엔터프라이즈의
모바일 업무 강화를 위한 방안

디모아 성동현 대리

DMOA

- 엔터프라이즈 업무 트랜드
- EMS 배경과 목적
- EMS 기능 소개 및 시나리오

• 엔터프라이즈 업무 방식의 변화

- 기업 사용자의 업무 방식이 개인화되고 소비화됨에 따라, 사용자가 선호하는 디바이스와 연결 방식의 업무를 지원해야 하며, 이동 환경에서도 보안이 고려된 비즈니스 요구를 지원할 수 있도록 Mobility를 제공하기 위한 사용자 중심의 업무 환경의 구성이 필요합니다.

전통적 업무 환경

획일화된 솔루션

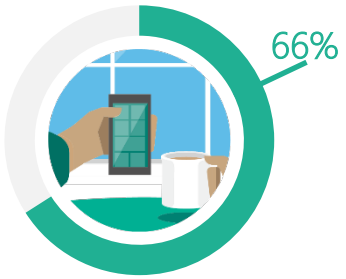
모든 사용자에게 동일환경

비즈니스와 IT 와의 GAP 존재

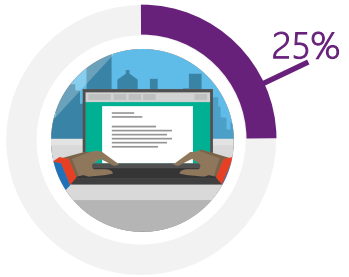
디바이스가 관리의 주체

응용프로그램	데이터	사용자

업무 방식의 변화



업무용으로 개인 기기를 사용



3대 이상의 디바이스로
여러 장소에서 다양한
앱을 이용해 업무를 수행

내근 직원 중 자주
자리를 떠나 업무 수행

사용자중심 업무환경

개인적 필요사항에 부합

기능마다 개인적 요청 상이

IT 는 Business 요구에 부합

모바일의 일상화

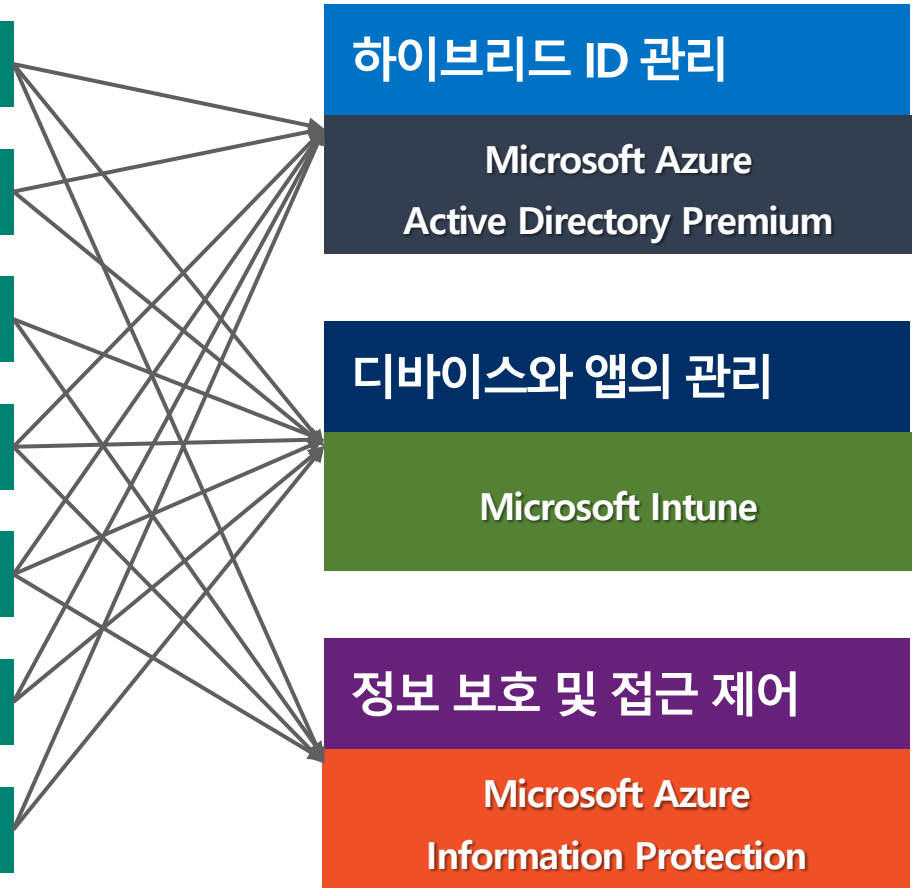
사용자가 관리의 주체

응용프로그램	데이터	디바이스

• EMS 개요

- 엔터프라이즈 이동 업무 방식의 지원을 위해 Microsoft EMS(Enterprise Mobility & Security)는 사용자가 관리의 주체가 되어 사용자의 디바이스나 위치에 상관없이 업무의 연속성을 가져가고 항상 엔터프라이즈 수준의 보안을 유지할 수 있습니다.

현업의 요구사항	모바일 업무 보안강화 방안
빠르게 변화되는 엔터프라이즈 업무 환경의 대응 필요	신규 OS에 대한 투자와 신속한 대응
많은 디바이스와 짧아진 수명 주기	사용자, 디바이스 중심의 관리(개인, 그룹)
업무의 이동성이 고려된 모바일 앱의 확장 요구	관리가 가능한 업무용 모바일 앱의 지원
디바이스, 플랫폼, 데이터에 걸쳐진 모든 레이어의 보호 요구	사용자 ID, 디바이스, 앱, 데이터 전반의 보호
다양한 모바일 디바이스를 수용하는 IT 환경	외부 모바일 업무 지원을 위한 클라우드 기반의 서비스 제공
이동 중에도 사내의 리소스에 대한 접근 요구	강력하고 간편한 인증과 사내 인프라와의 통합 인증 구성
디바이스에 대한 안전한 인증과 분실 관리	사용자 계정의 다중 인증 보안강화와 원격 디바이스 삭제



• EMS 구성

- 사용자 중심의 엔터프라이즈 이동 업무 강화를 위해 다양한 보안 솔루션을 제공합니다.

- 직원들이 선호하는 기기 사용을 허용하고, 직원들의 개인 기기를 사용하여 회사 리소스에 액세스할 수 있도록 지원함으로써 사용자 생산성을 증대.
(Windows, iOS, Android)

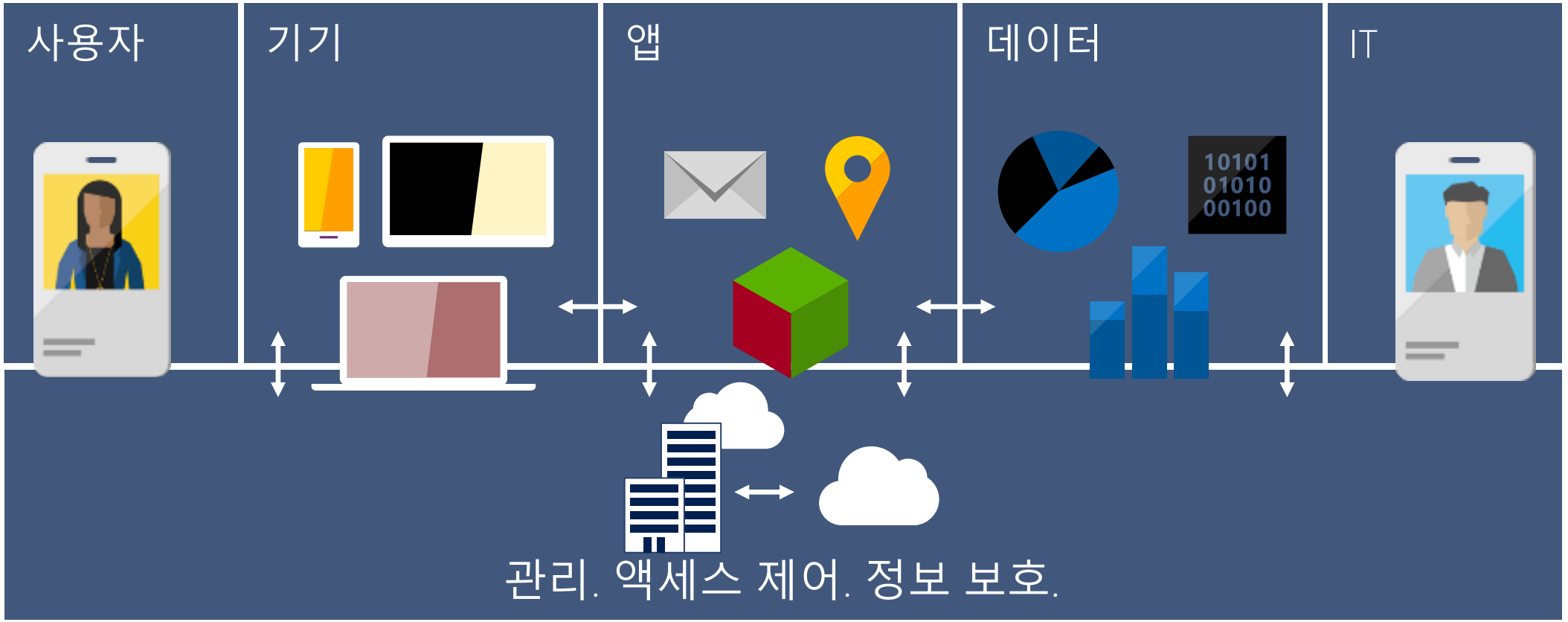
- 온-프레미스는 물론 클라우드 기반의 하이브리드 인증체계를 구현하여 시공간의 제약없는 정보의 공유 및 생산이 가능

- 사내 정보 보안정책적용 및 암호화, 인가되지 않은 접속의 제한, 기기 분실등 정보의 외부 반출등에 대한 대응을 통한 사내 자원에 대한 적극적 보호 가능

- Microsoft Azure 및 Office 365 등 Microsoft 기반의 클라우드 솔루션 및 타사 클라우드 솔루션 앱 , 솔루션 연계 가능

• 기대 효과

- Microsoft 의 Enterprise Mobility & Security(EMS)는 회사 내의 사용자가 회사의 어플리케이션과 데이터, 그리고 리소스를 어디서든지, 어떠한 디바이스로든 원하는 정보에 안전하고 긴밀하게 접근하도록 지원합니다.



엔터프라이즈 이동성 강화를 통해 새로운 모바일 사용자의 업무를 지원하고, 이동 환경에서도 회사의 리소스에 대한 보안 접근을 지원함으로써 위협은 낮아지고 업무 생산성 및 새로운 업무 환경에 대한 유연성 증대가 예상됩니다

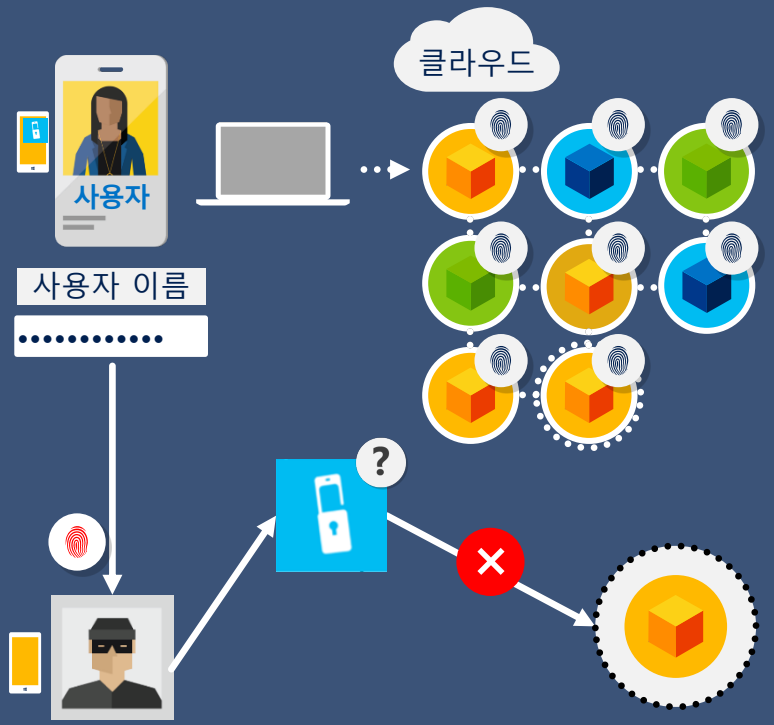
• 사용자 ID의 관리 및 보안 강화

Microsoft Azure
Active Directory Premium

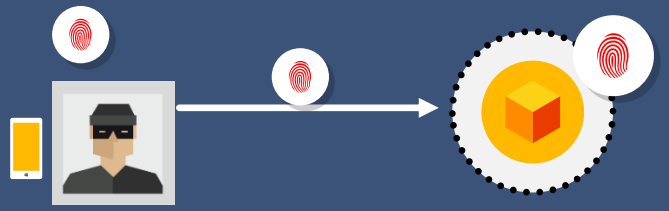
• 이동 업무 환경에서도 사용자의 ID를 관리하여 업무 시스템과의 인증 통합이 가능하며, 다중인증을 통해 보안을 한층 더 강화하여 사용자의 계정을 안전하게 보호할 수 있습니다.

① ID/PW가 너무 많고 앱 별로 입력하는 것이 너무 번거로움

SSO의 적용으로 인증 통합



② 사용자의 ID/PWD만으로는 보안 수준이 너무 낮음 (ID/PWD는 쉽게 노출됨)



다중 인증으로 보안 강화

[하이브리드 ID 검증 기능]

계정 및 그룹/사용자 관리

- 온프레미스 AD와 계정 동기화
- 사용자 라이선스 관리

앱 엑세스 패널

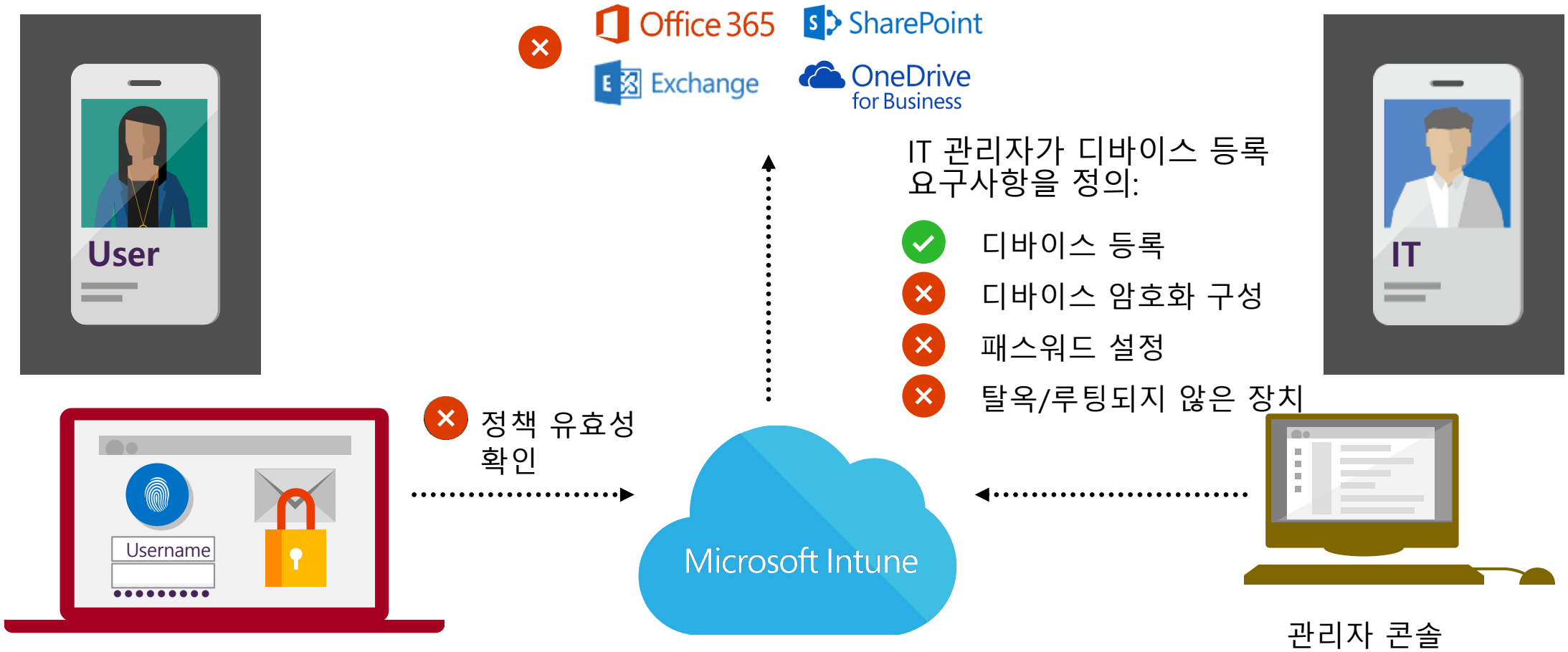
- 응용 프로그램 인증 통합 (SSO)
- 암호 변경 및 재설정

계정 보안

- 사용자 다중 인증 구성 / 확인
- 온프레미스 리소스 MFA 구성
- 온프레미스 ADFS 인증

• 조건부 액세스

- 정상적으로 등록된 디바이스에 대하여만 데이터에 액세스가 가능하도록 할 수 있습니다.



• 모바일 디바이스 관리

• 모바일 디바이스 및 디바이스 자원 관리, 정보유출 방지 등 다양한 기능을 제공합니다.

- 사용자가 직접 디바이스 등록 (셀프 서비스 포털)
- 원격 잠금
- 디바이스 공장 초기화
- 회사데이터 삭제
- 암호 재설정
- 데이터 암호화

디바이스 관리

정보유출 방지

- 중요 데이터 백업/복구/삭제
- 디바이스 기능 제어 (3G, Wi-Fi, 카메라, 녹음 등)
- 화면 캡쳐 방지
- 모바일 보안 정책 설정

- 디바이스정보 조회
- 소프트웨어 배포/관리
- 모바일 디바이스 Inventory 및 보고서
- MDM Agent 삭제 방지

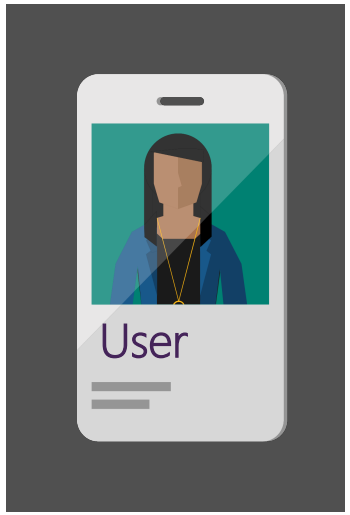
디바이스 자원관리

간편한 관리자 기능

- 웹 기반 단일 관리자 콘솔을 통한 통합관리
- 보안정책을 위한 연동 (인사DB, 출입시스템 등)
- 모바일 플랫폼 연동

• 모바일 앱의 관리

- 데이터 유출 방지 등을 위하여 관리되는 앱의 기능을 제어할 수 있습니다.



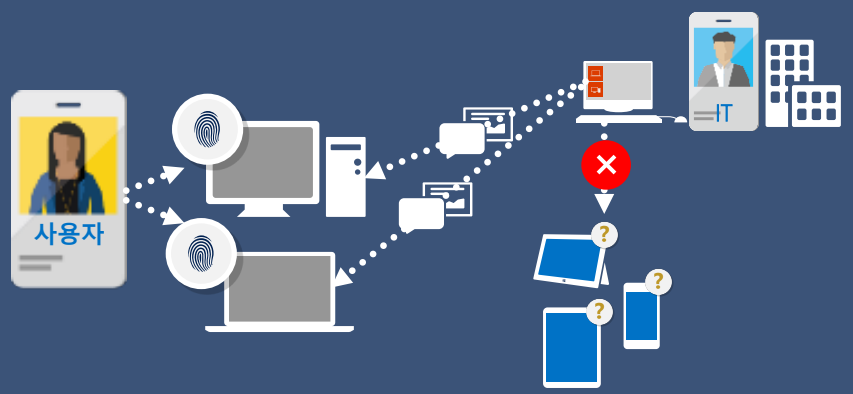
Copy/Cut/Paste/Save 등의 앱 내에서의 동작을 제어
회사 데이터 유출을 방지함으로써 앱 생태계의 관리와
함께 사용자 생산성의 향상 기대

• 시나리오 – 모바일 디바이스와 앱의 관리

Microsoft Intune

• 다양한 모바일 디바이스 및 디바이스 별 플랫폼과 앱을 모두 중앙에서 정책 배포를 통해 관리할 수 있으며, 분실/도난에 대해 디바이스를 원격에서 삭제함으로써 사용자의 편의성과 보안을 모두 고려한 모바일 디바이스 업무 환경을 제공할 수 있습니다.

① 관리되지 않는 디바이스는 회사의 리소스에 접근 차단

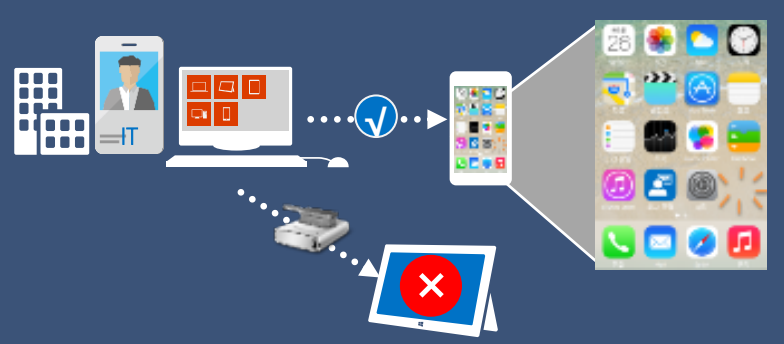


등록된 디바이스만 접근이 가능

② 관리되는 디바이스의 분실/도난에 대한 대책 필요

③ 앱의 허용과 차단 관리 필요

중앙에서 관리 정책을 적용



[MDM/MAM 검증 기능]

디바이스 관리

- 디바이스 등록 및 정책 배포
- 프로필 배포
  (Mail, Wi-Fi, VPN, 인증서)
- 디바이스 원격 삭제 및 초기화

회사 리소스 접근 제어

- 조건부 액세스
  (Exchange, SharePoint)

모바일 앱 관리

- 회사 관리용 앱 및 정책 배포
- 복사/붙여넣기/저장 통제

AIP(Azure Information Protection)

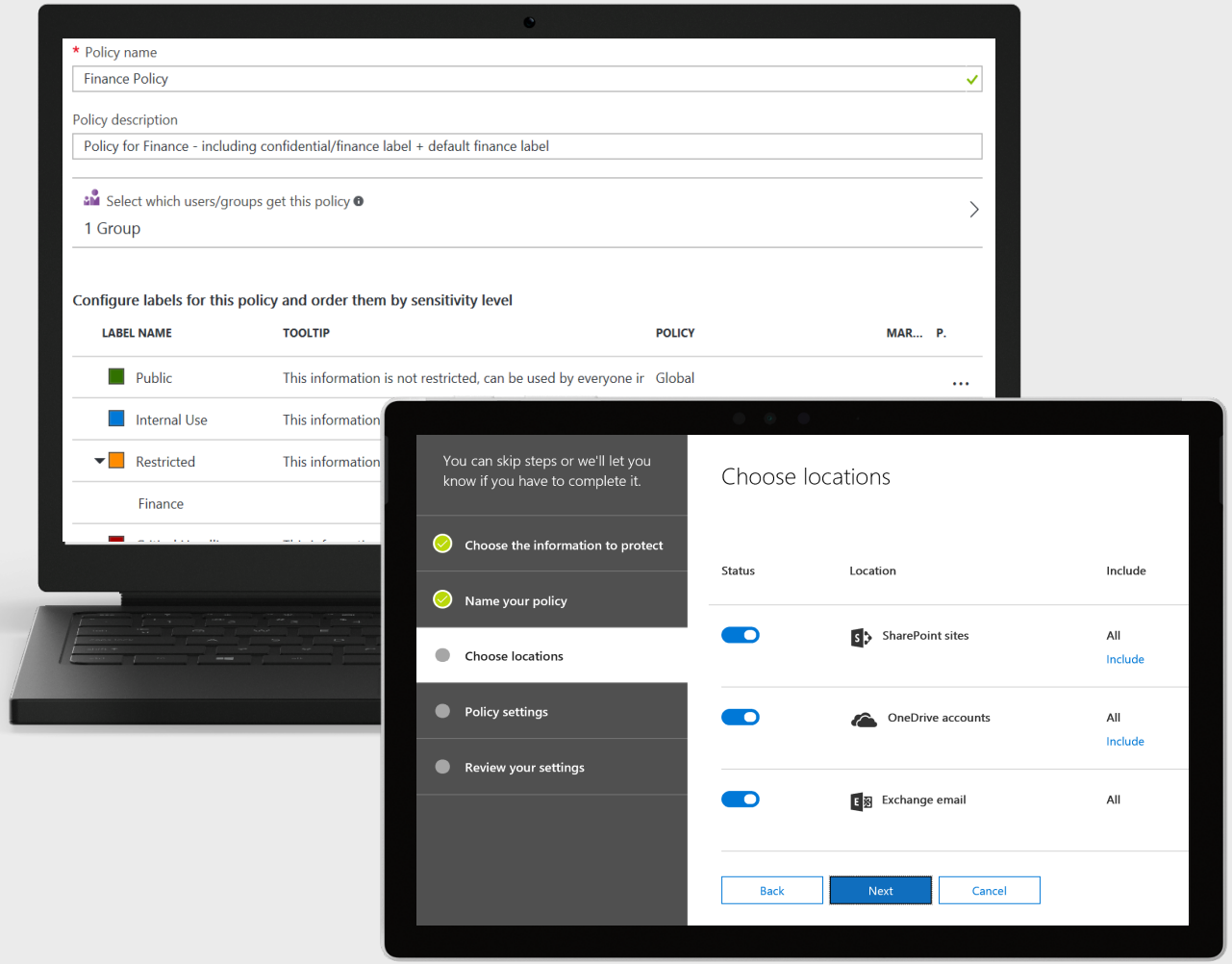
- 레이블을 적용하여 문서 및 전자 메일을 분류하고 보호합니다.

- 관리자가 정의한 규칙 및 조건을 자동으로 사용할 수 있습니다.
- 사용자가 수동으로 사용할 수도 있습니다.
- 권장 사항에 따라 자동 및 수동 방법을 결합할 수도 있습니다.

• 통합 레이블 정책 정의

• 레이블을 생성하여 정책을 적용 합니다.

- **특정 사용자 또는 그룹에 대한 정책 설정**
  - 해당 사용자 및 그룹의 구성원에만 정책 적용 가능
- **특정 위치를 대상으로 하는 정책**
  - Exchange Online 및 SharePoint Online과 같은 서비스 범위 지정 가능
- **레이블 스키마 및 설정 구성**
  - 레이블, 하위 레이블 및 필수 레이블, 기본 레이블 지정 등 다양한 설정 구성 가능



• 시나리오– 정보 보호와 접근 제어

Microsoft Azure Information Protection

- 이동 환경에서도 업무 간에 공유되는 데이터를 사용자 기준으로 공유 정보의 권한을 설정하도록 하여 잘 못 공유된 경우에도 데이터를 안전하게 보호할 수 있으며, 정보에 대한 사용 권한의 설정이 가능하여 정보의 공유와 유출을 방지할 수 있습니다.

① 클라우드 환경에서 중요 데이터에 대한 보호 및 인가된 사용자만 접근이 가능하도록 필요

② 보호된 문서에 대해 사용자 역할과 권한에 따른 동적으로 접근을 제어할 수 있는 권한 관리 필요

[정보 보호 검증 기능]

사용자 기반의 정보 보호

- 메일의 전달금지 설정
- 수신자 기반의 문서 열람 권한
- 다양한 파일의 보호 지원 (PDF, TXT, JPG, PNG 등)

문서의 사용 권한

- 읽기/편집/복사/저장/인쇄 등에 대한 제어

Thank you