

IBM Security

리더십 사고의 백서

## 생산성의 변화

이동 중에도 안전한 콘텐츠 협업



IBM

## 서론

이 문서에서는 직원들이 스마트폰과 태블릿을 이용하여 손 안에서 비즈니스를 수행할 수 있도록 기업 콘텐츠를 보호하는 방식으로 직장 생산성이 빠르게 변화하는 양상에 대해 살펴보고자 합니다.

점점 더 많은 사람들이 모바일 장치를 업무에 활용함에 따라, 모바일 장치에 콘텐츠 제작, 편집, 공유, 동기화 및 푸싱 기능을 완벽하게 제공하는 주요한 엔터프라이즈 이동성 관리 (EMM) 솔루션 요소는 무엇일까요? 이 문서에서는 이 질문에 대한 해답과 더불어 C-레벨에 준하는 생산성 요구와 IT 보안 및 유용성 요건을 균형적으로 충족할 수 있도록 도와주는 업계별 시나리오 및 정보를 제시합니다.

다양한 장치 크기가 작아질수록 그 기능이 점차 발달하여 기능 손실 또는 최종 결과물 형태의 손실 없이 장치 콘텐츠에 대한 액세스를 가능하게 함으로써 생산성 향상의 기반을 이루고 있습니다.

## 생산성의 변화



시카고에 거주하는 한 의사는 복잡한 사례와 관련하여 전문가를 초빙하고자 합니다. 주치의는 스마트폰을 이용하여 볼티모어에 있는 상담 외과 의에게 의료 기록과 X선 자료를 이메일로 전송하고, 이메일 첨부자료를 통해 서로의 통찰력 및 평가 내용을 교환합니다.



주요 주주를 대상으로 한 어느 발표 자리를 마무리하는 단계에서 다양한 기업 데이터 출처로부터 확보한 가장 최신의 금융 정보를 업데이트해야 하는 상황이 닥쳤습니다. CEO는 길거리에서 태블릿을 이용하여 CFO에게 연락하고 소비자 파일을 동기화한 뒤 앱을 공유합니다.

이러한 상황은 흔한 실제 시나리오지만 모범 사례는 아닙니다. 사실 안전한 콘텐츠 협업에 관련된 사례도 아닙니다. 오히려 매우 위험하고 잠재적인 규제 문제를 불러일으키는 사례입니다.

### 이동 중의 콘텐츠

기업 내 노트북의 도입과 더불어 모바일 생산성의 변화가 이루어짐에 따라, 오늘날 직원들은 쉽 없이 일하며 매우 중요한 기밀 콘텐츠를 모바일 장치에 넣고 다닙니다.

직원들은 공항을 비롯해 기차역, 커피숍 및 회의실에 이르기까지 사무실 외 다양한 환경에서 문서를 작성하고, 열고, 업데이트하고, 분석하고, 편집하며 공유하고 있습니다. 이제 동료 및 고객과의 협업을 통해 얻을 수 있는 효율성은 이동이 불가능했던 정적인 장치에만 국한되지 않습니다.

그러나 이러한 콘텐츠는 안전한 트랜잭션을 반드시 확인해야 하는 기업 네트워크상의 Windows File Share, SharePoint, 인트라넷 및 웹 앱과 같은 위치에 저장됩니다. 동료, 파트너 및 고객 간 협력에 필수적인 정보들은 현재 내부 드라이브, 데이터 저장소 및 wikis, 지식 기반, ERP, SCM, HRM, CRM, 그리고 기타 관리 시스템에 묶여 있습니다.

다양한 장치 크기가 작아질수록 그 기능이 점차 발달하여 기능 손실 또는 최종 결과물 형태의 손실 없이 장치에서 콘텐츠에 대해 액세스할 수 있게 함으로써 생산성 향상의 기반을 이루고 있습니다.

### IT: 생산성과 보안의 중심점

IT는 이렇게 핸드헬드 장치를 이용하며 끝없이 움직이고 성장하는 작업자의 영역을 구현하고 있으며, 이 영역에서 콘텐츠의 크기는 점점 더 커질 것으로 예상됩니다. BYOD (회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침)는 단순히 장치 조달 패러다임을 바꿔놓은 것에 불과하기 때문에 데이터 보안과 자유 분방한 전달 방식에 대한 책임은 전가되지 않습니다.

엔터프라이즈 이동성 관리 (EMM) 솔루션은 안전한 콘텐츠 협업을 가능케 할 뿐 아니라 C-레벨에 준하는 수익 요구와 더불어 비즈니스 생산성 요구를 동시에 충족할 수 있습니다. 이 문서에서는 모바일 장치 관리의 장치 분류에서 모바일 장치상 기업 콘텐츠 및 데이터에 대한 EMM의 선행적 보호로 전향하는 과정에 대해 살펴보고자 합니다.

### 성공적이고 안전한 콘텐츠 프로그램의 구축

물론 내과의와 상담하기 위해 이메일로 환자 기록을 공유하는 것은 편리한 일입니다. 이미 수년간 그렇게 해 왔으니까요. 하지만 그렇게 할 수 있다고 해서 그렇게 해도 된다는 뜻은 결코 아닙니다!

소비자 솔루션으로 아무 곳에서나 동기화하고 공유할 수 있는데, 얼마나 좋습니까? 특히 이제 막 비행기에 올라 타는 CEO에게 말이죠. 하지만 IT 현장에서는 언제 터질지 모르는 시한 폭탄을 기다리는 것과 다름이 없습니다.

스마트폰, 태블릿 및 착용식 장치는 끊임없이 협업하게 하지만, 올바른 EMM 솔루션을 마련함으로써 그 과정을 안전하게 지킬 수 있습니다! 파일이 사무실이나 ER의 공간을 벗어났다고 해서 더 이상 IT가 전송 지침을 제공하지 않는 것이 아닙니다.

### 이메일 및 파일 동기화/공유: 일반적인 솔루션, 그러나 잘못된 관행

오늘날에는 소비자 등급 클라우드 협업에 전송이 시도되었던 이메일 및 실제 전송된 이메일을 활용하여 데이터를 공유하는 방법이 백만 가지나 되지만, 이러한 접근법이 반드시 모범 사례인 것은 아닙니다. 이러한 방법은 기밀 정보를 확인하는 방법만 안다면 누구에게든 기밀 정보를 공유하고 직원 생산성을 위협하는 콘텐츠의 취약성을 방치하기 때문이죠.

### 새 우편물 도착... 그리고 제약 없는 공유의 수단

오래 전부터 우리가 문서 공유를 위해 사용해 온 이메일은 사실 별로 효율적이거나, 생산적이거나, 안전한 콘텐츠 저장소가 아닙니다. 이메일 첨부자료는 파일이 잘못 전송되거나 공유될 수 있다는 가능성을 안고 있을 뿐 아니라, 쾌적한 우편 서버 트래픽 로드와 적합한 크기보다 너무 커져 버렸습니다. 또한 이메일은 일반적으로 실시간 분류, 필터링, 편집 또는 동기화를 지원하지 않습니다. 결론적으로 이메일은 안전하지 않을 뿐더러 생산성과 협업에 지장을 줄 수 있습니다.

하지만 사람들은 계속해서 이메일을 사용하고 있죠. 이메일을 통한 공유는 일반적인 관행으로 자리잡았습니다. 최근 5,100명 이상의 직원을 대상으로 한 Ovum 국제 설문조사에 따르면, 이 직원들 가운데 44%는 지속적으로 이메일 및 메모리 스틱을 이용하여 문서를 공유하고 있습니다.

**설문에 참여한 IT 전문가 중 46%는 “파일 공유 제품의 사용 시 제대로 관리하지 않아 회사 데이터가 유출된다”는데 동의하고 있습니다.**

### 소비자 동기화/공유 애플리케이션: 위험하고 안전하지 않은 방법

소비자 시장은 파일 동기화 및 공유 앱으로 넘쳐나며, 그 중 일부로 Dropbox, Google Drive, Evernote 및 iCloud를 들 수 있습니다. 기업에서 개발한 (사내) 접근법은 현재 발생 초기 단계이며, 생산성 측면에서 실망스러운 경우가 많습니다. 그러니

직원들이 가족 사진을 보관할 때 쓰는 Dropbox를 대규모 발표 준비를 위한 주말 업무에 쓰기 십상이죠. Ovum이 실시한 연구에 따르면 직원들 중 89%는 회사에서 제재하는 접근법에 만족하지 못해 소비자 등급의 시스템을 사용하고 있습니다.<sup>3</sup>

소비자 파일 동기화 및 공유 애플리케이션은 직원들에게 접근성과 편리성을 제공하지만, 가시적인 보안 요구 또는 집중적인 콘텐츠 정책 집행 요구를 충족시키지는 못합니다. 이러한 솔루션은 보호하지 않은 채로 방치할 경우에 잠재적으로 기업의 데이터 유출, 보안 공격 및 규제 준수 위반 위험을 유발할 수 있습니다.

그러나 직원들은 Interlink 설문에서도 이러한 솔루션의 사용을 고집하고 있으며<sup>4</sup>, 설문에 참여한 IT 전문가 중 46%는 “파일 공유 제품의 사용 시 제대로 관리하지 않아 회사 데이터가 유출된다”는 데 동의하고 있습니다. 또한 84%는 직원들이 자유롭게 파일 동기화 및 공유 제품을 이용함으로써 잠재적 보안 문제가 발생할 수 있다는 의견을 밝혔습니다.

### 모바일 장치상의 기업 콘텐츠를 성공적으로 보호하기 위한 주요 요소

생산성을 확보하고 기업을 보호하기 위해서는 직장 내 직원들이 엔터프라이즈 이동성 관리의 안전성, 효과성 및 편리성에 대해 신뢰감을 가져야 합니다.

모두의 업무에 적합하도록 설계되는 솔루션에는 다음이 포함되어야 합니다.

**접근성이 우수하며 직관적인 도구:** 사용자는 일반적인 파일 유형 (Excel, Word, PowerPoint, PDF) 의 생성, 편집, 동기화 및 공유 시 콘텐츠에 더 쉽게 접근할 수 있도록 지원하는 도구가 필요합니다. IT는 문서를 보고 공유하는 방식에 초점을 맞추고, 더불어 편집과 관련하여 보다 강력한 제어를 규정하는 보안 정책을 활용해야 합니다.

**클라우드를 이용한 보안 및 확장성:** 견고한 EMM 솔루션은 민감 데이터를 보호할 수 있도록 암호화된 안전한 컨테이너를 이용하며, IT가 시간 및 위치 기반 정책, 비밀번호 준수 및 모범 사례 문서 작업 흐름을 확립, 구현 및 집행할 수 있도록 도와주기도 합니다. IT는 클라우드 기반 솔루션을 이용하여

집중적인 콘솔로부터 역할 기반의 접근 및 관리 기능을 제공할 수 있습니다. 동시에 사용자 장치상의 안전한 컨테이너 이외의 환경에서는 문서를 열 수 없습니다.

전체적인 관리 하의 클라우드 솔루션은 확장 가능한 배포를 위한 해답이 될 수도 있습니다. 문서를 한 번 저장하고 여러 번 배포함에 따라 저장 용량 또는 대역폭의 제한에 대한 우려를 덜 수 있는 것이죠.

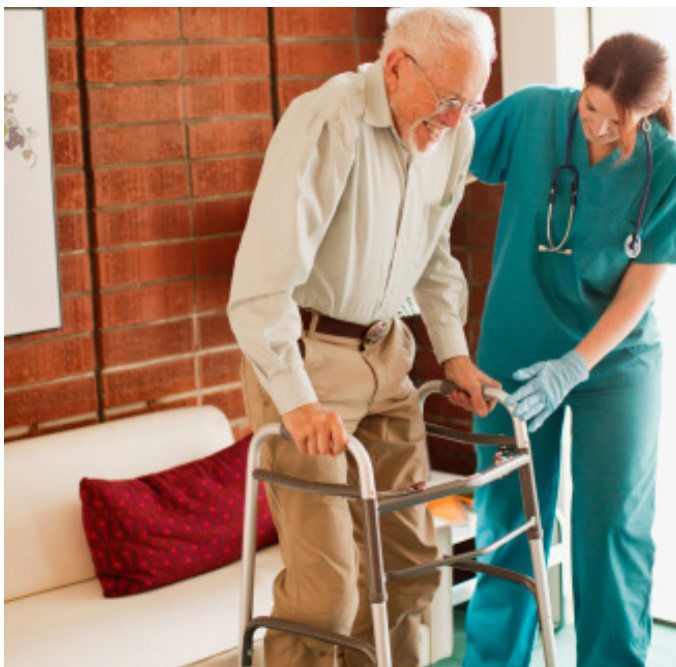
클라우드 EMM을 구현하는 것의 비용 효과성과 편리함은 빠르게 변화하는 모바일 시대에 투자 수익률 (ROI) 의 목표도 충족할 수 있습니다. 배치 및 유지관리 비용을 대폭 절감하고, 다른 서버를 구매 및 관리할 필요 없이 IT의 시간 및 자원을 더 높은 가치의 기업 이니셔티브에 할애하도록 도와주기 때문입니다. 모바일 운영 체제가 계속해서 새로운 앱을 지원하는 동안에도 여러분은 EMM 소프트웨어를 단일 업데이트하지 않고 모바일 군대를 무력화할 수 있는 것입니다.

**준수:** 각기 다른 여러 업계에서 준수 요건 제약을 받고 있습니다. EMM 솔루션은 이러한 규정을 수용해야 하죠.

상장 기업은 통제 하에 이루어지는 금융 보고 기간 이외에 금융 정보 배포를 제한하는 Sarbanes-Oxley Act (SOX) 법의 적용을 받습니다. 금융 서비스에서 분야에서 FINRA (금융 업계 규제 당국) 은 스마트폰 및 태블릿이 소비자 정보 보호를 위한 기업의 광범위한 특권적 정보 요건을 준수할 것을 요구합니다.

HIPAA (Health Insurance Portability and Accountability Act) 도 의료 업계를 대상으로 암호화된 개인 신상 정보와 보호된 건강 정보를 보관할 수 없도록 금지하는 규칙을 통해 유사한 제약을 가하고 있습니다. 소매업체의 경우에는 PCI DSS (Payment Card Industry Data Security Standard) 에 따라 카드 소유자의 데이터를 사용 방식 및 보관 위치와 관계 없이 철저히 보호해야 하는 엄격한 지침을 따르고 있습니다.

## 변화의 가능화



환자가 치료를 끝내고 집으로 향합니다. 환자는 본인의 주치의가 본인의 사례와 관련하여 최고 전문가의 도움을 받을 수 있다는 사실에 안심하고 있습니다. 이 환자의 의료 정보는 기밀로 유지되며 의사 장치의 이메일에 담겨 보호됩니다.



이 CEO는 야구장에서 발표를 진행합니다. 주주와 이사회에서는 한층 개선된 수치 결과에 매우 만족합니다. 또한 이 정보는 회사의 안전한 직장 내에서 지속적으로 보호됩니다.

이렇게 순간적인 모바일 모멘트가 끝나고 데이터가 오랜 기간 안전하게 보관되면, 기업에서는 EMM 솔루션을 확보하여 모바일 생산성을 구현하는 것뿐 아니라 정적, 동적 및 사용 중 상태의 데이터를 보호할 수 있다는 장점을 실감하게 됩니다.

### 안전한 콘텐츠의 장점

환자의 침상을 비롯해 공항 라운지와 그 이외 환경에서도 사람들이 콘텐츠에 접근하고 이를 생성, 편집, 관리, 공유 및 동기화할 수 있도록 가능화하는 것의 장점은 무수히 많습니다. IT의 경우에는 비즈니스 리더, 직원 및 기업 전체가 되겠죠.

전 세계가 직장이라면 **기업은** 사람들이 언제 어디서든 일을 할 수 있고 서로 시간대가 달라도 콘텐츠와 관련하여 타인과 지속적으로 협업할 수 있는 장소로 변화합니다.

**생산성과 협업**은 직원들이 문서에 액세스하고 이를 편집, 관리, 공유 및 동기화하며 이와 관련하여 협업을 하기 위해 갖은 고생을 할 필요 없이 연속적으로 일을 할 수 있을 때 비로소 향상됩니다. IT와 C-레벨은 민감 데이터와 콘텐츠가 정적 또는 동적 여부와 관계없이 누출 또는 오용의 위험으로부터 안전하다는 사실을 인지할 때 안심할 수 있습니다.

직원들이 회사에 영향을 주지 않고 개인 및 사적인 용도로 본인의 장치를 사용할 수 있다면, **직원들의 만족도도** 높아 집니다. 그리고 직원들의 만족도 향상에 따라 생산성이 또 한 번 향상될 것입니다!

### 안전한 콘텐츠의 주요 요건

언제 어디서든 콘텐츠를 안전하게 보호하려면 다음이 필요합니다.

- **안전하고 직관적인 직장:** 모바일 플랫폼상에서 기업 파일을 개인 데이터와 완전히 분리하여 저장, 공유 및 동기화할 수 있어야 합니다.
- **중앙 집중 관리식 제어:** 이를 통해 IT가 문서 액세스 및 규칙 기반의 제한사항에 대한 완전한 가시성을 확보할 수 있습니다.
- **원활한 통합:** 기존 인증 및 허가 시스템과 원활히 통합되어야 합니다.
- **원격 문서 푸싱 기능과 작업 흐름 수립 및 집행 기능:** 대량 또는 선택적 배포 시 필요합니다.
- **기존 자산 및 투자에 대한 안전한 접근:** 맞춤형 데이터 저장소부터 IBM Connections, SharePoint 및 Google과 같은 기타 제품에 이르기까지 다양한 환경에서 안전한 접근이 가능해야 합니다.
- **특정 파일 공유 및 동기화 애플리케이션 블랙리스트:** 모바일 장치상에서 특정 사용자, 집단 또는 전체 인구를 대상으로 사용할 수 없도록 차단해야 할 블랙리스트를 구축합니다.
- **포함된 이메일 및 첨부자료:** 이메일로 공유되는 문서를 보호합니다.
- **원격 삭제:** 오래된 정보, 장치 분실, 직원 퇴사 또는 “탈옥” 또는 “루팅”된 비준수 장치를 원격 삭제합니다.

### IBM® MaaS360®

MaaS360은 조직에서 모바일 장치상에서 콘텐츠에 보다 안전하고 손쉽게 액세스하고 이를 푸싱, 생성, 편집, 공유 및 동기화할 수 있도록 도움으로써 변화를 가능화하고 있습니다. MaaS360의 EMM 솔루션은 직원들이 이러한 장치에서 독립적으로 업무를 수행하고 문서를 공유하는 동시에, IT가 확장적 관리와 암호화 및 보호된 컨테이너 내에서의 통제를 구현할 수 있도록 도와줍니다.

MaaS360 솔루션이 제공하는 바는 다음과 같습니다.

- **콘텐츠 저장 기능 및 콘텐츠 관리 시 손쉽게 사용할 수 있는 간편한 인터페이스:**
  - 클라우드 기반 Box, Google Drive, Dropbox 및 MaaS360을 포함한 여러 데이터 저장소 옵션 (사내 또는 하이브리드 클라우드) 과 IBM Connections, Windows File Share 및 SharePoint 등의 사내 제품

- **장치상 컨테이너로 iOS, Android, Windows Phone 및 PC용 콘텐츠에 액세스:**

- 장치에서 보호된 파일 전송
  - 여러 유형의 데이터 저장소에 액세스 (클라우드 및 사내)
  - 저장소에서 장치로의 데이터 이동 중 데이터 보호
- 모바일 장치 보안 통합: 인증, 비밀번호 보호 및 원격 삭제
- 컨테이너화 및 데이터 손실 방지
  - 컨테이너 내 정적 데이터 암호화
  - 데이터에 대한 다른 앱의 액세스 제한, 잘라내기/복사/붙여넣기 차단, 그리고 화면 캡처 방지
  - 콘텐츠의 선택적 삭제 가능
  - 이메일과 같은 다른 엔터프라이즈 이동성 앱과 통합

- 동기화 및 공유:

- 사용자가 소유한 콘텐츠를 여러 가지 장치 유형에서 동기화하고, 노트북에서 콘텐츠를 생성하여 스마트폰/태블릿에 동기화시키며, 이메일과 통합하여 첨부자료 보안 및 통제 촉진
- 다른 모바일 앱, 그리고 내부 및 외부 사용자 (동료, 파트너 또는 고객) 와 콘텐츠를 공유하고 공유 인증 및 만료 등의 공유 정책 집행

- 콘텐츠 조작

- 더 안전하게 생성, 편집 및 주석 추가

### 변화의 시작

생산성의 변화는 이미 현재 진행형입니다. 여러분은 귀사 직원들을 위해 이러한 변화를 가능하게 함에 있어 어떤 역할을 하고 계십니까? 전체적인 기업을 변화시키고자 한다면 우선 몇 가지 주요 질문에 대한 답을 구함으로써 시작할 수 있습니다.

- 여러분의 비즈니스 라인은 생산성을 확보하기 위해 무엇을 필요로 합니까?
- 이러한 비즈니스 라인은 현재 어떻게 운영되고 있습니까?
- 현재 어떤 유형의 보안 또는 파일 동기화 및 공유 정책을 제공 또는 집행하고 계십니까?
- 현재 여러분의 도구는 확장이 가능합니까?
- 개선을 위한 계획은 무엇입니까?

## 사례 연구

한 국제 보험 회사에서는 MaaS360이 생산성을 증진시켜 줄 뿐 아니라 비용 및 시간을 절약해 준다고 이야기합니다.

“IBM® MaaS360® Content 제품군은 저희에게 정말 유용해요. 영업 담당자가 새 보험 가입자를 만날 때 보험 비용 및 등록 세부 사항을 요청할 수 있고, 우리는 담당자가 고객을 만나는 동안에 적합한 문서를 제공해 줄 수 있거든요. 그럼 고객들도 바로 그 자리에서 등록 양식을 작성할 수 있으니 마무리 과정을 속행할 수 있죠.”

– 국제 보험 회사 네트워크 지원 전문가.

기업에서 발급하는 BlackBerry Bold 장치를 iPhone과 iPad로 교체한 어느 소매 및 서비스업 결제 전문 기업은 BlackBerry 기업 서버를 이용하던 때와 동일한 수준의 보안 및 관리를 제공할 필요성을 인지하고 있었습니다. 이 기업은 조직이 직원들의 기업 문서 접근 방식을 더 쉽고 효율적으로 개선할 수 있도록 도와주는 MaaS360에서 해답을 찾을 수 있었습니다. “MaaS360은 모든 방면으로 손쉽게 이용이 가능하니까 확실히 다른 것 같아요. 인터페이스도 훨씬 간단하면서 직관적입니다. 보고 방식도 간편할 뿐 아니라 비용 관리를 위한 사용량 추적도 가능하죠. 그리고 IBM® MaaS360® Secure Mobile Browser와 컨테이너 기능은 저희 네트워크의 취약성을 자동으로 감소시켜 줍니다.”

– 소매 및 서비스업 결제 전문 기업 기술 시스템 책임자.

## IBM MaaS360 정보

IBM MaaS360은 엔터프라이즈 이동성 관리 플랫폼으로서 사람들의 업무 방식과 관련된 생산성 및 데이터 보호 기능을 제공합니다. MaaS360은 수천여 개의 조직들로부터 이동성 이니셔티브의 기반으로 인정받고 있습니다.

MaaS360은 어떤 모바일 배포 과정이든 지원할 수 있도록 사용자, 장치, 앱 및 콘텐츠 측면에서 모두 강력한 보안 제어를 가능케 함으로써 종합적인 관리를 도와줍니다.

IBM MaaS360에 대한 자세한 정보를 보고, 무료 30일 시험판을 시작하려면, 다음 웹페이지를 방문하십시오.

[www.ibm.com/maas360](http://www.ibm.com/maas360)

## IBM Security 정보

IBM의 보안 플랫폼은 조직에서 직원, 데이터, 애플리케이션 및 인프라를 총체적으로 보호할 수 있도록 도와주는 보안 인텔리전스를 제공합니다. IBM은 ID 및 액세스 관리, 보안 정보 및 이벤트 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 차세대 침입 보호 등을 위한 솔루션을 제시합니다. IBM은 전 세계 가장 광범위한 보안 연구 개발 및 인도 성과를 자랑하는 조직 중 하나입니다. 자세한 정보는 다음 웹사이트를 참조하십시오.

[www.ibm.com/security](http://www.ibm.com/security)



© Copyright IBM Corporation 2016

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589

Produced in the United States of America  
2016년 3월

IBM, IBM 로고, ibm.com 및 X-Force는 전 세계 많은 관할지에 등록된 International Business Machines Corp의 상표입니다. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® 및 장치, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility®, Trusted Workplace™, Visibility360® 및 We do IT in the Cloud.™ 와 장치들은 IBM Company인 Fiberlink Communications Corporation의 상표 또는 등록 상표입니다. 그 밖의 제품 및 서비스 이름은 IBM 또는 해당 회사의 상표입니다. 현재 IBM 상표 목록은 다음 웹사이트의 “저작권 및 상표 정보”에서 확인할 수 있습니다. [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Apple, iPhone, iPad, iPod touch 및 iOS는 미국 및 기타 국가에서 사용되는 Apple Inc.의 등록 상표 또는 상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 및/또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

본 문서는 출판 시점에 유효한 문서로서, IBM에서 언제든지 변경할 수 있습니다. IBM이 사업을 운영하는 모든 국가에서 모든 제한이 제외되는 것은 아닙니다.

본문에 인용된 실적 데이터 및 고객 사례는 단순한 예시용입니다. 실적 실적 결과는 구체적인 구성과 운영 조건에 따라 달라질 수 있습니다. IBM 제품 및 프로그램과 함께 사용하는 기타 제품 또는 프로그램의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 비침해에 대한 보증이나 조건을 포함하여 명시적 또는 묵시적으로 어떠한 보증 없이 “있는 그대로” 제공됩니다. IBM 제품은 제공된 약정에 명시된 조항 및 조건에 따라 보증됩니다.

관련법과 규정을 준수해야 할 책임은 고객에게 있습니다. IBM은 법률 자문을 제공하지 않으며, IBM이 고객에게 서비스 또는 제품을 제공한다는 사실이 고객이 관련 법률 또는 규제를 준수하고 있음을 IBM이 확인하거나 보증하는 것은 아닙니다.

IBM의 향후 방향에 대한 언급은 통보 없이 변경 또는 철회할 수 있으며, 단순히 목표와 목적을 제시하는 용도입니다.

올바른 보안 관행 기술: IT 시스템 보안은 기업 내에서의 부적절한 접속에 대한 예방, 탐지 및 대응을 통하여 시스템 및 정보를 보호하는 일을 담당합니다. 부적절한 접속으로써 정보를 변경, 파괴 또는 악용하거나 다른 정보를 공격하는 등 시스템 손상 또는 시스템 오용으로 이어질 수 있습니다. 어떠한 IT 시스템 또는 제품도 완전히 안전하다고 고려되지 않으며, 어떠한 단일 제품 또는 보안 조치도 부적절한 접속 방식에 완전히 효과적일 수는 없습니다. IBM 시스템 및 제품은 포괄적인 보안 접근법의 일환으로 설계되었고, 추가 운영 절차에 필연적으로 관여하고, 최대한 효과적으로 되기 위해 기타 시스템, 제품 또는 서비스를 요구할 수도 있습니다. IBM은 시스템 및 제품이 제3자의 악성 또는 불법적인 행위로부터 면역되어 있다고 보증하지 않습니다.

1 *Ovum Mobility Survey 2014* (September 2014) <http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/>

2 *Intralinks Survey Report, Safe Sharing: A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications* (Intralinks, June 2014) [https://www.intralinks.com/sites/default/files/file\\_attach/via14\\_65324\\_email\\_harrispaper\\_v1.1.pdf](https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf)

3 *Ovum Mobility Survey 2014* (September 2014) <http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/>

4 *Intralinks Survey Report, Safe Sharing: A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications* (Intralinks, June 2014) [https://www.intralinks.com/sites/default/files/file\\_attach/via14\\_65324\\_email\\_harrispaper\\_v1.1.pdf](https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf)



재활용하세요