보적인 모바일 디바이스 관리 기능
- 단일 관리서버에서 25만대의 디바이스 관리
- Fixlet이란 기능으로 손쉽게 정책을 정의하고 구현
- Relay서버 기능으로 별도의 관리 서버를 필요로 하지 않음
- 짧은 시간 안에 구현 가능

Endpoint Manager는 모바일 디바이스들을 어떻게 관리하는가?

- Apple의 MDM API를 통한 iOS상의 고급 관리*



- TEM 에이전트를 통한 Android상의 고급 관리



- Exchange(ActiveSync) 및 Lotus Traveler(IBM Sync)를 통한 이메일 기반의 관리

- iOS
- Android
- 윈도우 폰
- 윈도우 모바일
- Symbian

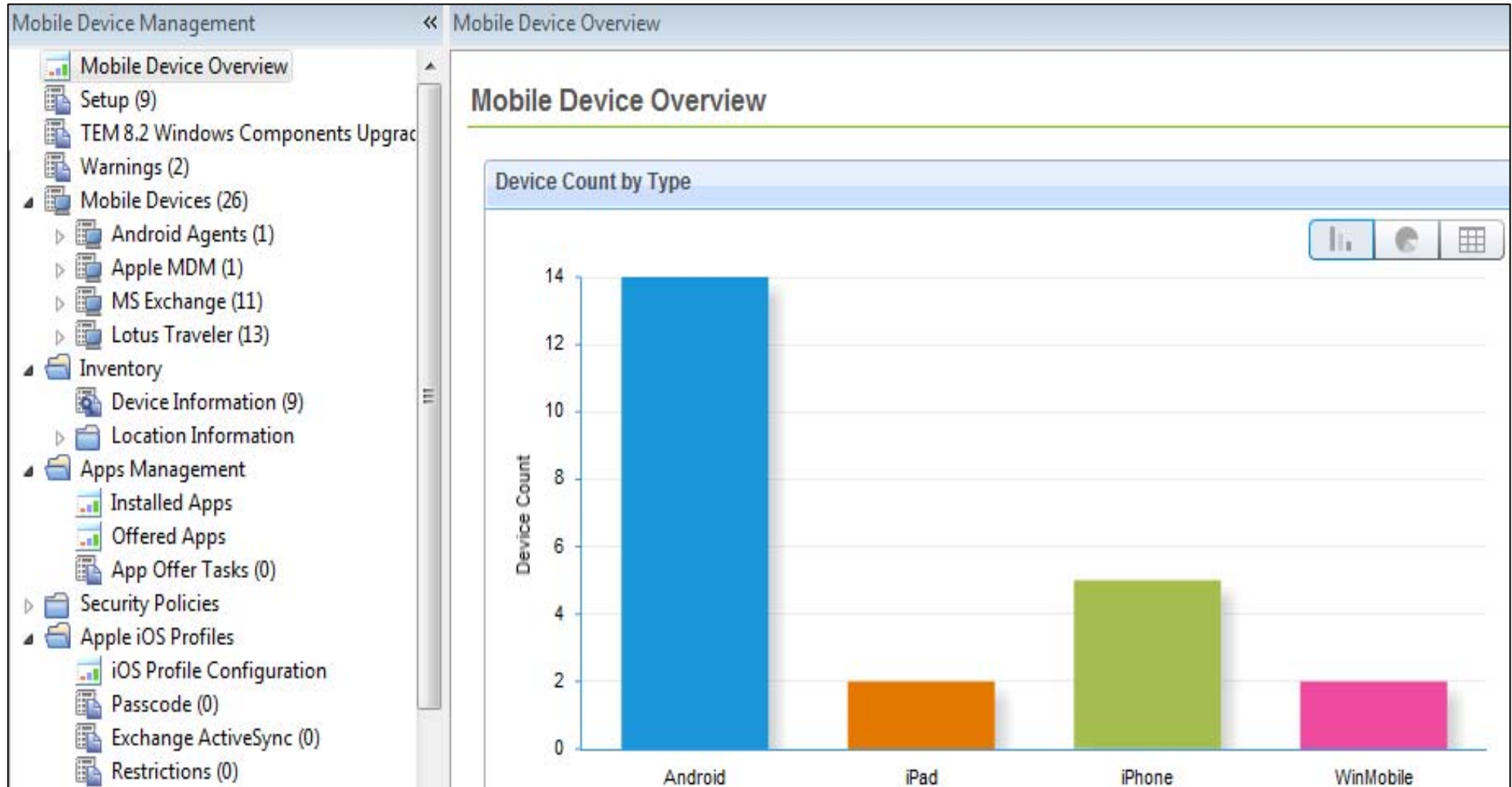


* MDM 벤더에게 제공하는 기능에 대한 자세한 내용은 Apple의 MDM 문서인 http://images.apple.com/iphone/business/docs/iOS_MDM.pdf에서 확인하실 수 있습니다.

TEM for MDM 기능 개요

카테고리	IBM Endpoint Manager 기능
플랫폼 지원	Apple iOS, Google Android, Nokia Symbian, 윈도우 폰, 윈도우 모바일
관리 작업	선택적 삭제, 완전 삭제, 이메일 액세스 거부, 원격 잠금, 사용자 알림
애플리케이션 관리	애플리케이션 인벤토리, 기업 앱스토어, 화이트리스트, 블랙리스트
정책 및 보안 관리	비밀번호 정책, 디바이스 암호화, 탈옥 및 루팅 감지
위치 서비스	디바이스 추적 후 지도에 위치 표시
기업 액세스 관리	이메일 설정, VPN, Wi-Fi

모바일 디바이스 대시보드를 위한 Endpoint Manager



모바일 OS 전반에 걸친 비밀번호 정책의 통합 보고를 통해 관리자가 호환되지 않는 디바이스들을 쉽게 식별할 수 있습니다

Analysis: Password Settings

View as list

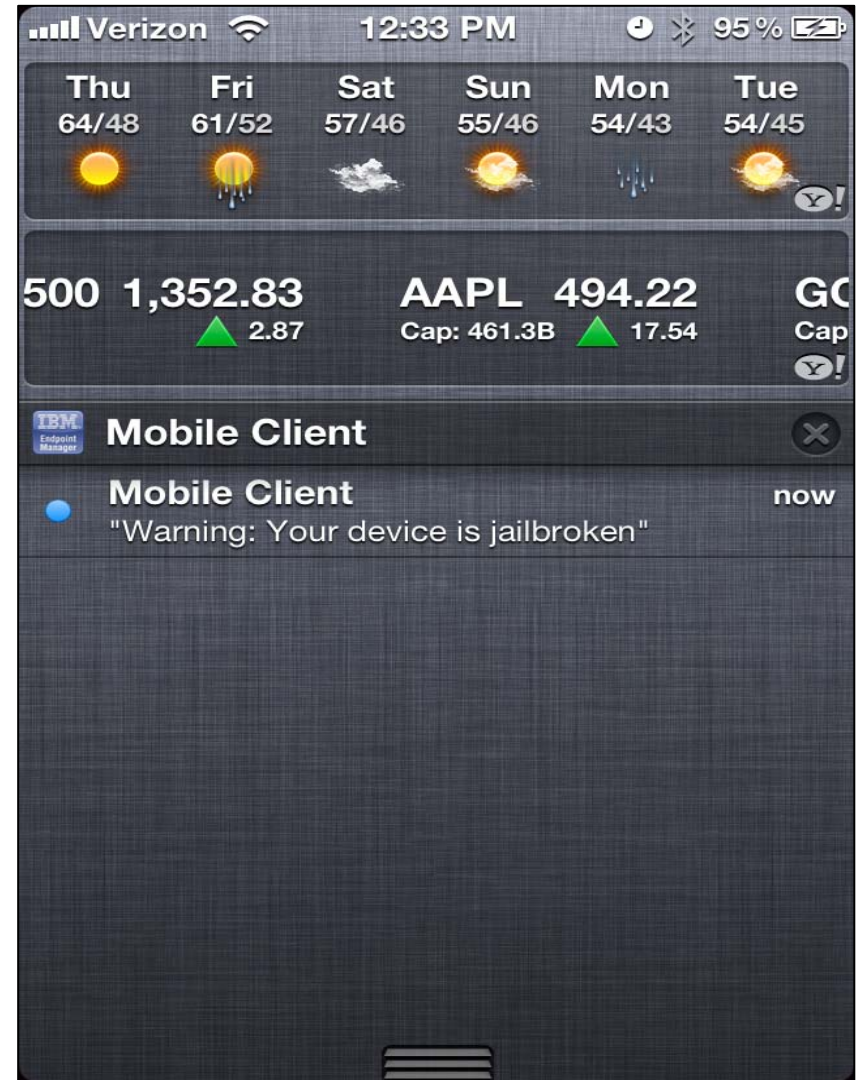
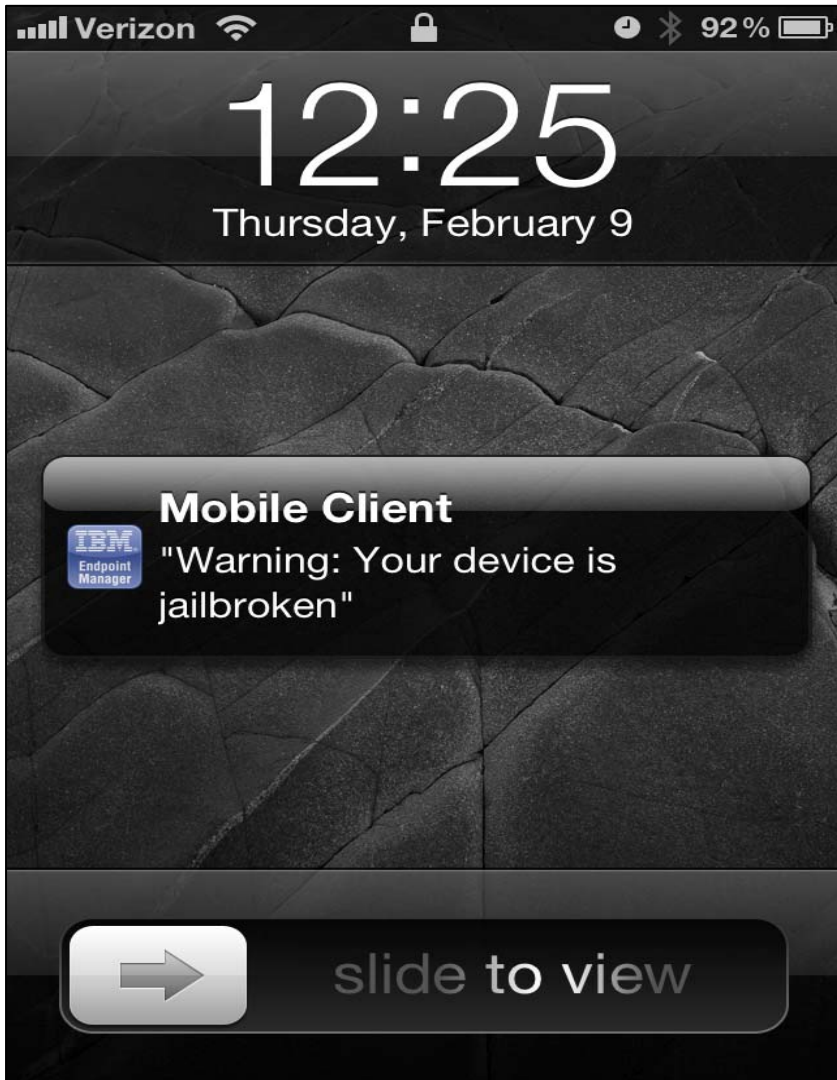
Computer Name	OS	Password Enabled	Password Compliant	Password Leng...	Require Alphan...	In...
358920045232227	Android (2.3.3)	False	True	0	False	0
0000000000000000	Android (2.3.3)	False	True	0	<undefined>	<u
FB61B605A0F74...	Android (2.3.4)	False	True	0	False	0
99000033060984	Android (2.3.4)	False	True	0	<undefined>	<u
99000052220657	Android (3.2.1)	False	True	0	<undefined>	<u
jniskala@us.ibm...	Android (4.0.1)	False	True	0	<undefined>	<u
Guille's iFoca	Apple iOS 4.3.5	True	True	8	True	30
Jim's iPad	Apple iOS 5.0.1	False	True	n/a	False	n/a
Ben's iPhone4	Apple iOS 5.0.1	True	True	8	True	5
Kelly Gibson's iP...	Apple iOS 5.0.1	True	True	4	False	5
Ben's iPad	Apple iOS 5.0.1	True	True	8	True	15
ApplJ3049UUXA90	iOS 4.3.3	False	False	n/a	False	n/a
ApplJ3049UUXA90	iOS 4.3.5	False	False	n/a	False	n/a
Appl7R049JM0A45	iOS 4.3.5	False	False	n/a	False	n/a
ApplV50S1FERA90	iOS 4.3.5	False	False	n/a	False	n/a
ApplV50S1FERA90	iOS 4.3.5	False	False	n/a	False	n/a
Appl7W05224EA45	iOS 4.3.5	False	False	n/a	False	n/a
Appl7R049JM0A45	iOS 4.3.5	False	False	n/a	False	n/a
Appl7W05224EA45	iOS 4.3.5	False	False	n/a	False	n/a

단일 디바이스 보기를 통해 관리자 및 헬프데스크 담당자는 디바이스 세부 정보를 쉽게 확인하며 필요한 조치를 취할 수 있습니다

The screenshot displays the Mobile Enterprise management interface. On the left, a sidebar shows a 'VIEW DEVICE LOG' button. The main area is divided into several panels:

- Android Device Overview:**
 - Device Name:** 0000000000000000
 - User Name:** <none>
 - Operating System:** Android (2.3.3)
 - Model:** sdk
 - Status:** This device has been rooted (indicated by a yellow warning banner).
 - Report Details:**
 - Last Report Time: Dec 01, 2011 12:32:14 PM
 - Manufacturer: unknown
 - Carrier: generic
 - LastSyncTime: n/a
 - Phone Number: n/a
 - Agent Version: 8.2.867.0
 - Data Source: Native
- Device Management Panel:**
 - Buttons: Device Wipe (Apply), Clear Passcode (Apply)
- iPhone Device Overview:**
 - Device Name:** 7R049JM0A4S
 - Operating System:** Apple iOS 4.3.5 (iPhone3,1)
 - Model:** iPhone
 - Report Details:**
 - Last Report Time: Oct 31, 2011 8:30:10 PM
 - Manufacturer: Apple
 - Carrier: AT&T
 - LastSyncTime: 21 Oct 2011 09:00:52 +0000
 - Phone Number: +15106040334
 - Agent Version: 0.1.2.0
 - Data Source: Apple MDM
- Device Details - Android / Apple iOS:**
 - Manufacturer: Apple
 - Last Server Communication: 21 Oct 2011 09:00:52 +0000
 - Carrier: AT&T
 - Model: iPhone
 - Name: MDM's iPhone
 - Model ID: MC318LL
 - GUID / IMEI: 01 253500 233561 1
 - Phone Number: +15106040334
 - UUID / UDID: bfeee8da93696e9ed5971470f8338fa0b8e70c5d
- Storage Information:** (Section header visible)

iOS의 탈옥 알림 기능



Android 및 iOS 디바이스에 설치된 애플리케이션 보기

Apps Management - Installed Apps

This dashboard reports back the applications that are installed on devices.

Android Apps | Apple Apps

Apps List

Tag checked as: --- Clear tag Search

<input type="checkbox"/>	Display Name	Tag	1 ▼	Package Name	Description	API Versions	Computer Count
<input type="checkbox"/>	TEM Agent	Enterprise		com.bigfix.engine	Tivoli Endpoint Manager 8.2	8	1
<input type="checkbox"/>	è°-æ-Œæc¼éÿ*è¼*ã...¥æ	Blacklisted		com.android.inputmethod.p		10	1
<input type="checkbox"/>	TTS Service			android.tts		10	1
<input type="checkbox"/>	Contacts			com.android.contacts		10	1
<input type="checkbox"/>	Fallback			com.android.fallback		10	1
<input type="checkbox"/>	Calculator			com.android.calculator2		10	1
<input type="checkbox"/>	Custom Locale			com.android.customlocale		10	1
<input type="checkbox"/>	Settings Storage			com.android.providers.sett		10	1
<input type="checkbox"/>	Search			com.android.quicksearchbc		10	1
<input type="checkbox"/>	HTML Viewer			com.android.htmlviewer		10	1
<input type="checkbox"/>	Camera			com.android.camera		10	1
<input type="checkbox"/>	OpenWnn			jp.co.omronsoft.openwnn		10	1
<input type="checkbox"/>	DRM Protected Content Sto			com.android.providers.drm		10	1
<input type="checkbox"/>	Dev Tools			com.android.development		10	1
<input type="checkbox"/>	Pico TTS			com.svox.pico		10	1
<input type="checkbox"/>	Search Applications Provid			com.android.providers.app		10	1
<input type="checkbox"/>	Desktop Access Util...			com.android.desktop...		10	1

사용자 친화적인 iOS 프로파일 구성 마법사는 Apple의 MDM API를 통해 모든 구성 기능을 보여줍니다

Profile Details

Identity

Passcode

Require passcode on device
Enforce the use of a passcode before using device

- Allow simple value**
Permit the use of repeating, ascending, and descending character sequences
- Require alphanumeric value**
Require passcodes to contain at least one letter

Minimum password length
Smallest number of passcode characters allowed

Minimum number of complex characters
Smallest number of non-alphanumeric characters allowed

Maximum passcode age (1-730 days, or none)
Days after which passcode must be changed

Auto-Lock (1-5) minutes, or 0 for none
Device automatically locks when time period elapses

Passcode history (1-50 passcodes, or 0 for none)
The number of unique passcodes required before reuse

Grace period for device lock
Amount of time device can be locked without prompting for passcode on unlock

Maximum number of failed attempts
Number of passcode entry attempts allowed before all data on device will be erased

Exit New Profile Mode

Save Profile

Endpoint Manager 콘솔을 통해 Exchange 정책을 직접 구성하고 배치할 수 있습니다

Exchange ActiveSync Mailbox Policy - Configuration

1) Choose a Client Access Mailbox Policy

Currently Enforced Policies

Name	Non-Provisionable ...	Device Password R...	Default	Creation Time	Modification Time	Device Count
Default	True	False	True	Thu Jul 21 12:23:48 GMT	Tue Sep 27 10:06:25 GM	5
Exchange Policy Example	True	True	False	Thu Jul 28 02:42:38 GMT	Tue Aug 9 04:18:45 GMT	3
Exchange Policy Example	False	False	False	Tue Aug 30 04:18:18 GM	Tue Aug 30 05:12:33 GM	1

2) Edit Policy Details

General Password Sync Settings Device **Device Applications** Other

- Allow removable storage
- Allow Camera
- Allow Wi-Fi
- Allow infrared
- Allow Internet sharing from device
- Allow remote desktop from device
- Allow desktop synchronization
- Allow Bluetooth

Endpoint Manager 콘솔에서 Lotus Traveler 정책을 직접 구성하고 배치할 수 있습니다

Lotus Traveler Device Security Settings - Configuration

Windows Mobile | **Nokia** | Apple | Android

Device Security	Violation Action
<input checked="" type="checkbox"/> Require device password	Enforce
<input type="checkbox"/> Prohibit ascending, descending and repeating sequences	
<input type="checkbox"/> Require alphanumeric value	
Minimum password length:	8
Minimum number of complex characters:	0
Auto lock period (maximum):	30 minutes
Password expiration period:	90 days
Password history count:	0
<input type="checkbox"/> Wrong passwords before wiping device	7
<input type="checkbox"/> Prohibit unencrypted devices	
<input checked="" type="checkbox"/> Prohibit camera	Enforce
<input checked="" type="checkbox"/> Prohibit devices incapable of security enablement	Enforce

정책적으로 이메일 액세스를 거부할 수 있습니다

Description

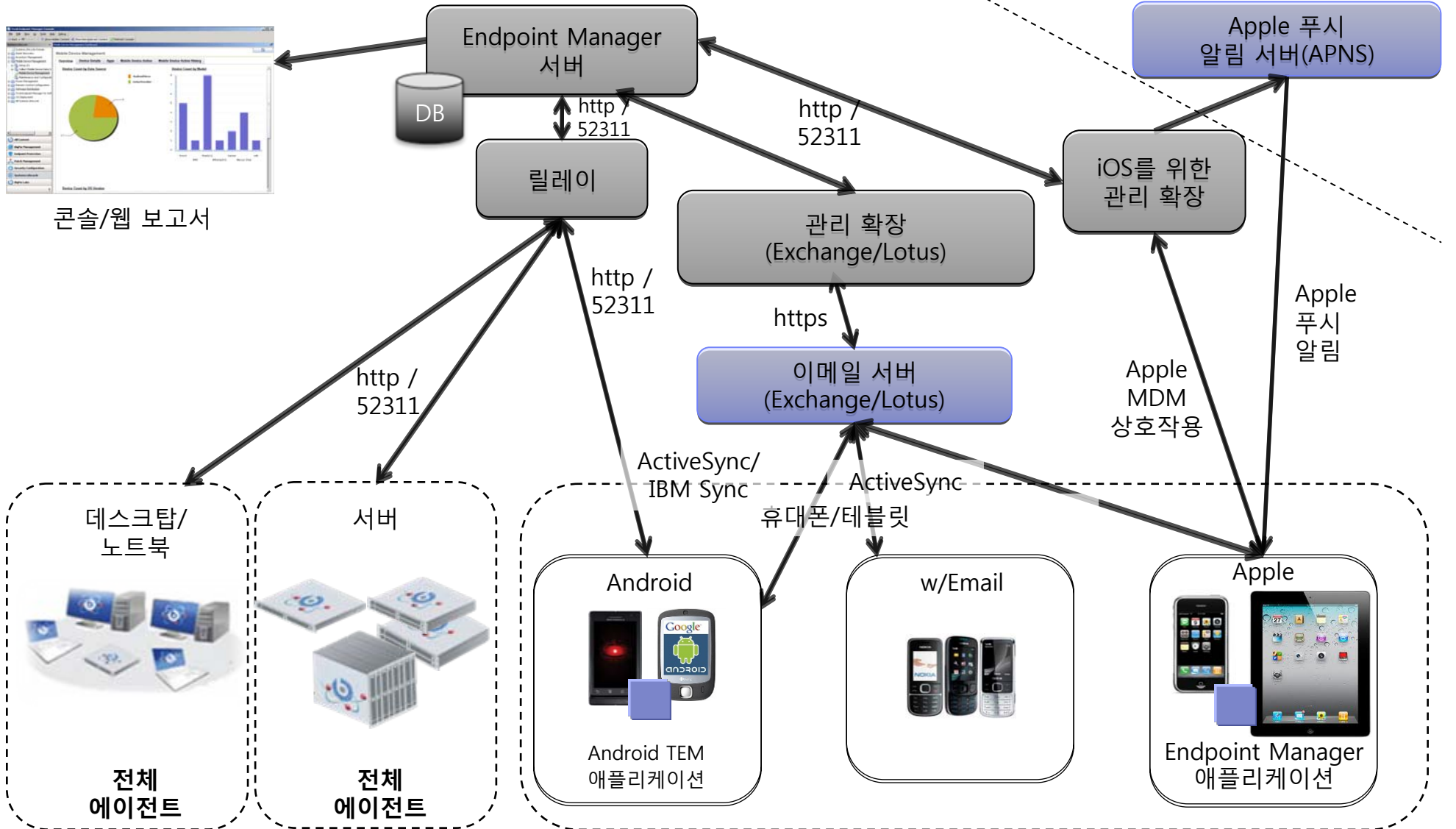
This task will deny targeted mobile devices access to their email server (Lotus Traveler or Microsoft Exchange). Use [Allow Email Access](#) to restore access.

Actions

- Click [here](#) to deny email access.

Description	Details	Applicable Computers (13)	Action History (0)																												
<ul style="list-style-type: none"> ▲ Applicable Computers (13) <ul style="list-style-type: none"> ▲ By Retrieved Properties <ul style="list-style-type: none"> ▶ By Computer Name ▶ By OS ▶ By Agent Type ▶ By Last Report Time ▶ By User Name ▶ By Network Adapter - Windows ▶ By Locked ▶ By BES Relay Selection Method ▶ By Relay ▶ By Free Space on System Drive ▶ By Total Size of System Drive ▶ By Subnet Address ▶ By BES Relay Service Installed ▶ By Test OS ▶ By IP Address ▶ By Group 		<table border="1"> <thead> <tr> <th>Computer Name</th> <th>OS</th> </tr> </thead> <tbody> <tr><td>Android_bf48fac3f41d6e2e</td><td>Android 2.3.6</td></tr> <tr><td>Android_f32067a6cfdb0088</td><td>Android 3.1</td></tr> <tr><td>AppI5K131B6DA4T</td><td>Apple-iPhone3C1/...</td></tr> <tr><td>Android_5514FCEDC0C948F08E9E1...</td><td>Android 2.2</td></tr> <tr><td>Android_354795044824958</td><td>Android 2.2</td></tr> <tr><td>Android_c4207440ef0a152d</td><td>Android 2.3.4</td></tr> <tr><td>AppI87938J5M3NR</td><td>Apple-iPhone2C1/...</td></tr> <tr><td>60A5B61B8144024A3698A9390933F...</td><td>PocketPC/6(5.2.19...</td></tr> <tr><td>AppI7W05224EA4S</td><td>Apple-iPhone3C1/...</td></tr> <tr><td>Android_8f166312739dc043</td><td>Android 2.3.3</td></tr> <tr><td>AppI9C80243A14P</td><td>Apple-iPod/705.18...</td></tr> <tr><td>Android_1292e80b9e00f5f9</td><td>Android 2.3.4</td></tr> <tr><td>AppI3049UUXA90</td><td>Apple-iPad1C1/81...</td></tr> </tbody> </table>	Computer Name	OS	Android_bf48fac3f41d6e2e	Android 2.3.6	Android_f32067a6cfdb0088	Android 3.1	AppI5K131B6DA4T	Apple-iPhone3C1/...	Android_5514FCEDC0C948F08E9E1...	Android 2.2	Android_354795044824958	Android 2.2	Android_c4207440ef0a152d	Android 2.3.4	AppI87938J5M3NR	Apple-iPhone2C1/...	60A5B61B8144024A3698A9390933F...	PocketPC/6(5.2.19...	AppI7W05224EA4S	Apple-iPhone3C1/...	Android_8f166312739dc043	Android 2.3.3	AppI9C80243A14P	Apple-iPod/705.18...	Android_1292e80b9e00f5f9	Android 2.3.4	AppI3049UUXA90	Apple-iPad1C1/81...	
Computer Name	OS																														
Android_bf48fac3f41d6e2e	Android 2.3.6																														
Android_f32067a6cfdb0088	Android 3.1																														
AppI5K131B6DA4T	Apple-iPhone3C1/...																														
Android_5514FCEDC0C948F08E9E1...	Android 2.2																														
Android_354795044824958	Android 2.2																														
Android_c4207440ef0a152d	Android 2.3.4																														
AppI87938J5M3NR	Apple-iPhone2C1/...																														
60A5B61B8144024A3698A9390933F...	PocketPC/6(5.2.19...																														
AppI7W05224EA4S	Apple-iPhone3C1/...																														
Android_8f166312739dc043	Android 2.3.3																														
AppI9C80243A14P	Apple-iPod/705.18...																														
Android_1292e80b9e00f5f9	Android 2.3.4																														
AppI3049UUXA90	Apple-iPad1C1/81...																														

모바일 디바이스 아키텍처를 위한 IBM Endpoint Manager



모바일 디바이스 관리에 대한 Endpoint Manager 기반의 접근 혜택

기업들은 **PC, 테블릿, 스마트폰 전반에 걸쳐 동일한 툴의 사용**을 선호하는데 이는 이러한 유형의 디바이스를 지원하는 사람도 갈수록 동일화되기 때문입니다.

- Gartner, PCCLM Magic Quadrant(2011년 1월)

비록 어떤 수준에서는 모바일이 독특하지만, **모바일 디바이스들은 여러분의 인프라에서 단지 다른 형태의 엔드포인트일 뿐**입니다. 이것은 여러분이 보유한 어떤 기술이든 광범위한 엔드포인트 보호 전략에 통합하기 위한 로드맵을 가지고 있어야 함을 의미합니다.

- Forrester, 시장 개요: 모바일 보안(2011년 4사분기)

하드웨어 및 관리 비용 절감

- 모바일, 디바이스, 노트북, 데스크톱 및 서버를 위한 **단일 플랫폼**
- 25만 개 이상의 디바이스에 이르는 단일 엔드포인트 매니저 서버
- 통합 인프라/관리 모델은 FTE 요건을 줄임

신속한 시간 대비 가치

- 엔터프라이즈급 API는 서비스 데스크, CMDB 등과의 통합을 실현함 (통합 서비스 운영)
- 클라우드 기반의 콘텐츠 제공 모델은 소프트웨어의 업그레이드 또는 설치 없이 신속한 업데이트 가능

IBM®