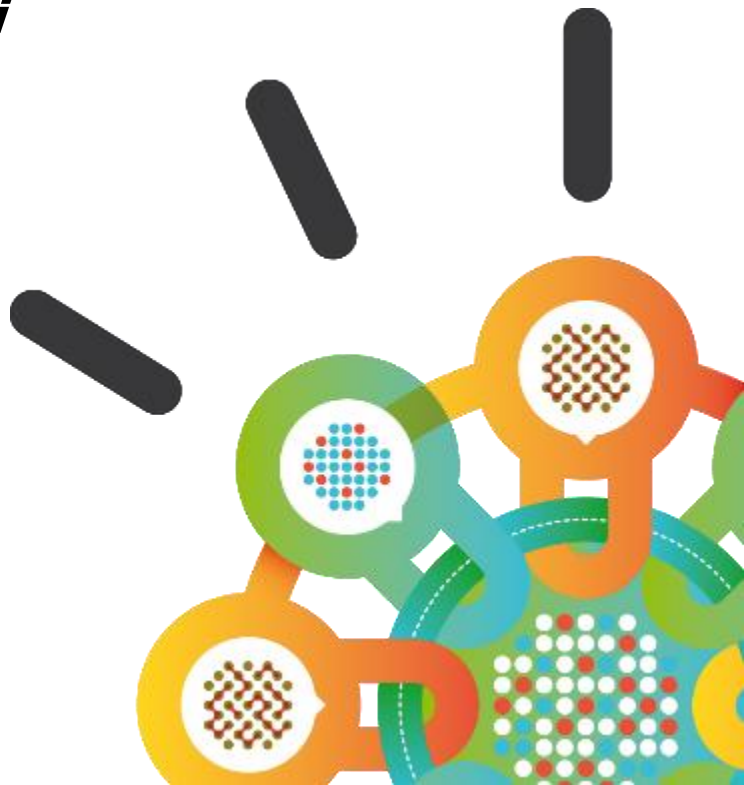
Security Intelligence.
Think Integrated.

모바일 디바이스와 콘텐츠관리

"금융 모바일의 망분리" 전략

김상환 실장
IBM Security Security



Executive Summary

고객 관점에서의 Pain point

- 모바일을 활용한 기업 업무(B2E, B2B)가 증가함에 따라 기업 내 **BYOD 환경의 모바일 장치(스마트폰, 태블릿) 관리와 보안 유지** 방안이 필요함
- 기존 회사가 지급하던 PC 운영 방식과 달리 **상대적으로 보안에 취약한 모바일 장치**를 BYOD 환경으로 활용함에 따라 **다양한 O/S 플랫폼**(iOS, Android, Blackberry, Windows Phone 등) 관리의 복잡성과 보안 대처의 어려움이 존재함
- BYOD 환경에서 **개인과 기업 데이터를 분리(Dual Persona)**하여 운영해야 하며 분실/퇴사 시 기업 데이터만 선택적으로 삭제 운영이 필요함

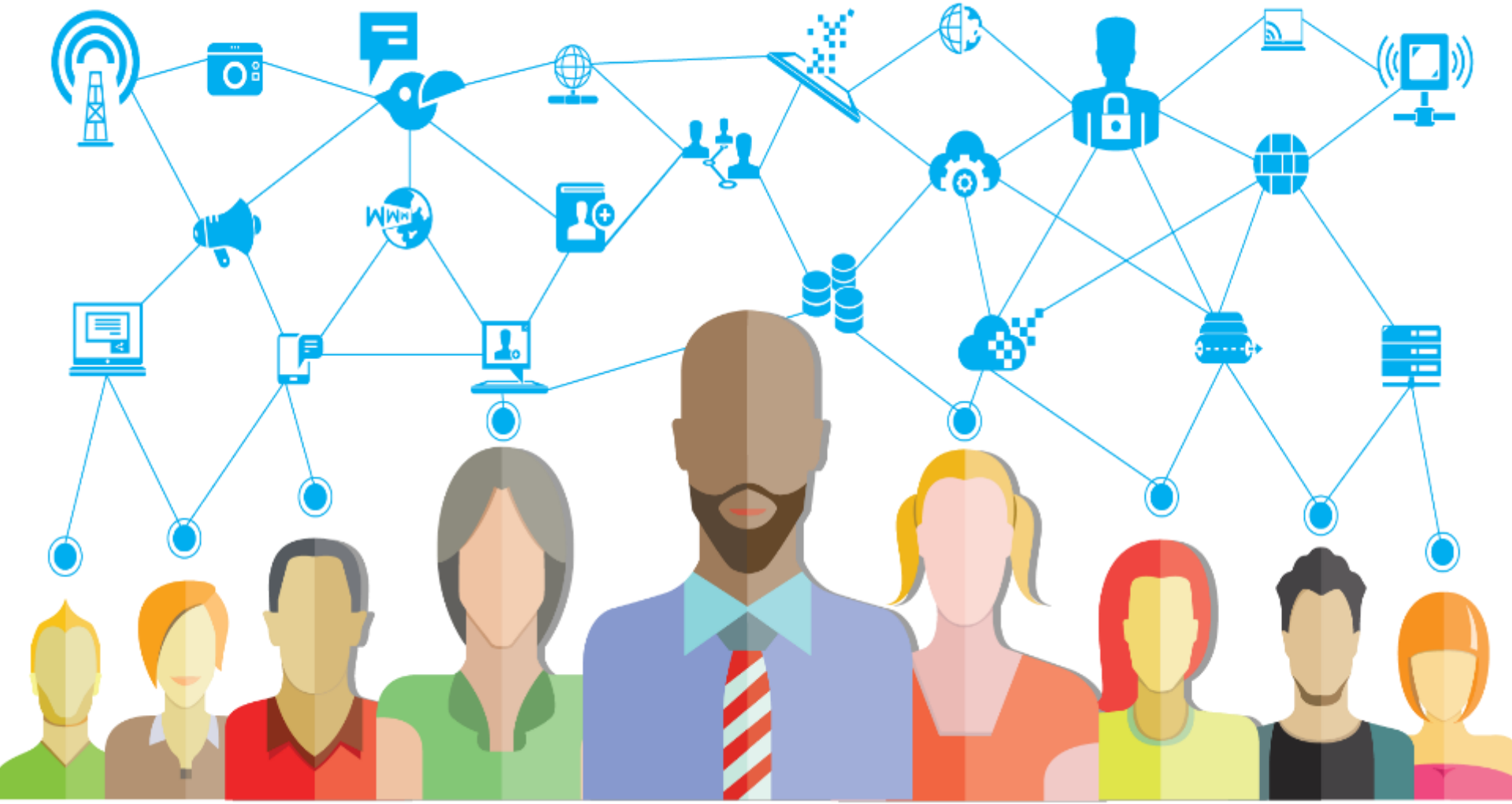
MaaS360 주요 기능 및 장점 (고객 활용가치)

- BYOD 환경의 모바일 장치를 효율적으로 관리하기 위해서는 모바일 장치에 대한 기기 관점의 관리, 앱 제어/관리와 더불어 기업 공간에서의 컨텐츠(문서) 관리를 수용할 수 있는 발전적인 **기업 모빌리티 관리(EMM)** 솔루션을 고려하는 것이 필요함
- 또한 사용자가 어디서나 **수분 내** 자신의 모바일 장치를 손쉽게 등록하도록 유도할 수 있는 방안이 필요하며, 기기 분실 시 빠르게 대처하는 방안이 필요함
- 다양하고 **빠르게 변화하는 모바일 단말유형을 신속히 수용하여** 대처하기 위한 관리 방식이 요구됨

MaaS360 제공 방식 및 가격 정책

- IBM은 고객 니즈에 따라 **다양한 방식(SaaS, On-premise)**의 MDM 솔루션을 공급하고 있음
- IBM 이 제공하는 MaaS360 솔루션은 **MDM, MAM, MCM** 기능을 모두 보유한 토탈 모빌리티 관리 솔루션이며, 모바일 장치뿐만 아니라 **PC(Windows, Mac Os)**까지 동일하게 관리할 수 있어 고객 value를 제공함
- 또한 Device당, User당, 혼합 형태의 **다양한 price** 정책을 제공하며, 고객 상황에 맞게 선택 가능


예전 보안 방식



현재 우리가 일해야 하는 환경

모바일이 보편화됨에 따라 그 중요성은 점점 대두되고 있습니다.

모바일의 중요성은 일하는 방식에 많은 변화를 가져다 주었습니다.

38%

해 마다 모바일을 통하여 구매를 하는 전체 시장매출 금액의 증가율

81%

본인의 회사 일을 처리하기 위해 최소한 1개의 개인 기기를 쓰는 성인 비율

200 million

비즈니스 관련 모바일 앱을 최소한 1개라도 쓰는 사용자 수 (2억명)

* 1시간마다 10번 이상씩 모바일을 확인

모바일이 기업에 중대한 영향을 미치는 5가지 동향

1 **모바일은 가장 중요한 수단**
91%의 모바일 사용자들이 항상 디바이스를 곁에 두고 있습니다

2 **모바일 데이터의 통찰력이 새로운 비즈니스 기회 제공**
75%의 모바일 쇼핑 고객이 위치 기반 서비스 메시지에 반응합니다

3 **모바일이 주요 거래 수단으로 부상**
2015년 모바일 보안 시장규모는 약 250억 수준으로 예상하고 있습니다.

4 **모바일은 지속적인 브랜드 경험을 제공**
90%이상의 사용자가 여러 채널에 걸친 다양한 화면을 접하게 되면서 통합된 경험이 형성되고 있습니다.

5 **모바일이 사물 인터넷(Internet of Things) 시대를 실현**
글로벌 M2M(Machine-to-Machine) 연결이 2022년 말에는 **180억** 건으로 증가할 것으로 예상됩니다

모바일은 기업의 IT 과제에도 영향을 끼칩니다.

- BYOD/COPE/Shared Kiosk 모드
- 외부 및 기업 내부 앱 관리
- 개인정보보호 정책
- 데이터 유출 방지
- 블랙/화이트 리스트 관리
- URL 필터링
- File 연동 및 공유
- 내부망 접속
- 말웨어 차단

8

기업의 CIO와 중역들도 모바일의 중요성을 인식

CIOs[1]:

77%는 기업의 데이터와 어플리케이션에 접근하기 위해 **개인용 모바일 디바이스를 사용할 계획이 있음**

25+ : 향후 2년 이내에 25개 이상의 모바일 어플리케이션이 배포/적용될 것으로 예견

LOB:

CEO의 최우선과제[2]로서 고객 통찰력과 함께 **"모바일이 모든 것을 바꾼다"**의 실행

#2 : CMO들의 디지털 우선 과제 2위는 **태블릿과 모바일 앱을 배포/적용하는 것**임[3]

[1]A report from McKinsey & Company: Based on a survey of 250 CIOs on their mobility strategies.
[2]IBM 2012 CEO study [3]IBM 2011 Global CMO study

하지만 모바일에 대한 보안은 제대로 갖추어져 있지 않습니다.

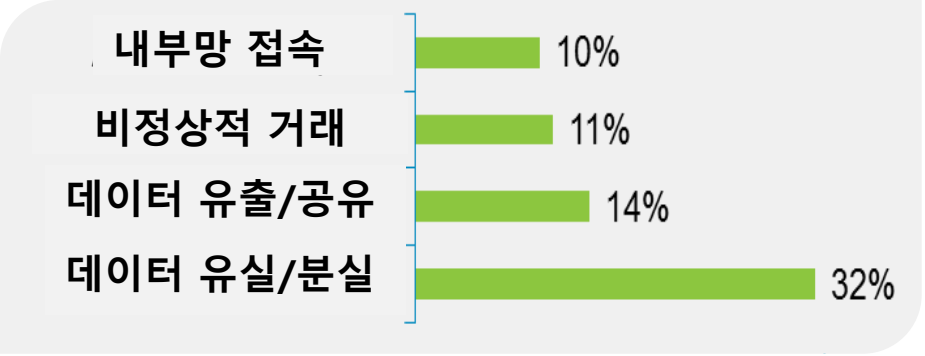
고객들에게 미치는 위협

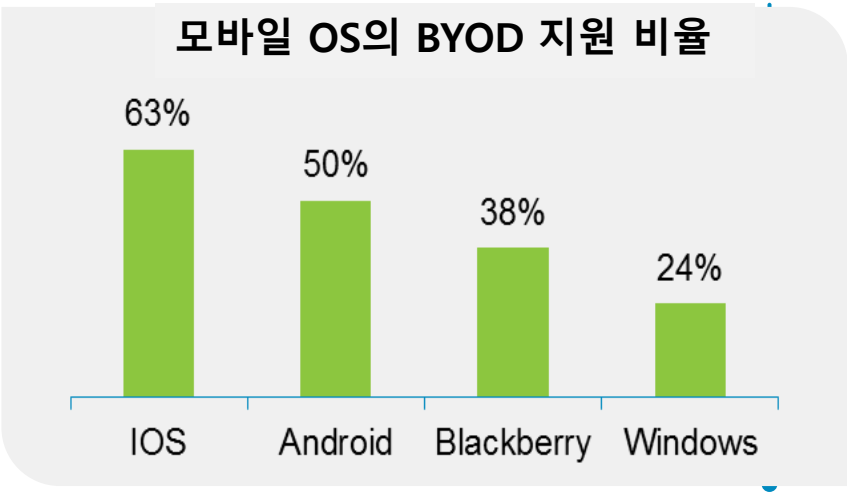
53% 안드로이드 기반 금융 앱들은 이미 해킹을 당한 이력이 있습니다.

100% 상위 100개의 안드로이드 앱들 모두 이미 해킹을 당한 이력이 있습니다.

8.9 billion 연간 보안 사고의 피해 금액 (약 8조9천억)

내부 직원들에게 미치는 위협





기업의 모바일 관리 Challenge

과거에는 모바일 통신 및 협업에 적은 수의 비즈니스 부서가 관여했지만, 현재는 모바일 컴퓨팅은 어디에나 존재하고 조직은 더욱 강력한 관리/보안 방안이 필요한 시기입니다.

관리대상

운영 Challenge

1 관리 관점

- *전통적인 PC 환경에서 모바일 장치(스마트폰, 태블릿 등)로 관리 영역 확대*
- *모든 기기, 애플리케이션, 사용자, 문서를 완벽하게 관리해야 하는 필요성 증가*
- SW 컴플라이언스 유지, 데이터 유출방지, 액세스 통제, 매체제어 니즈 증가

2 보안 관점

- 장비 자체에 대한 관리보다 데이터 보호에 대한 중요성 증가
- *모바일 기기는 더욱 민감한 시스템에 액세스하는 만큼 보호가 필요하며, 인증되지 않은 기기로부터 보호가 필요함*
- *모바일 환경에서의 데이터 보호 중요성 증가*

기업용 모빌리티 관리 영역

Users,Devices, Apps Docs, Web 보호

Mail, Calendar, Contacts

Doc Sharing & Editing

App SDK/ Wrapping

Web & Intranet

기업용 Workplace™

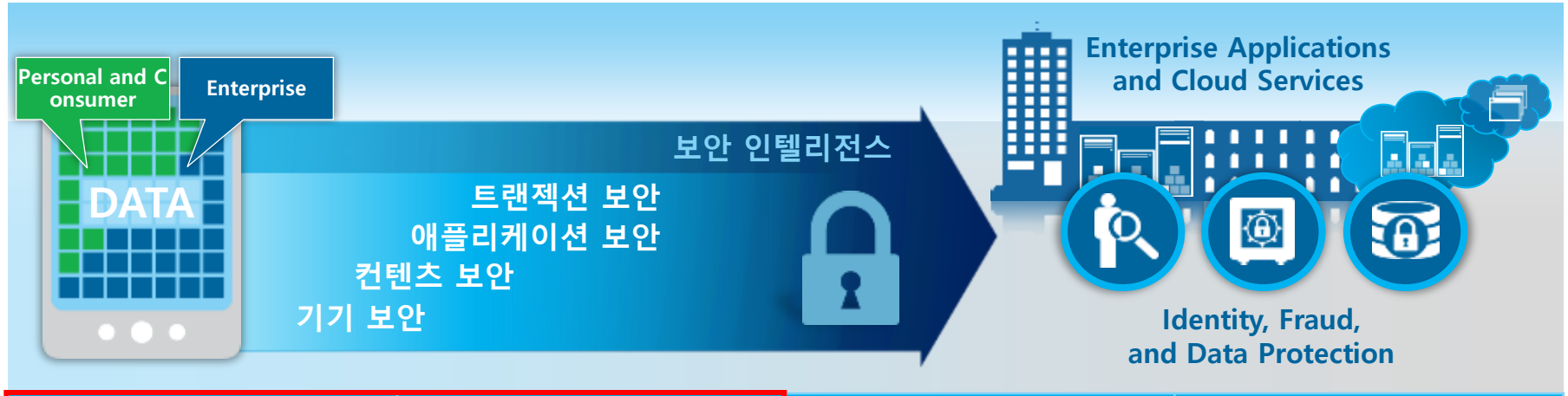
Mail

Docs

Apps

Web

기업 모바일 보안을 위해 갖추어야 하는 영역



기기 보안	컨텐츠 보안	애플리케이션 보안	트랜젝션 보안
기업 소유의 모바일 기기부터 BYOD 기기까지 모든 이기종간 모바일을 클라우드 상에서 편하게 관리	파일 및 문서를 기기간 안전하게 공유하며 기업 문서들을 체계적으로 관리	어플리케이션 개발 시 보안을 고려하여 앱을 설계. 기업의 데이터를 개발 단계부터 어떻게 보호할지에 대해 체계적으로 관리.	기업 모바일 관리 프레임워크에 포함되어 있지 않은 고객, 협력 업체등의 모바일 거래등을 보호
MaaS360 by Fiberlink	MaaS360 by Fiberlink	Worklight	Trusteer an IBM Company

보안 인텔리전스

통합화된 아키텍쳐를 통하여 모바일 보안 정보 뿐만 아니라
이벤트 관리(SIEM), 로그 관리, 비이상적 행위 탐지, 취약점등을 관리

그 외에도 IT측면에서 고려해야 할 요건은 너무 많습니다.

- 산업 규제 및 규정 준수
- 기업 거버넌스
- 개인 정보 보호
- 지적 재산권
- 기업 법무부 및 인사부 지침

다른 기업들은 어떻게 하고 있을까요?

IBM MobileFirst Protect

6000 개 이상의 기업이 모바일 어플리케이션 및 컨텐츠 보호를 위해 사용하고 있습니다.

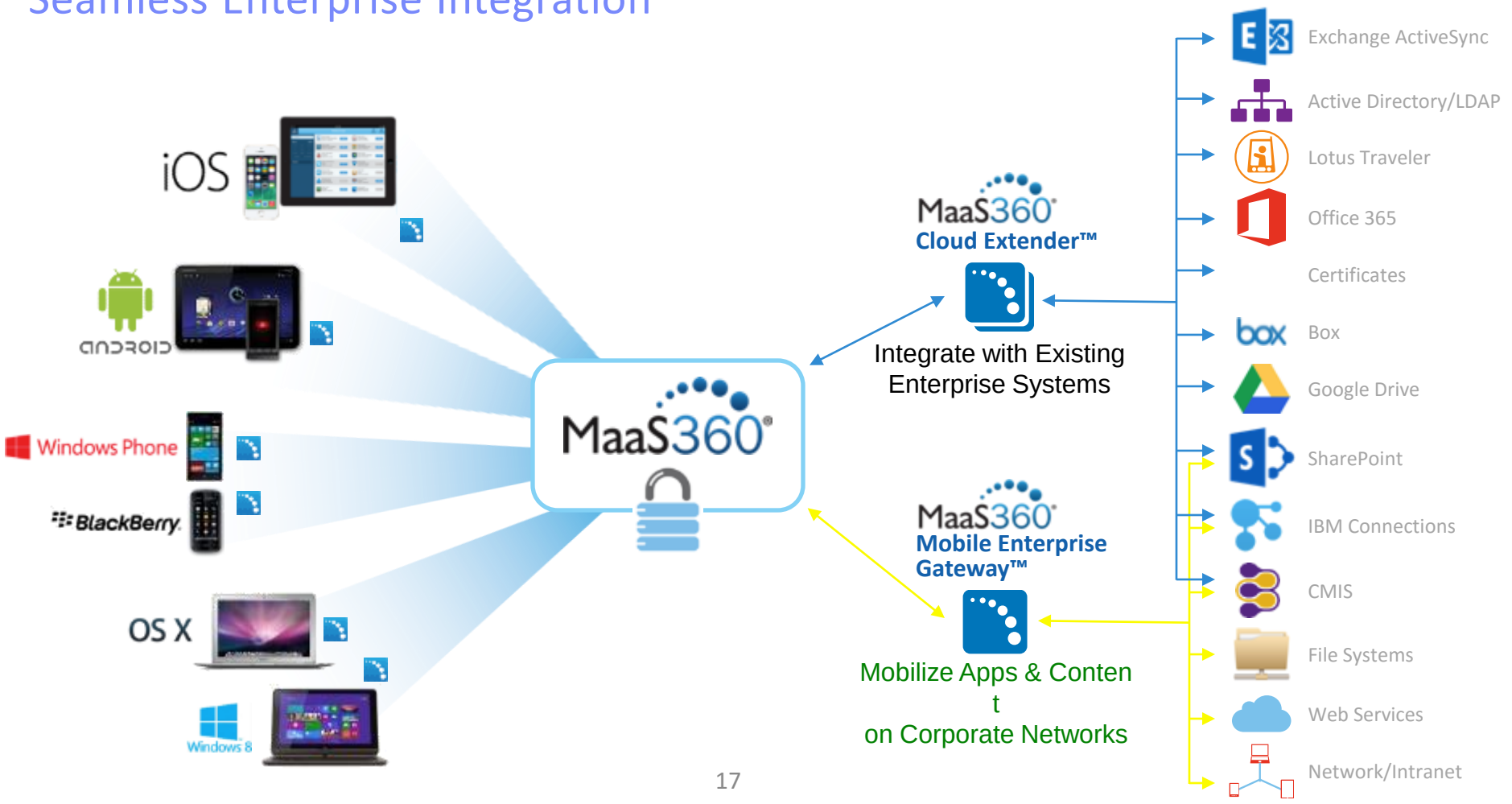
- 백만개 이상의 다른 어플리케이션 등록
- 십만개 이상의 기업용 어플리케이션이 등록
- 200개 이상의 어플리케이션을 관리하는 기업도 존재
- 50/50 비율로 iOS 와Android 외부 어플리케이션 배포
- 기업용 어플리케이션의 70% 는 iOS로 개발

IBM MobileFirst Protect는 아래와 같은 구성으로 기업 모바일 보안을 책임지고 있습니다.

에코 시스템을 받아 들이는 것도 매우 중요합니다.

외부 및 기업 내부 앱의 보안 수준을
끌어올리기 위하여
SDK 또는 어플리케이션 **Wrapping**

Seamless Enterprise Integration



단계별로 모바일 보안을 구축시에는 아래와 같은 과정을 거치게 됩니다.

디바이스 보안

컨텐츠 보안

앱 보안

네트워크 보안

개인 정보와 기업 정보를 분리

디바이스 보안

지속적인 모바일 기기 모니터링을 하여 유동적으로 보안 정책 및 규정 준수를 위한 조치

- 세분화된 비밀번호 규정
- 암호화 세팅 강화
- 탈옥 및 루팅 기기 탐지
- 말웨어 탐지
- 위치 추적, 기기 잠금 및 원격 삭제
- 기기안 데이터 선택적으로 삭제

OTA 설정

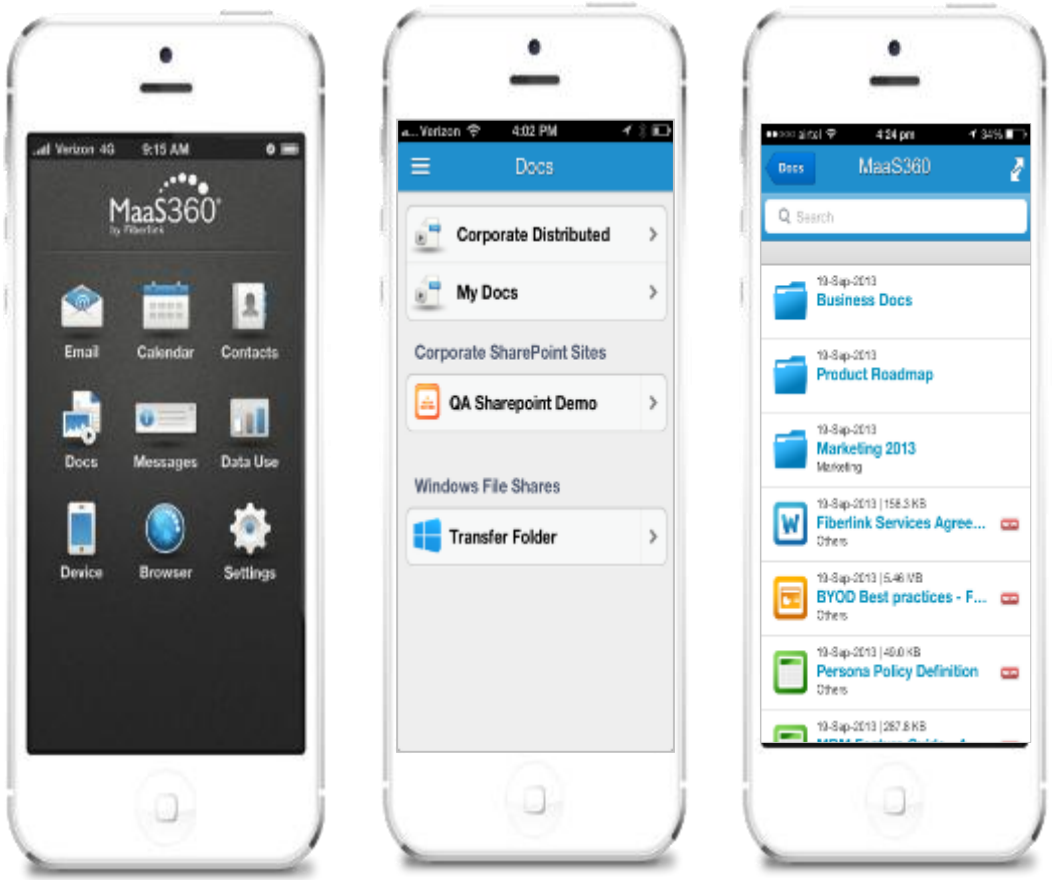
자동화된 조치

정책 수립 및 변경

컨텐츠 보안 :이메일 및 기업 문서

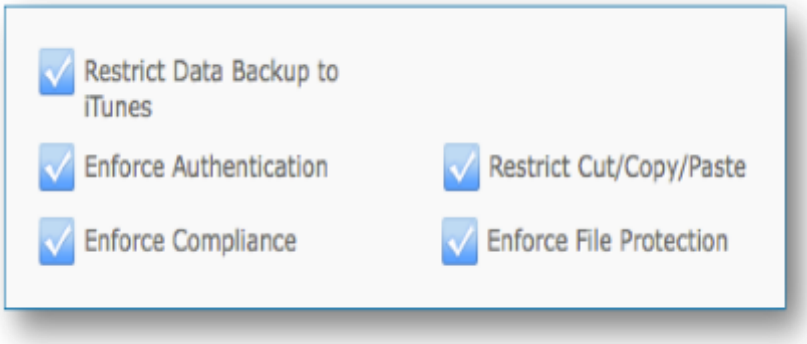
이메일, 캘린더, 연락처 및 컨텐츠를 통한 업무 생산성 향상

- 기업 데이터 포함
- 강력한 암호화
- DLP 설정
- 온/오프라인 규정 준수



앱 보안

데이터 유출을 방지하기 위한 관리적, 보안적 조치



- 사용자 인증 강화
- 보안 취약 기기의 접속 금지
- 정책 위반시 관리자에게 자동 통보
- 정책 위반시 자동화된 조치
- 잘라내기/복사하기/ 붙여넣기 기능 차단
- 파일 보안 강화
- iTunes로 데이터 백업 제한

네트워크 보안

VPN 없이도 기업 내부망에 안전하게 접속할 수 있는 모바일 기업용 게이트웨이 제공

- 기업용 컨텐츠 스토어에 접속 허가
- 내부망을 완벽하게 모바일화
- 앱 내부의 VPN 터널을 이용한 기업 시스템 접근

IBM MobileFirst Protect는 기기 내에서분리된 구성으로 기업 모바일 보안을 책임지고 있습니다.

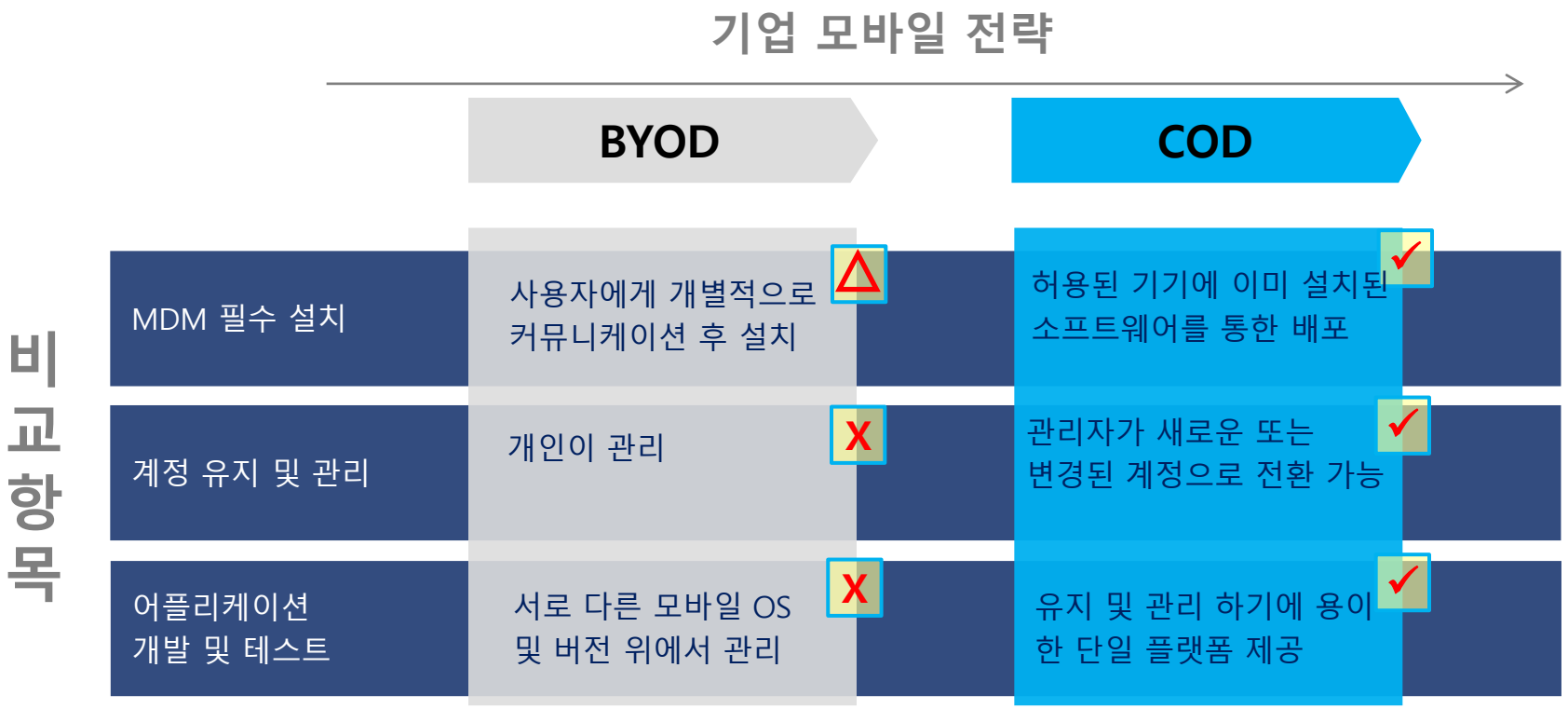
MobileFirst Protect

개인과 기업의 모빌리티를 분리

기업의 자산 및 사용자 보호

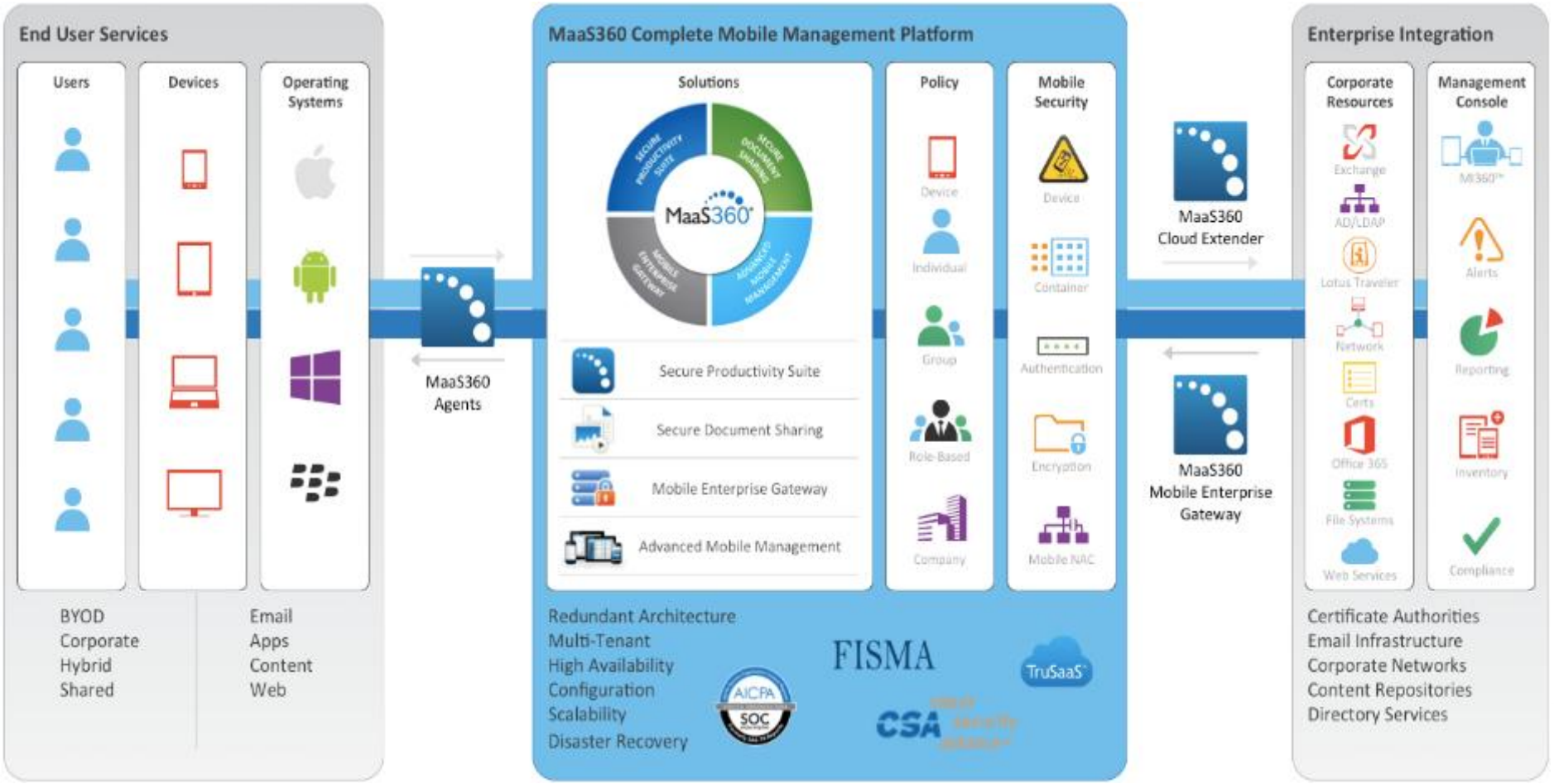
IT 관리자를 위한
직관적인 인터페이스

보안 관점에서 바라보는 BYOD와 COD



BYOD : Bring Your Own Device
COD : Corporate owned Device

완벽한 보안 관리 아키텍처



IBM MaaS360 – 주요 기능(강력한 모바일 보안 관리)

기기 보안

암호화 및 패스코드
탈옥/루팅 발견
위치, 잠금

이메일 보안

자동 격리/이메일 및
첨부파일이 포함된 접속 허용
원격으로 업무용 메일 삭제

앱 보안

모바일 앱에 대한
블랙/화이트 리스트 관리
컴플라이언스 규칙 정의
원격으로 관리 앱 삭제

문서 보안

패스워드 인증
복사, 붙여넣기, 공유 제한
원격으로 업무용 파일 삭제

웹 보안

URL 필터와 카테고리 정의
인트라넷 사이트 접속 허용
네이티브/외부 브라우저
비허용

네트워크 보안

Wi-Fi 및 VPN 프로파일 설정
인증서 제공 및 인증 등록
SSID 기반 동적 규칙 적용

26

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security