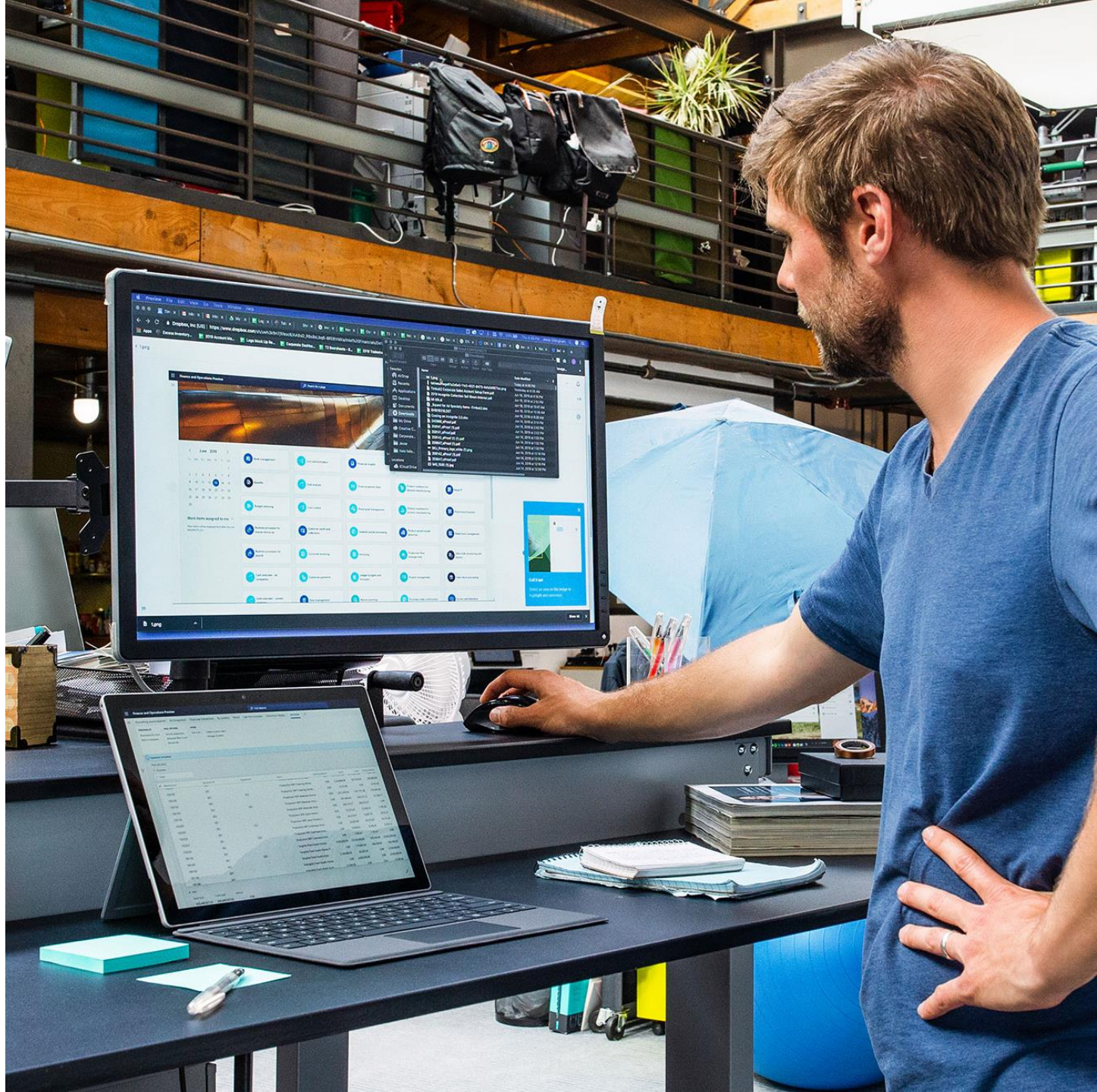
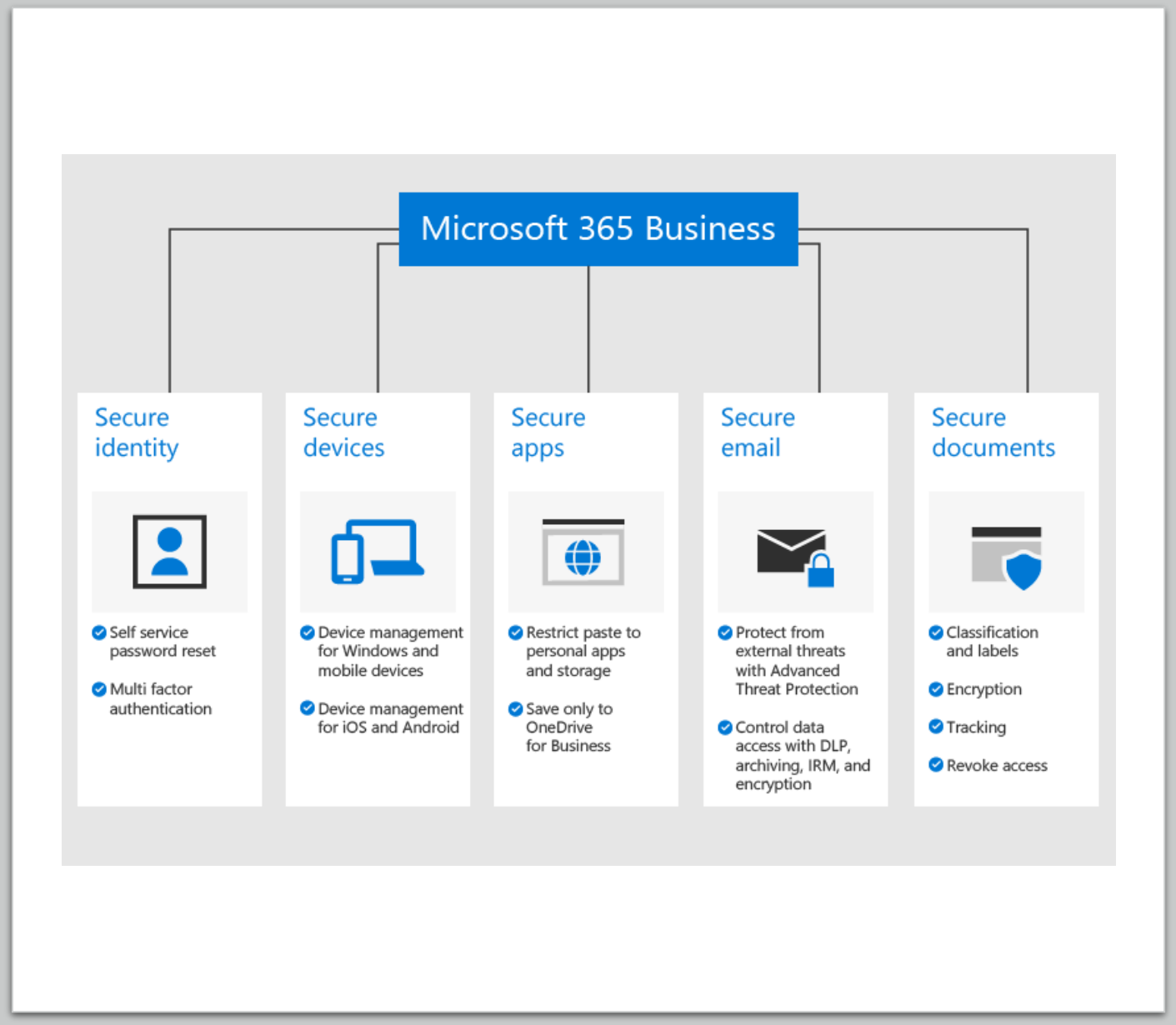
Microsoft365 Business Premium

Security Deployment

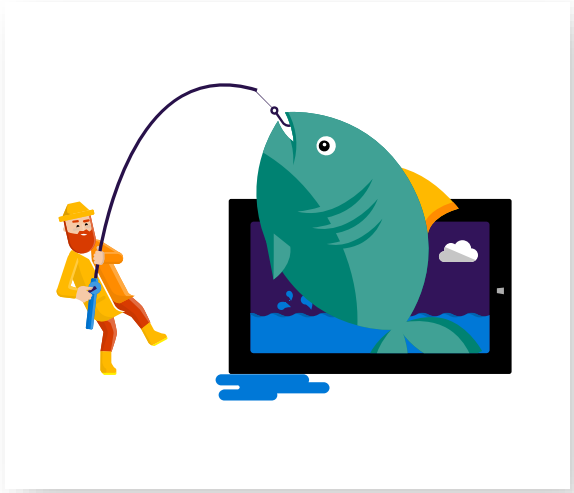


Microsoft365 Business Premium

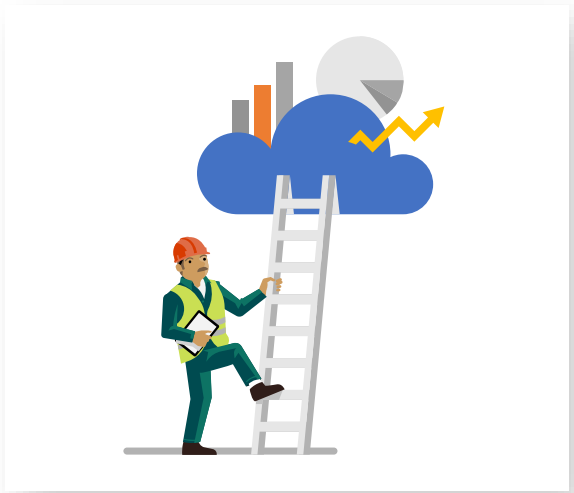
Microsoft 365 Business Premium은 직원의 수가 300명 미만인 비즈니스를 위한 포괄적인 구독 서비스입니다. 좋아하는 Office 생산성 앱 및 서비스와 Microsoft Teams와 같은 공동 작업 도구를 고급 보안 및 장치 관리 기능과 통합 합니다.



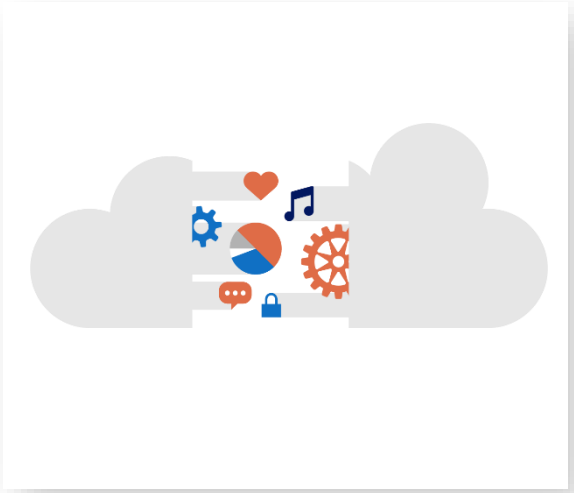
사이버위협 대응과 비즈니스 데이터 보호



Protect users against cyberthreats like phishing



Safeguard confidential business data



Get visibility into cloud app use

이메일 위협으로부터 보호

GoWorks

사전 설정 보안 정책

기본 제공 보호

기본 제공 Microsoft Office 365 보안은 조직의 모든 사용자에게 적용되어 악의적인 링크 및 첨부 파일로부터 보호합니다.

- ✓ 추가 기계 학습 모델
- ✓ 더욱 공격적인 데토테이션 평가
- ✓ 환경의 시각적 표시

메모: 기본 제공 보호 기능은 Office 365용 Microsoft Defender 테넌트에 대해서만 사용할 수 있습니다.

제외 추가(권장되지 않음)

표준 보호

스팸, 피싱 및 맬웨어 위협으로부터 보호하는 기준 보호 프로필입니다.

- ✓ 악성 콘텐츠에 대한 균형 잡힌 작업
- ✓ 대량 콘텐츠의 균형 처리
- ✓ 안전한 링크 및 안전한 첨부 파일을 통한 첨부 파일 및 링크 보호

표준 보호 기능이 켜져 있습니다.

보호 설정 관리

엄격한 보호

높은 가치의 대상 또는 우선 순위 사용자와 같이 선택한 사용자에 대한 보다 강력한 보호 프로필입니다.

- ✓ 악성 메일에 대한 보다 공격적인 작업
- ✓ 대량 보낸 사람에 대한 제어 강화
- ✓ 더욱 공격적인 기계 학습

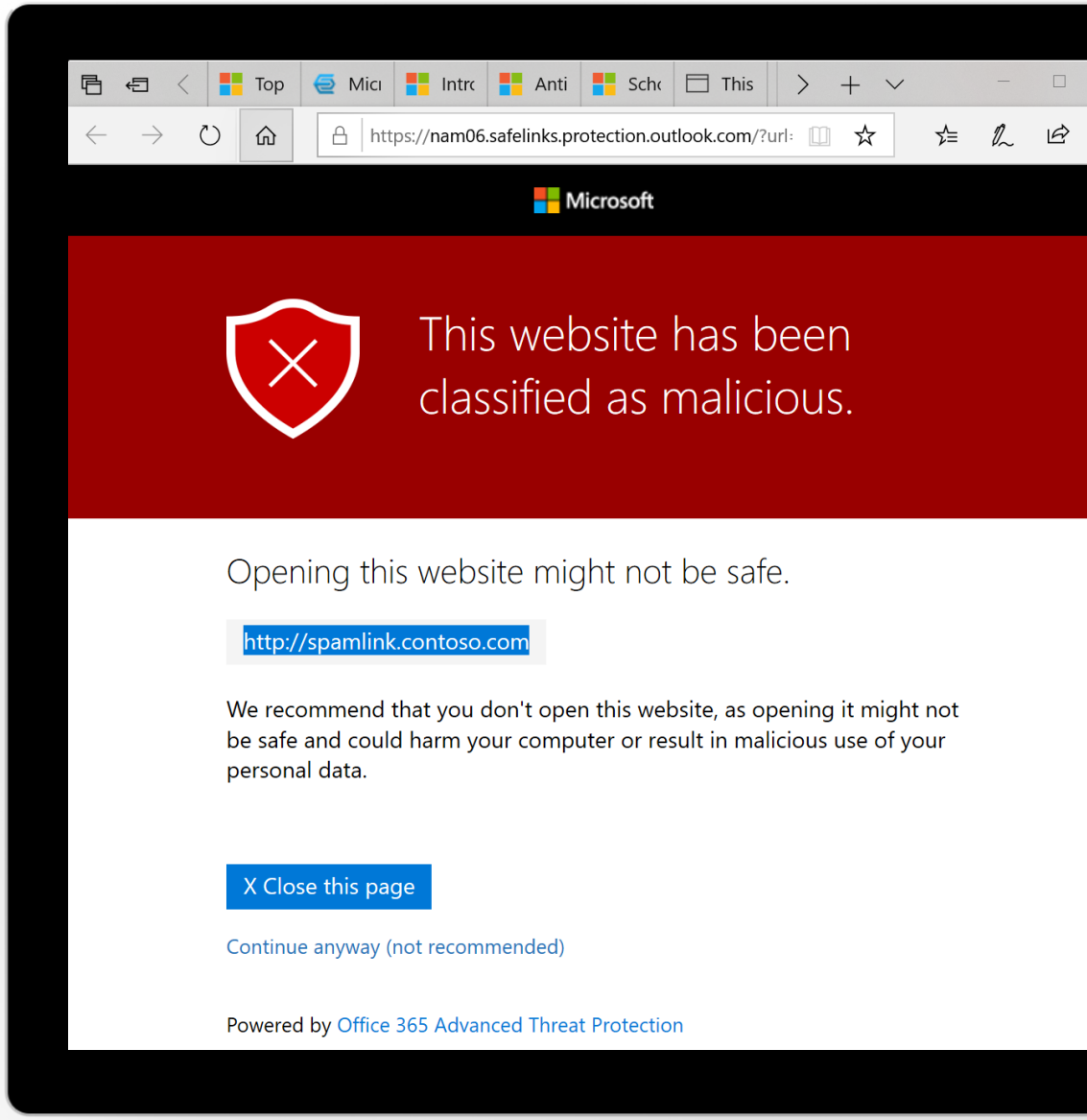
엄격한 보호 기능이 켜져 있습니다.

보호 설정 관리

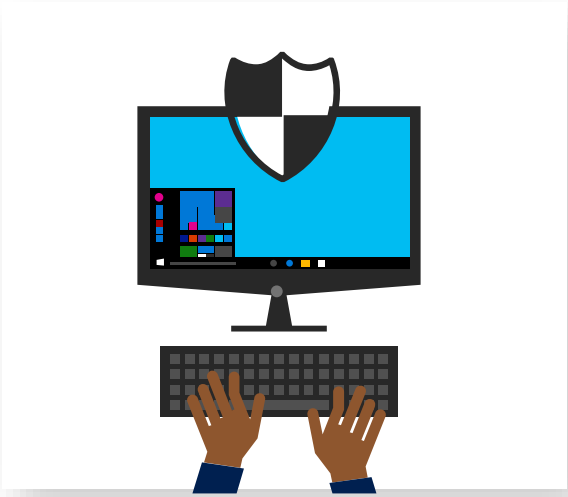
gowit
on your side

위협으로부터 보호

- 실시간으로 전자 메일과 문서의 링크를 검색하여 안전하지 않은 웹 사이트를 차단합니다(ATP 안전한 링크)
- 샌드박스 환경에서 전자 메일 첨부 파일에 대한 고급 분석을 수행하여 새로 개발된 맬웨어를 탐지합니다(ATP 안전한 첨부 파일)
- 기계 학습 모델과 가장 탐지 기능을 사용하는 피싱 방지 정책을 활성화하여 고급 공격으로부터 보호합니다(ATP 피싱 방지 인텔리전스)

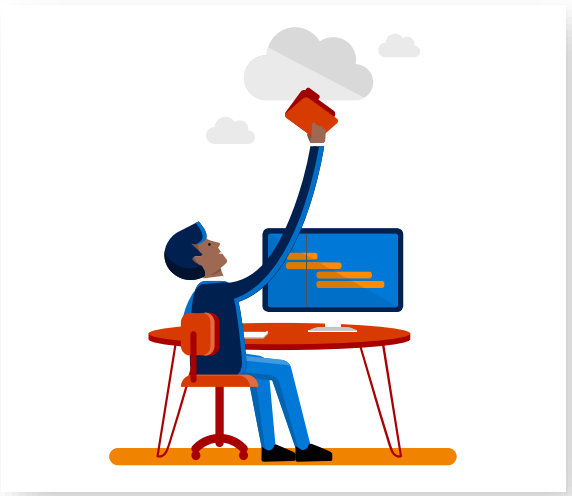


안전한 ID 관리와 접근관리



비밀번호 분실, 탈취로 부터 사용자 계정 보호

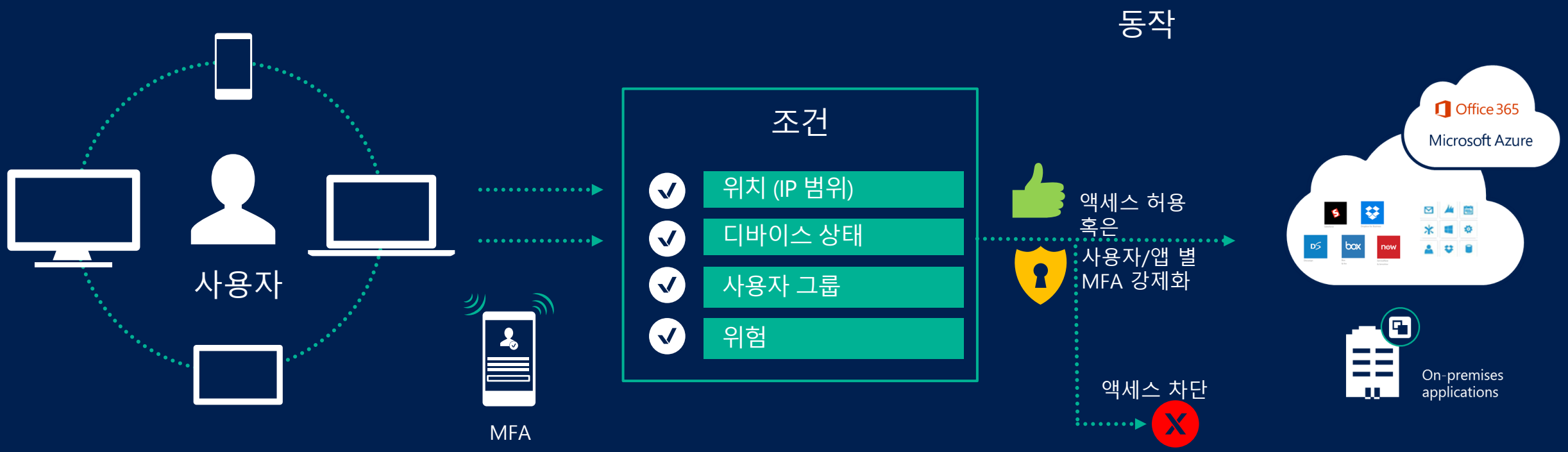
업무용 앱의 안전한 접근



원격 PC로 부터 안전한 접속

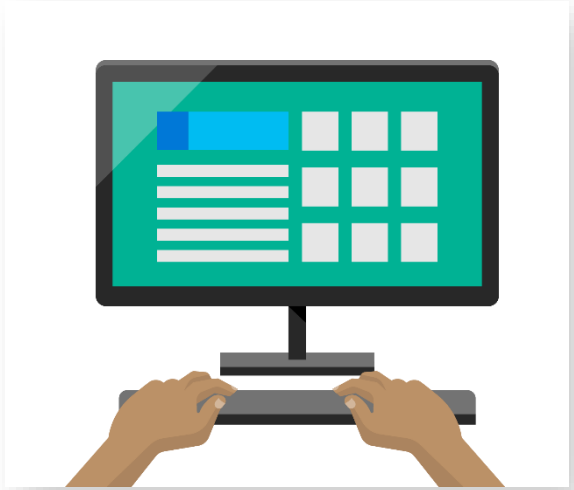
GowIT

Identity 기반identity-driven 보안



회사의 데이터에 액세스하는 장치 보안 및 관리

모바일 기기에서
회사데이터 관리



Windows
PC 보안 관리

Autopilot을 이용한
자동 배포

장치 보호

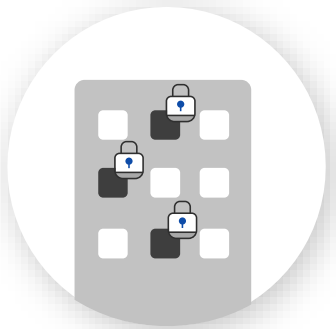
- 사용자가 집 컴퓨터, 승인되지 않은 앱에서 또는 근무 외 시간에 로그인하지 못하도록 차단하는 옵션을 사용하여 Microsoft 데이터에 액세스할 수 있는 장치와 사용자를 제어합니다.(조건부 액세스)
- iOS와 Android 장치에서 비즈니스 데이터를 보호하기 위해 보안 정책을 적용합니다. 예를 들어 사용자가 비즈니스 데이터에 액세스하는 데 PIN 또는 지문을 제공하도록 요청하고 모바일 장치에서 데이터를 암호화할 수 있습니다.(Office 모바일 앱에 대한 앱 보호)
- 승인된 Office 모바일 앱 내에 비즈니스 문서, 전자 메일 및 기타 데이터를 보관하고 직원이 이를 승인되지 않은 앱과 위치에 저장하지 못하도록 합니다.(Office 모바일 앱에 대한 앱 보호)
- 개인 정보에 영향을 주지 않고 분실하거나 도난당한 장치에서 비즈니스 데이터를 원격으로 지웁니다.(Intune 선택적 지우기)
- 간단한 컨트롤을 사용하여 회사의 모든 Windows 10 PC에 대한 정책을 관리하고, BitLocker 암호화를 적용하고, 중요한 Windows 업데이트를 자동으로 설치합니다.(Windows 업데이트 정책 적용)
- 사내 응용프로그램과 모바일 앱을 사용자 장치에 자동으로 설치 할 수 있습니다.

모바일 장치 관리

Mobile Device Management (MDM)

- 장치등록
- 설정, 인증서, 프로필 관리
- 장치의 등록 및 준수상태 확인
- 원격 장치 데이터 삭제

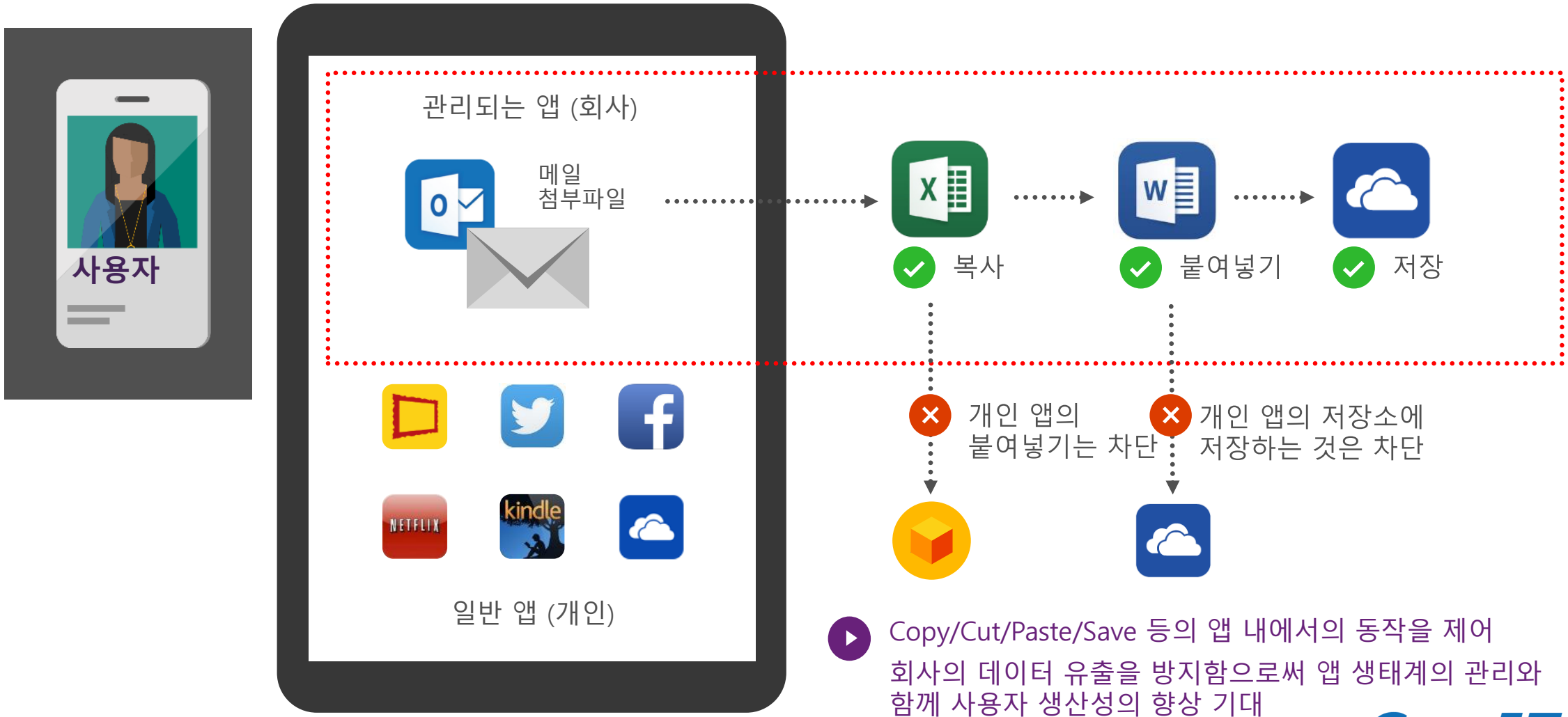
Mobile Application Management (MAM)



- 모바일 앱 배포
- 앱 설정 및 업데이트 관리
- 개인 기기에 회사 데이터 저장 금지
- 모바일 앱 데이터 내에서 회사데이터 보호

GowIT

MAM회사 데이터 보호



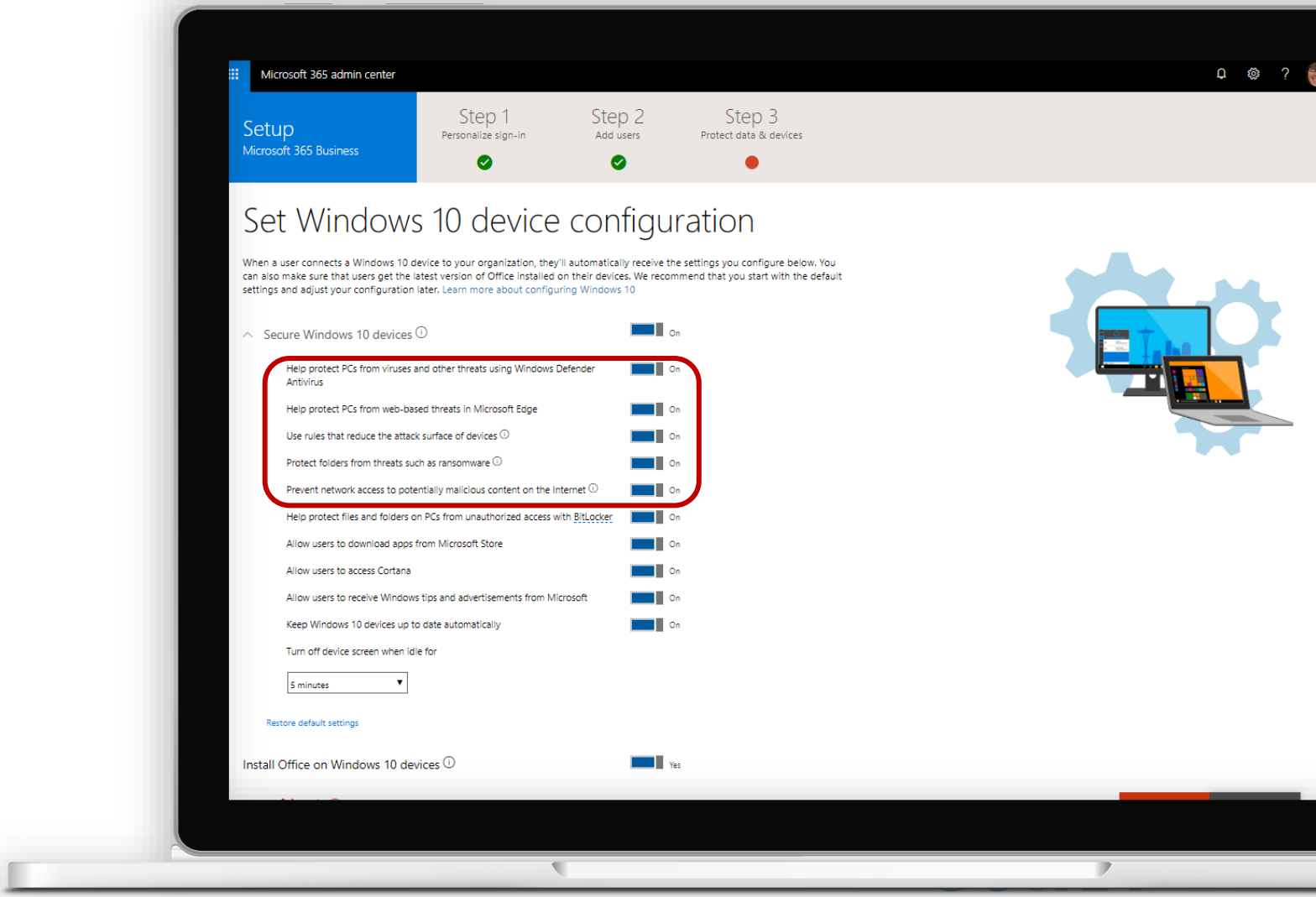
Copy/Cut/Paste/Save 등의 앱 내에서의 동작을 제어

회사의 데이터 유출을 방지함으로써 앱 생태계의 관리와 함께 사용자 생산성의 향상 기대

GowIT

Windows devices 장치 보안

- Windows 10 devices 자동 업데이트 설정
- Microsoft Defender protections 강제 활성화
- BitLocker encryption활성화를 통해 데이터 보호

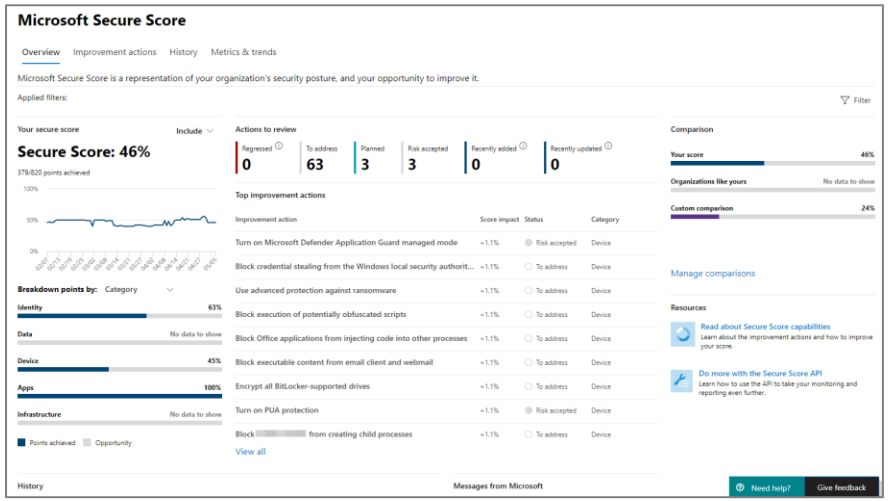


비즈니스 데이터 보호

- 주민등록번호 또는 신용 카드와 같은 중요한 정보가 회사 외부로 유출되는 것을 방지할 수 있습니다.(데이터 손실 방지)
- 중요한 전자 메일을 암호화하여 고객 또는 조직 외부의 사용자와 안전하게 의사 소통합니다. 암호화를 사용하면 받는 사람만 메시지를 읽도록 할 수 있습니다.(Office 365 메시지 암호화)
- 전자 메일 및 문서에 복사 금지 및 전달 금지와 같은 제한 사항을 적용하여 회사 정보에 액세스할 수 있는 사용자를 제어합니다.(Azure Information Protection)
- 무제한 클라우드 보관을 활성화하여 이전 직원의 사서함을 포함하여 조직의 모든 전자 메일을 보관합니다.(Exchange Online 보관)
- 보안 및 준수 센터에서 감사 로그 검색을 켠 후에는 & 로그에서 관리자 및 기타 사용자 활동을 유지 하 고 검색할 수 있습니다.
- SharePoint 및 OneDrive 파일 및 폴더에 대한 공유 설정 조정을 통해 외부와 공유되는 데이터에 대한 유출을 방지할 수 있습니다.
- 활동 알림을 사용 하 여 관리자 및 사용자 활동을 추적 하 고 조직의 데이터 손실을 방지할 수 있습니다.

모니터링

- 사용자 로그인등 Azure AD 내의 다양한 기능에 의해 수행된 모든 변경 내용에 대한 로그를 통한 추적 기능을 제공합니다.
- 경고 정책을 사용하여 조직의 사용자 및 관리자 활동, 맬웨어 위협 또는 데이터 손실등 위협을 추적합니다
- Office 365 감사로그 검색을 통해 사용자가 특정 문서를 보았는지 또는 사서함에서 항목을 제거했는지 확인 할 수 있습니다.
- Microsoft 365 보안 센터의 중앙 집중식 대시보드를 통해 id, 데이터, 앱, 장치 및 인프라의 보안을 모니터링 할 수 있습니다.
- 보안 점수는 조직의 보안 상태를 측정 한 값으로 권장 사항을 따라 위협으로부터 조직을 보호할 수 있습니다



GowIT

Microsoft 365
POC

GowIT

시나리오 1: 회사 장치 등록

모바일 디바이스의 메일 앱을 실행하여 회사 메일을 설정해 봅니다.

목적

- 스마트폰과 같은 모바일 기기를 통해 회사의 중요 메일을 열람할 때 보안을 강화 할 수 있습니다.
- 안전하지 않는 디바이스로 회사의 리소스에 접근하는 악의적인 행위를 미연에 방지할 수 있습니다.

특징

- 사용자는 디바이스를 등록 과정에서 회사의 보안 정책이 적용되며 정책에 준수하는 디바이스만 리소스에 접근할 수 있습니다.
- 회사 메일 뿐만 아니라, SharePoint, OneDrive for Biz와 같은 업무 시스템에 적용할 수 있습니다.
- 온프레미스 환경에 대한 조건부 접근도 구성이 가능합니다.

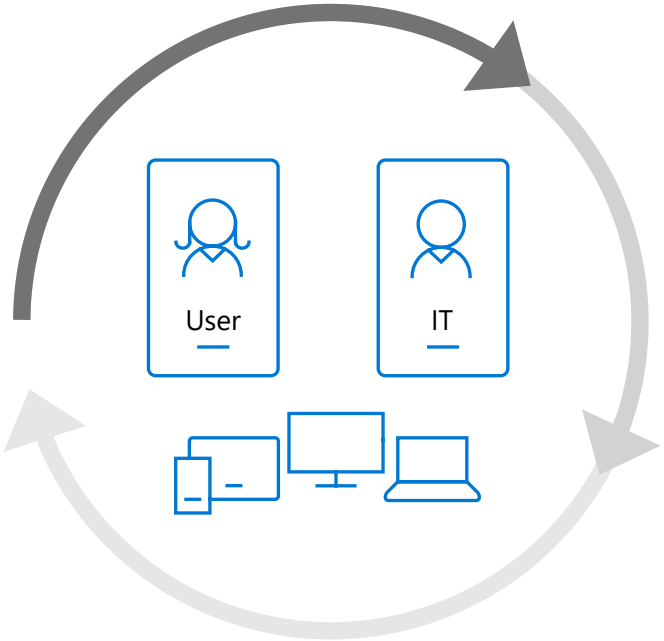
Device Lifecycle

Enroll

- ✓ Provide specific enrollment methods for iOS/iPadOS, Android, Windows, and macOS
- ✓ Provide a self-service Company Portal for users to enroll BYOD devices
- ✓ Deliver custom terms and conditions at enrollment
- ✓ Zero-touch provisioning with automated enrollment options for corporate devices

Configure

- ✓ Deploy certificates, email, VPN, and Wi-Fi profiles
- ✓ Deploy device security policy settings
- ✓ Install mandatory apps
- ✓ Deploy device restriction policies
- ✓ Deploy device feature settings



Support & Retire

- ✓ Revoke access to corporate resources
- ✓ Perform selective wipe
- ✓ Audit lost and stolen devices
- ✓ Retire device
- ✓ Provide Remote Assistance

Protect

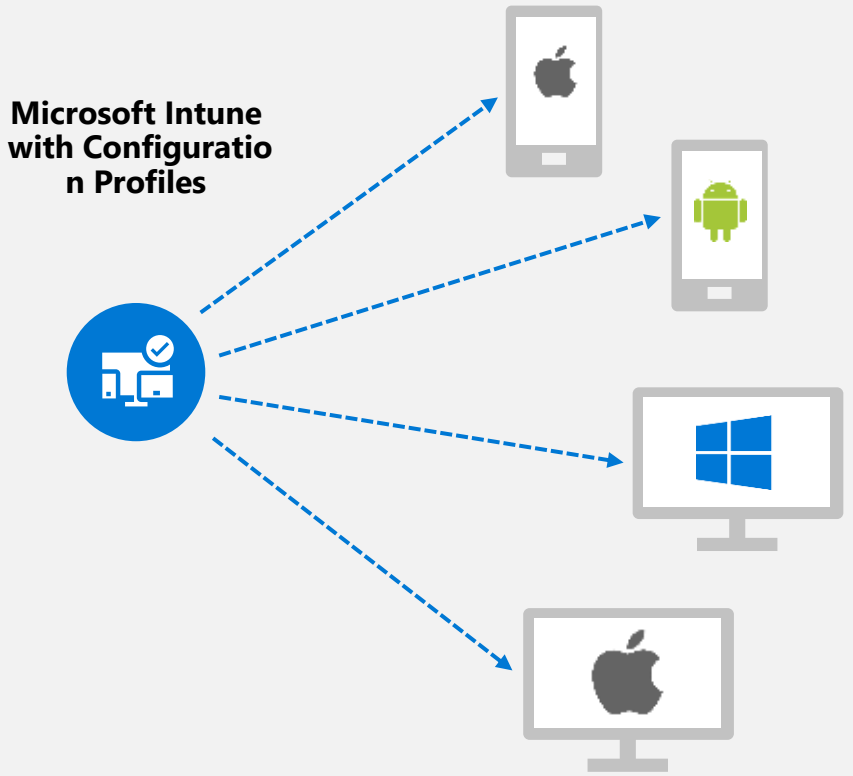
- ✓ Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- ✓ Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- ✓ Report on device and app compliance

What are Configuration Profiles?

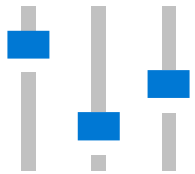
Microsoft Intune provides **Configuration Profiles** which includes **settings** and **features** that can be enabled or disabled on different devices within your organization.

Configuration Profiles can be applied to:

- iOS/iPadOS devices
- Android devices
- Windows 10 devices
- macOS devices



What do Configuration Profiles provide?



Device features

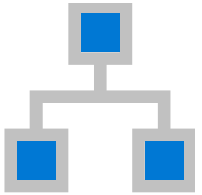
Controls features on the device.

Examples: Airprint, notifications and lock screen messages.

Device restrictions

Controls security, hardware, data sharing and more settings on the devices.

Examples: require a PIN, data encryption, etc.



Access configuration

Provide organization's access configuration to the device.

Examples: email profiles, VPN profiles, Wi-Fi settings, certificates, etc.

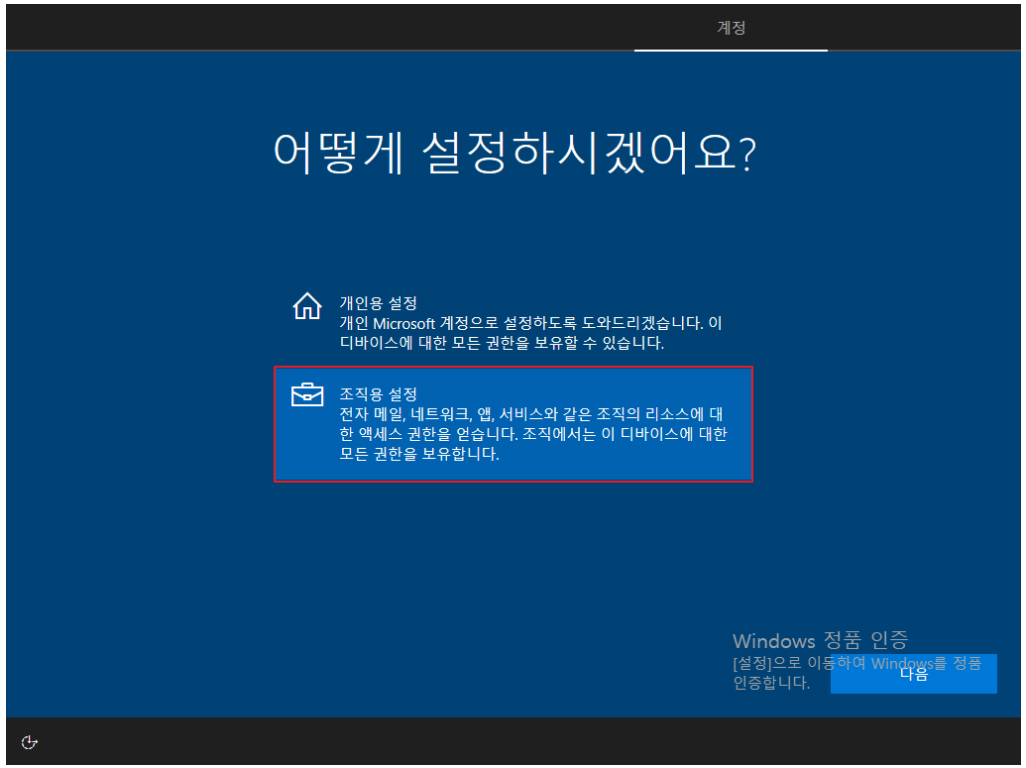
Custom

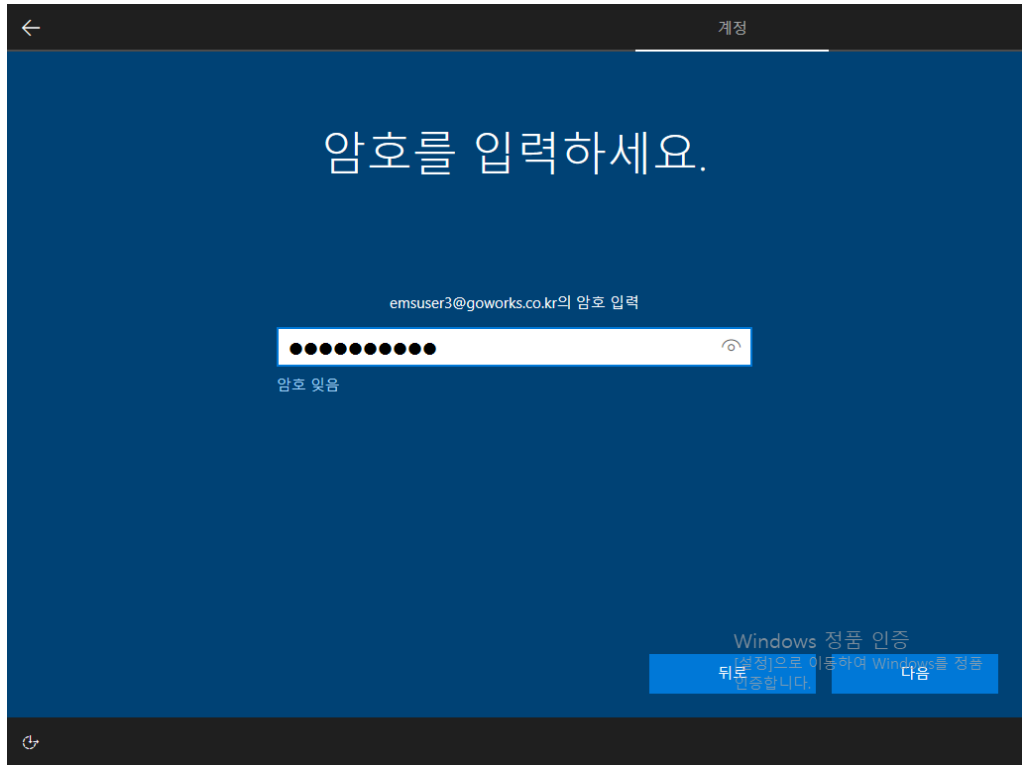
Set custom configuration or execute custom configuration actions.

Examples: set OEM settings, execute PowerShell scripts, etc.

사용자 Windows 장치 등록(설치 시 등록)

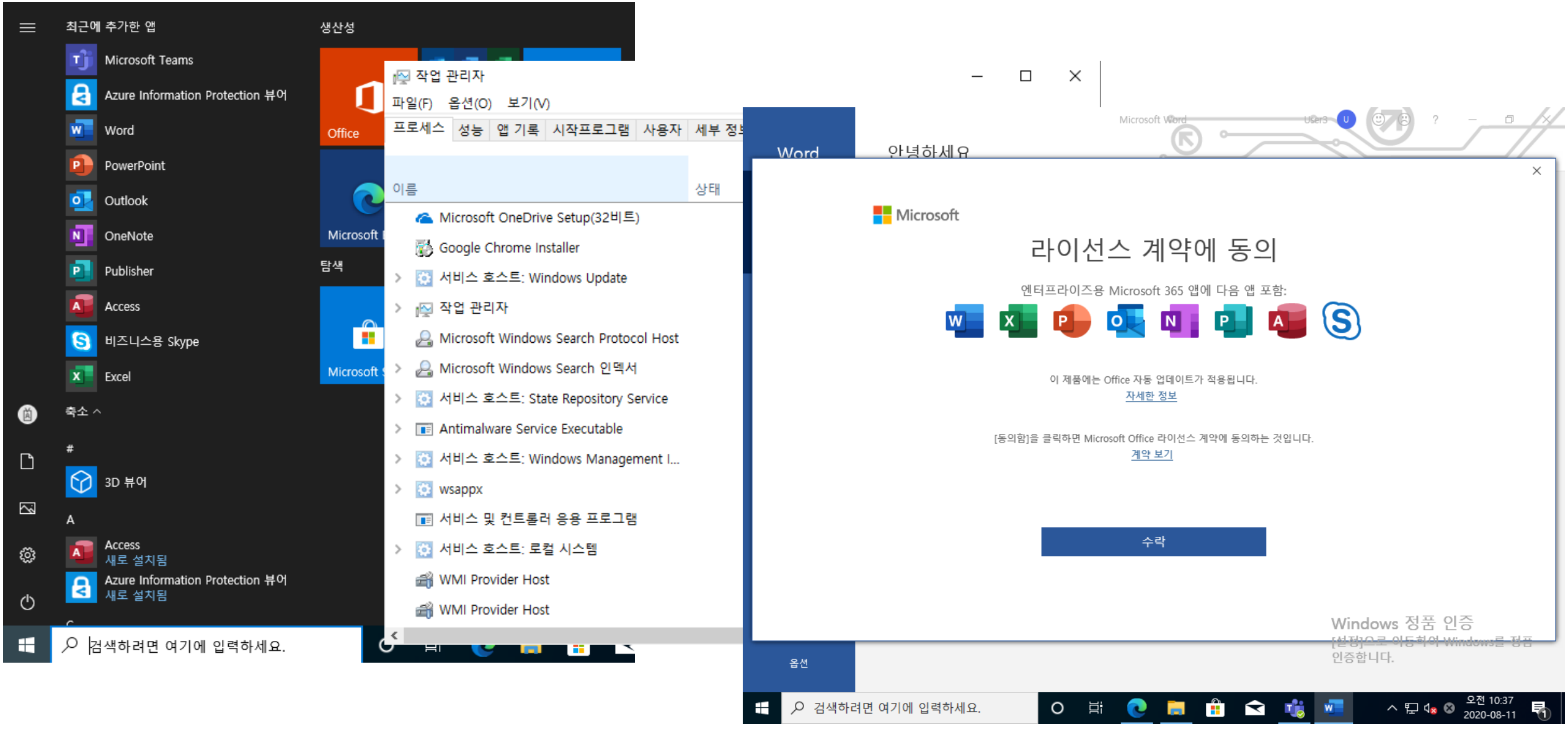
- 설정을 일부 완료하면 계정에 대하여 묻는 항목이 표시됩니다. 해당 설정에서 "조직용 설정"을 통해 회사의 계정을 등록합니다.





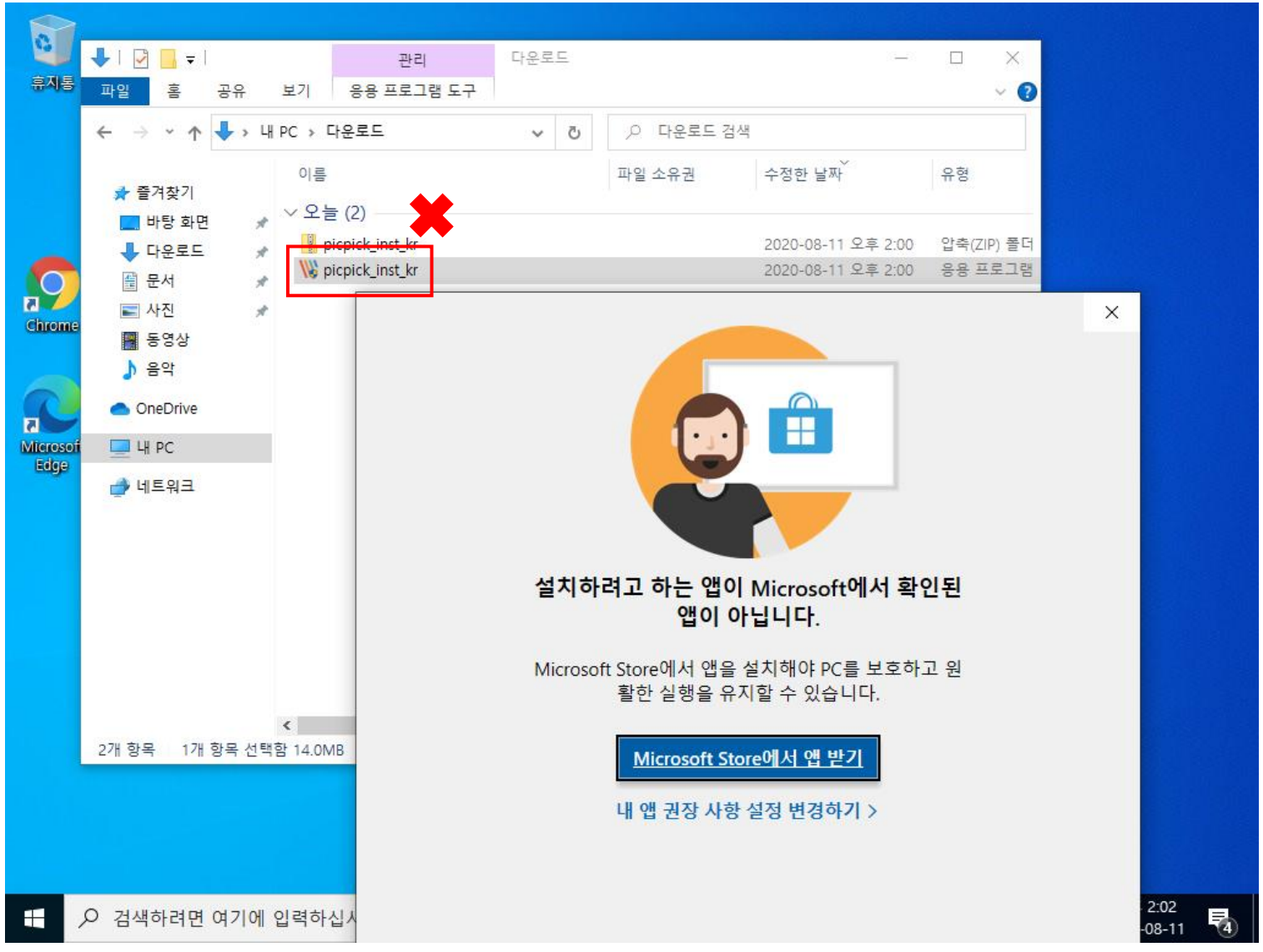
사용자 Windows 10 설정

- 등록이 완료된 Windows 10 설정에서 Teams, Outlook, Chrome, AIP, Edge와 같은 필수 업무 응용 프로그램 배포가 된 것을 확인합니다.

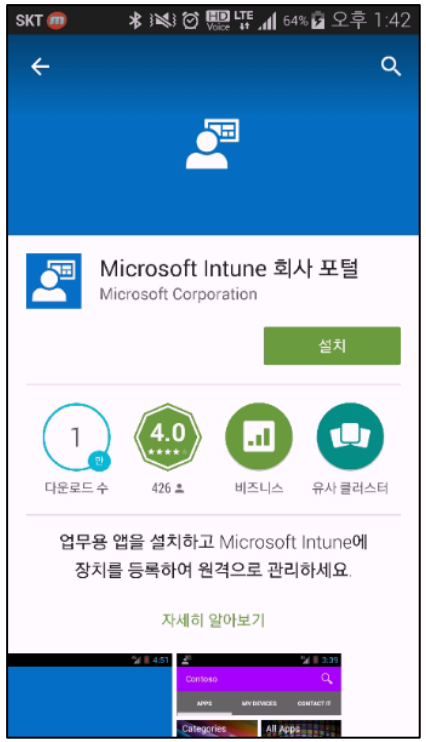


사용자 Windows 10 설정

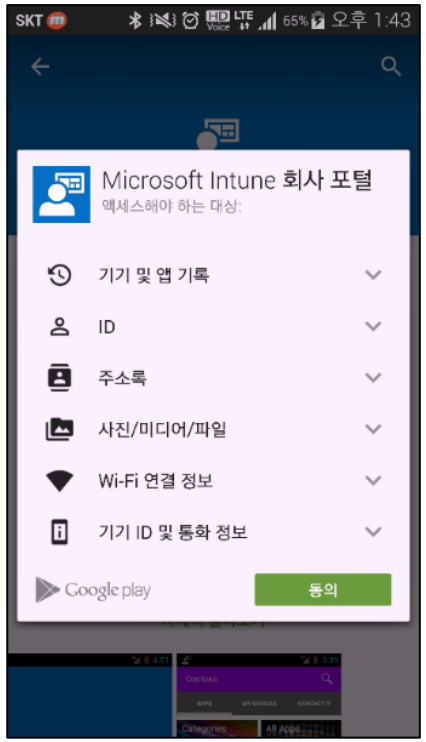
- 사용자는 PC에 일반적인 프로그램을 설치할 수 없습니다.
  관리자의 설정에 따라 Windows 앱 스토어에서 인가된 앱만 설치하거나, 중앙에서 배포되는 앱만 사용할 수 있습니다.



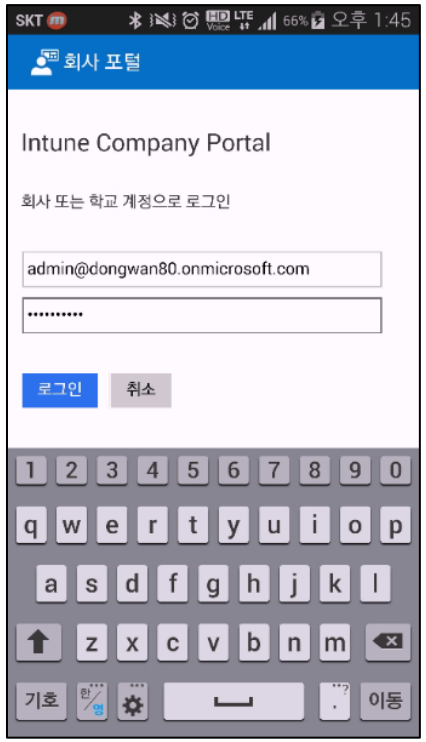
모바일 장치 등록



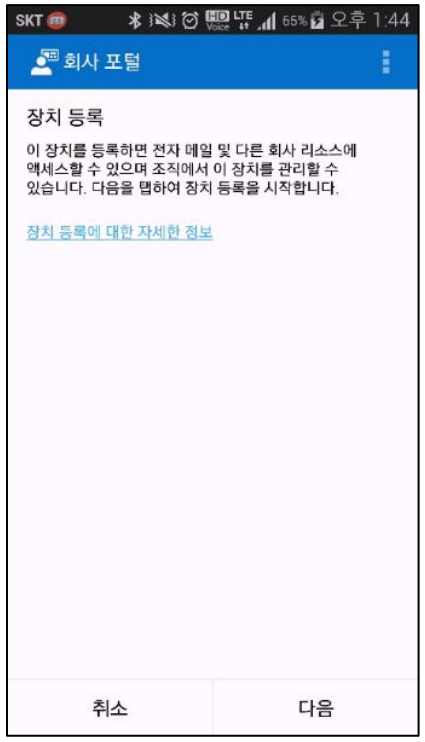
구글플레이에서
회사포털 검색



회사포털 설치



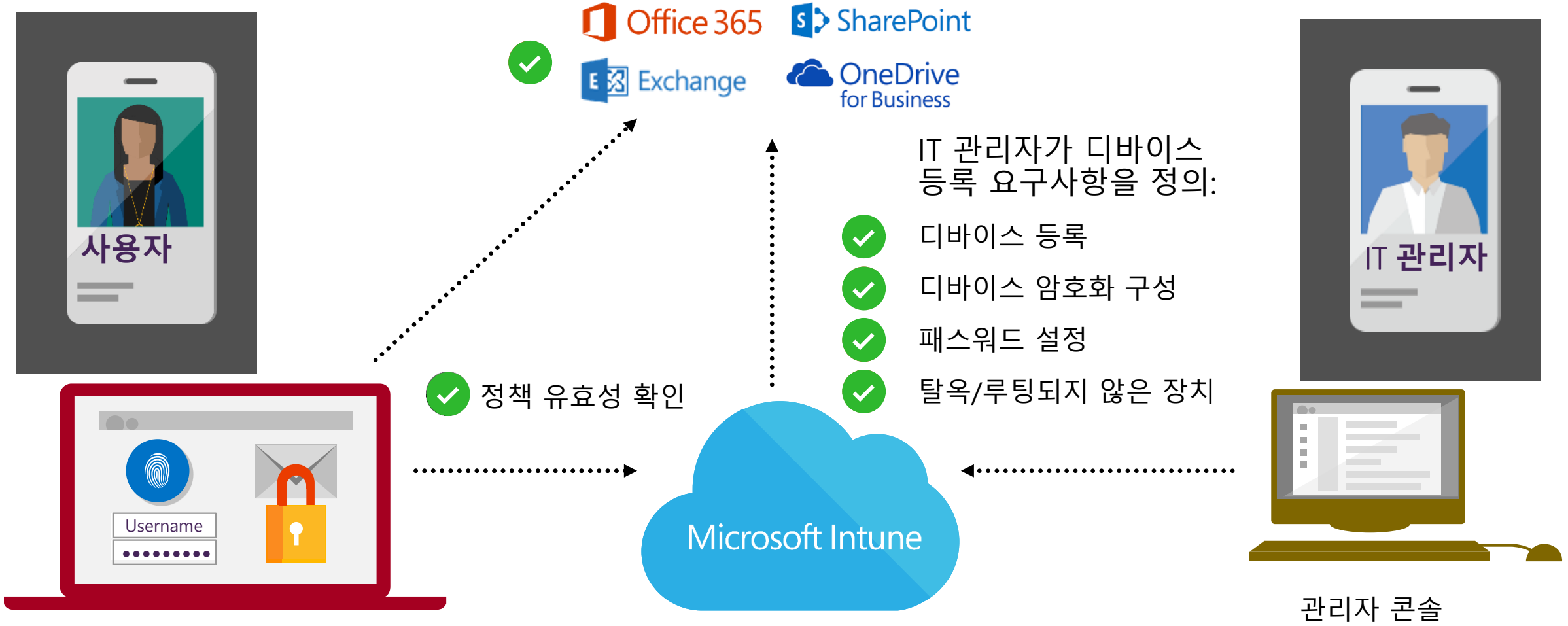
회사 계정 로그인



장치 등록

회사포털 화면

전자 메일에 대한 조건부 액세스



시나리오 2: 로그인 보안 강화

모바일 디바이스로 업무 시스템에 로그인하는 과정에서 추가 인증을 하여 계정 보안을 향상시킬 수 있습니다.

목적

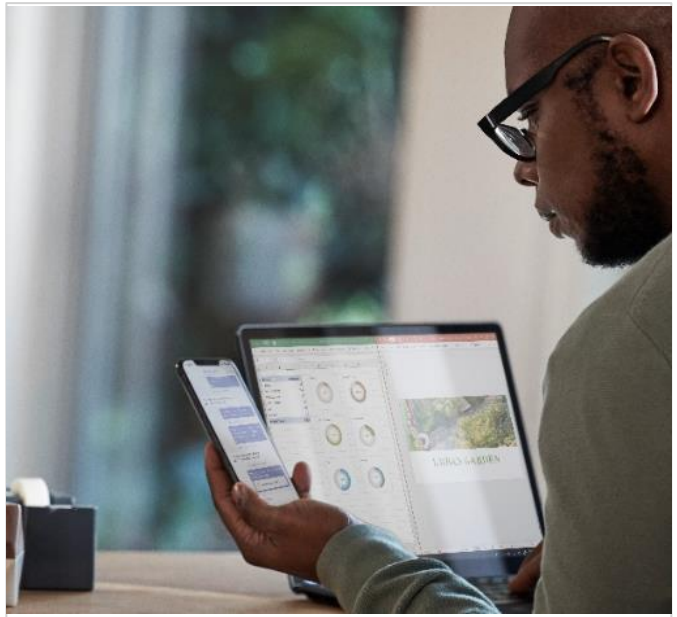
- 모바일 디바이스로 회사의 시스템에 로그인 시 사용자의 ID/PWD에 대한 유출 및 악의적인 로그인을 방지 할 수 있습니다.
- ID와 PWD 인증에 추가로 제공되는 추가 인증을 적용하여 사용자의 계정 인증에 대한 보안을 강화할 수 있습니다.

특징

- 사용자의 ID/PWD만을 통한 인증은 노출과 유출의 위험이 있으므로 추가 인증(MFA) 구성을 통해 사용자 인증 보안을 강화 할 수 있습니다.
- 추가 인증 구성은 클라우드와 온프레미스 모두 구성할 수 있습니다.
- 사내 업무시스템에 대한 2단계 인증 구성도 지원합니다.

Multi-Factor Authentication (MFA)

Verify user identities with strong authentication to establish trust



We support a broad range of multi-factor authentication options

Push Notification

SMS, Voice

Soft Tokens OTP

Hard Tokens OTP

Including passwordless technology

Microsoft Authenticator

Windows Hello

FIDO2 Security key

Biometrics

Multi-factor authentication prevents 99.9% of identity attacks

Ways to enable Azure MFA

Azure Multi-factor Authentication can be enabled in these three ways:

Conditional Access

The most versatile way of enabling MFA.

Recommended approach.

Security Defaults

Enables MFA for all users.

Recommended primarily for small business, with careful consideration.

Per-user account

Legacy way of enabling MFA.

Not recommended.

Azure MFA with Conditional Access

Azure MFA enabled through Conditional Access policies which are applied during sign in time to

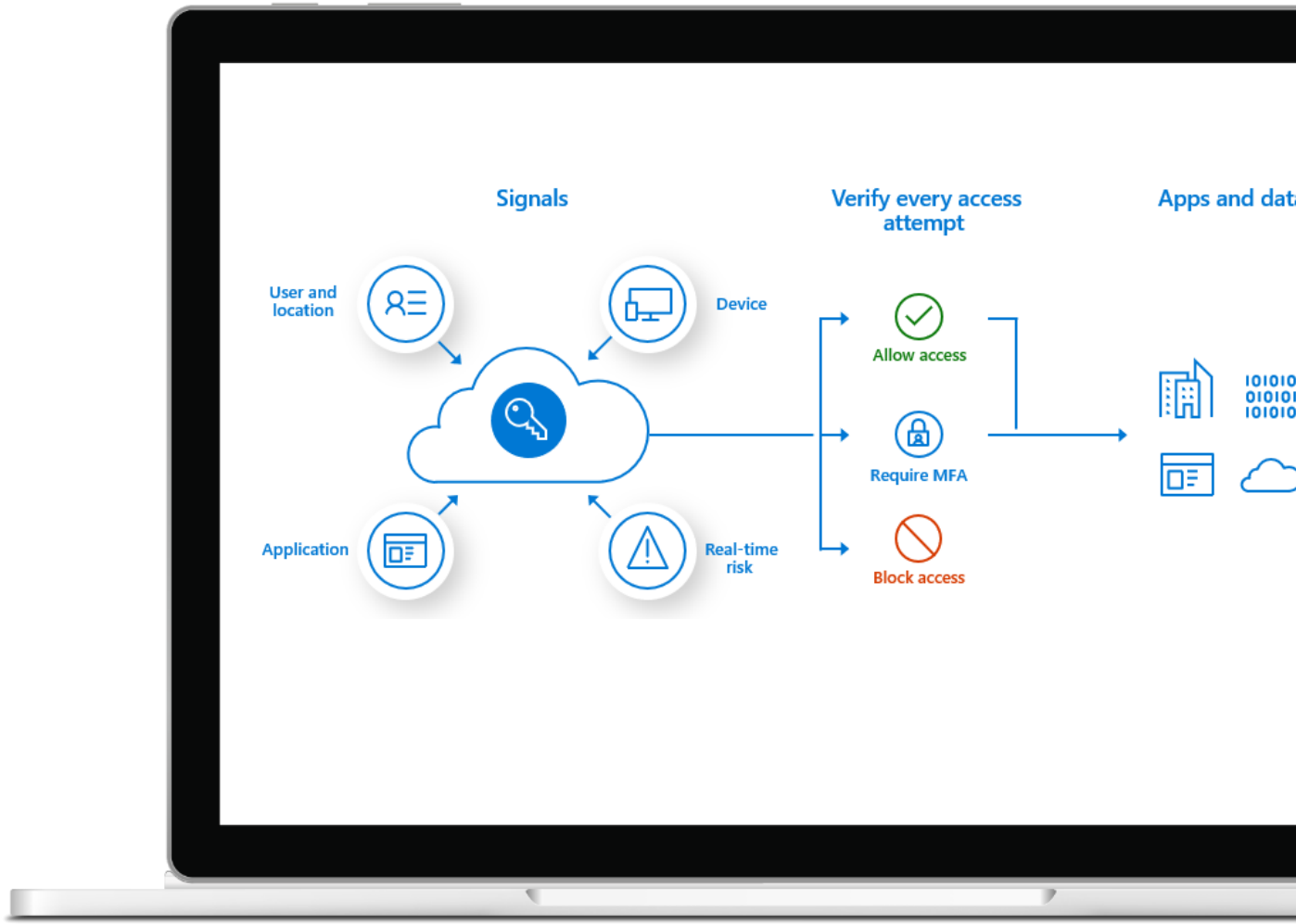
- all or any selected group(s) of users
- all or any cloud application

Requirement for Azure MFA can also be based on

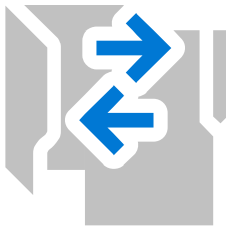
- location
- type of cloud application,
- real-time risk (requires AAD P2 license),
- device state (requires Intune license)

User registration for second factor at next sign in after enablement of Conditional Access policy Requires Azure Active Directory Premium P1 license

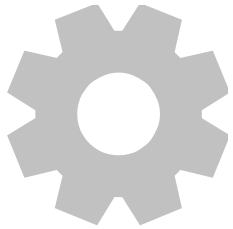
- Or any license that also includes both MFA and Conditional Access, such as Azure Active Directory Premium P2, Microsoft 365 Business, Microsoft 365 E3 or Microsoft 365 E5



Self-Service Password Reset (SSPR)



Self-service password registration and reset



Self-service password change

Account unlock

Password writeback

시나리오 3 : 업무용 앱 사용

디바이스에 배포 구성된 업무용 앱으로 문서를 작성하고 공유해 봅니다.

목적

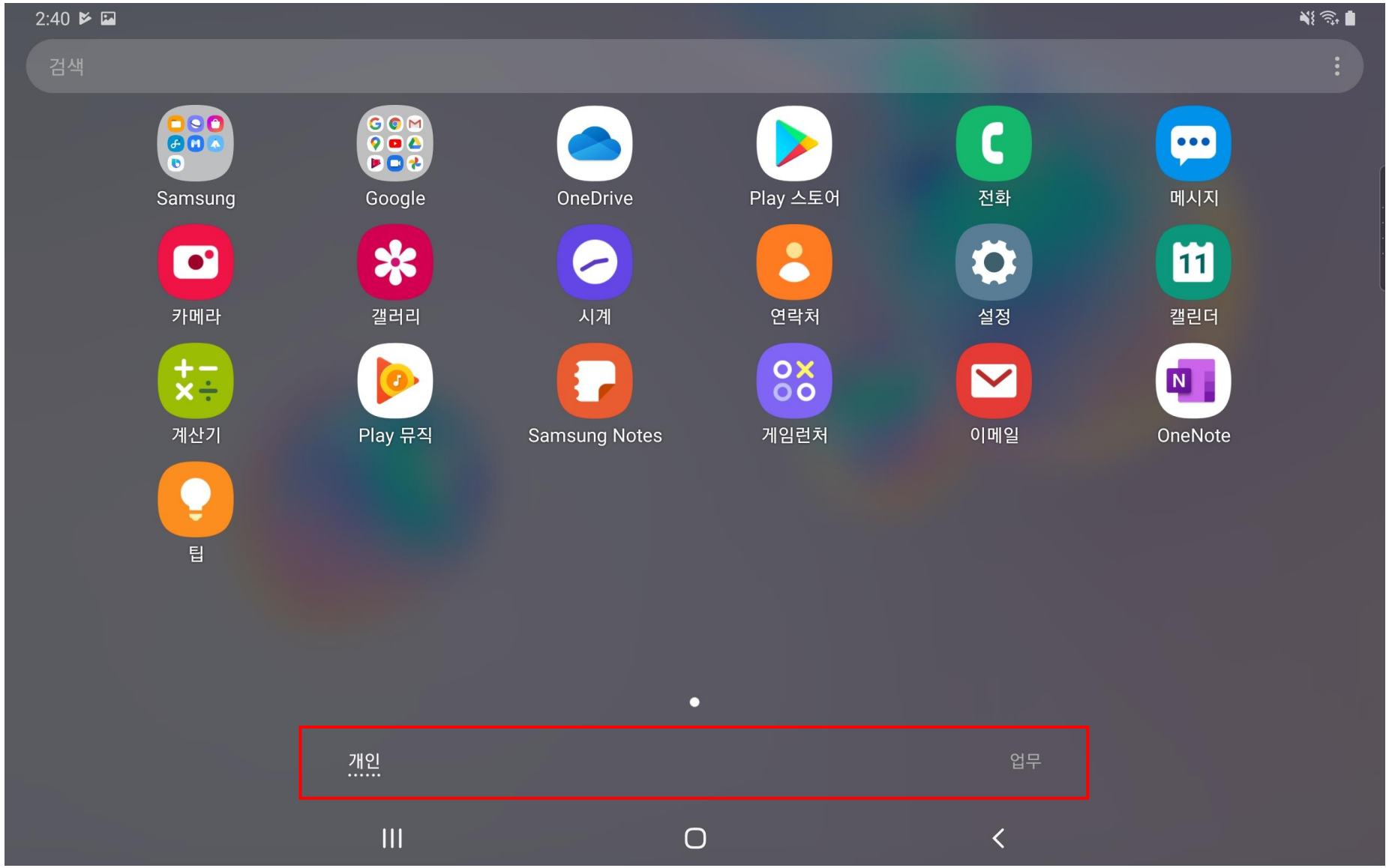
- 회사에서 관리되는 앱에서 작성된 문서는 업무용 앱외의 개인용 앱에서 공유가 될 수 없습니다.
- 업무용 앱에서 개인용 앱으로 클립보드(복사/붙여넣기) 및 저장 기능을 제한하여 데이터의 외부 유출을 방지합니다.

특징

- 업무용 앱과 같은 회사에서 관리되는 앱은 앱 관리 정책으로 인해 개인용 앱으로의 데이터 공유 기능을 제한 할 수 있습니다.
- 업무용 앱과 개인용 앱 간의 데이터 공유 여부를 각각 별도로 설정할 수 있습니다.

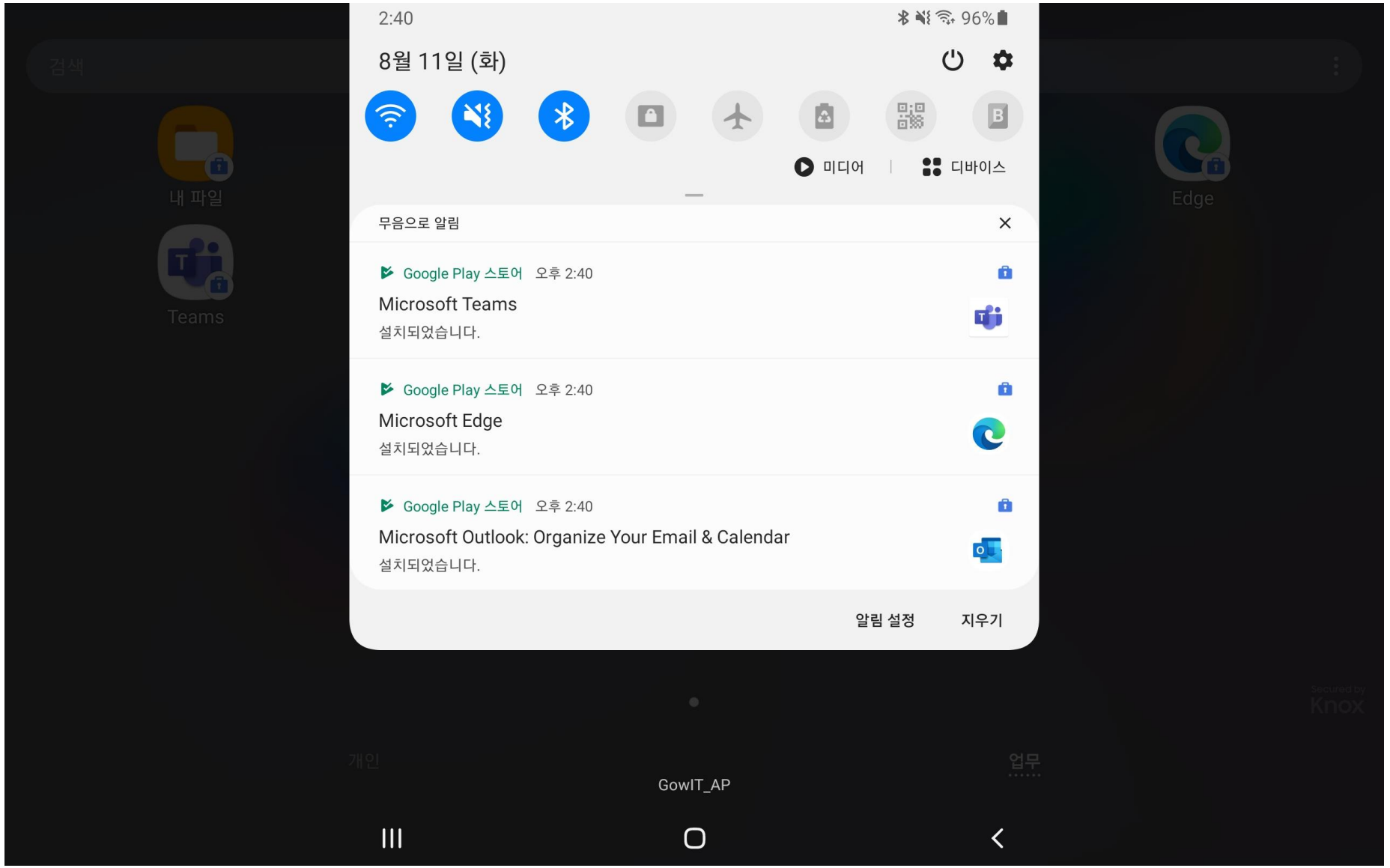
사용자 회사 모바일 장치 등록

- 등록이 완료된 후 홈화면으로 돌아오면, 모바일 UI가 "개인"과 "업무" 영역으로 분리된 것을 확인할 수 있습니다.



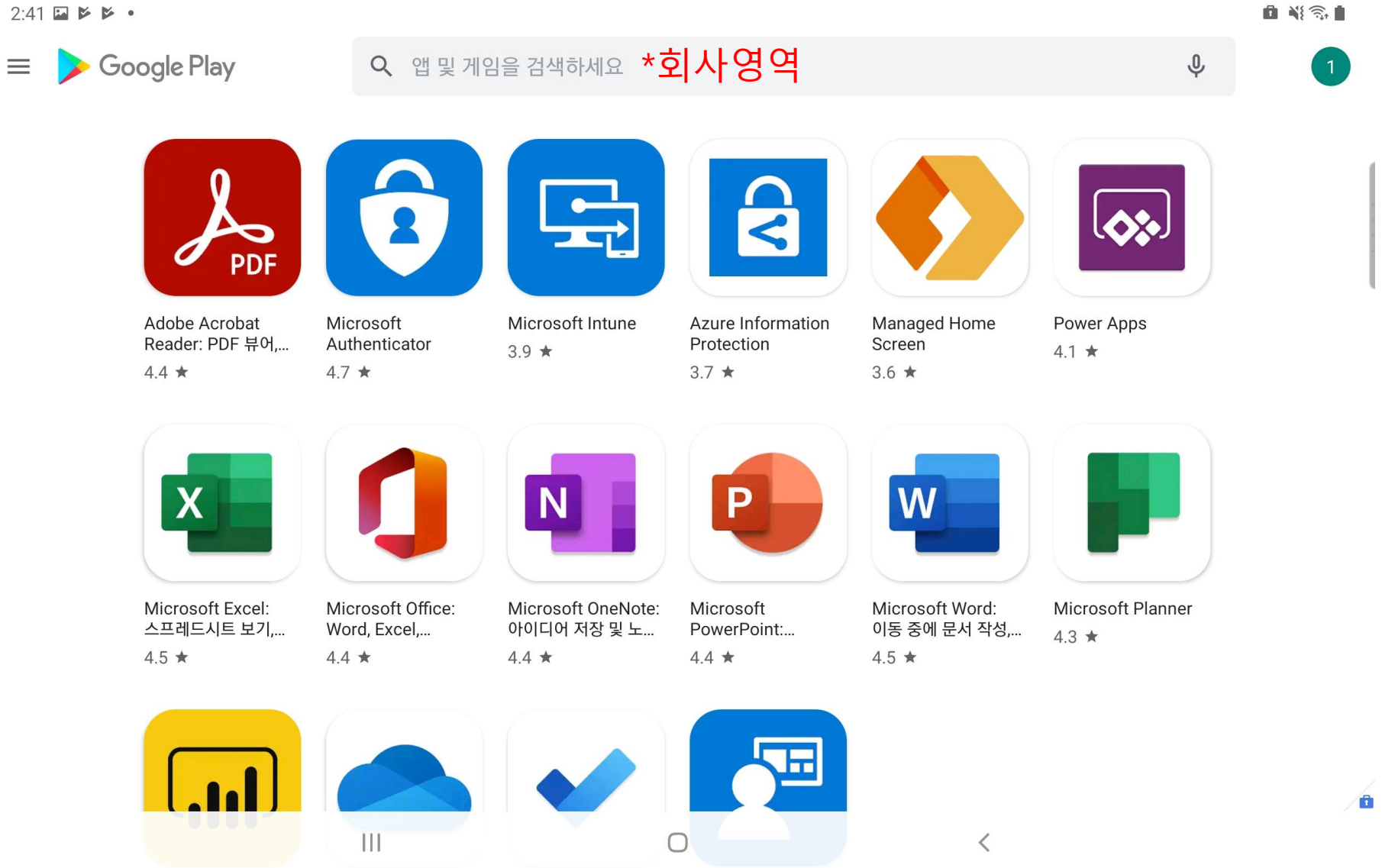
사용자 회사 모바일 앱 다운로드

- 사용자의 장치 등록 작업이 완료되면 별도의 작업을 하지 않아도 관리자가 배포한 앱을 자동으로 설치할 수 있습니다.



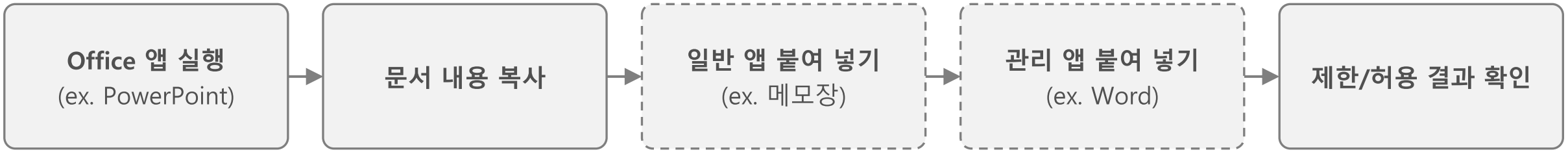
사용자 회사 모바일 앱 다운로드

- "업무" 영역의 앱 스토어에서 관리자가 설정한 회사 전용 앱을 설치할 수도 있습니다.

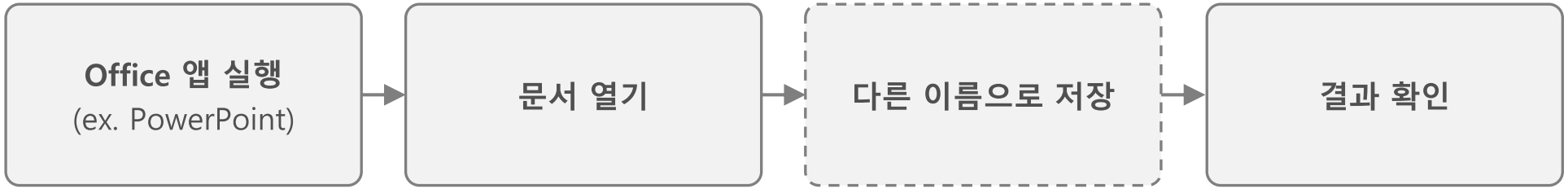


앱 데이터 보호

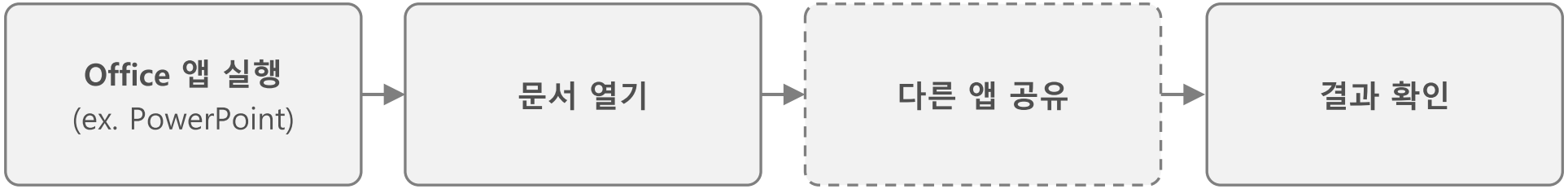
앱 허용/차단 - 클립보드



다른 이름으로 저장(Android)

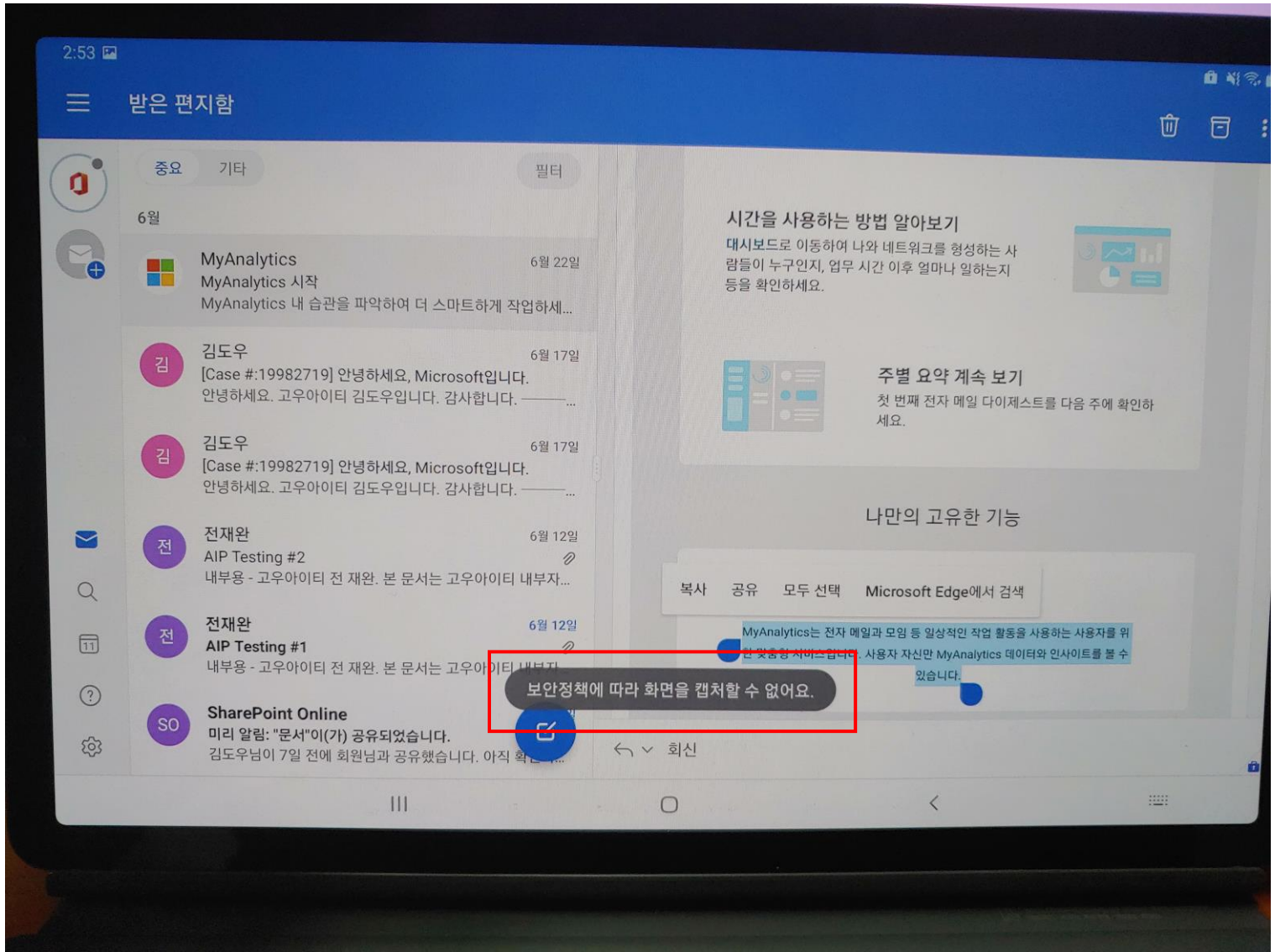


앱 허용/차단 – 공유



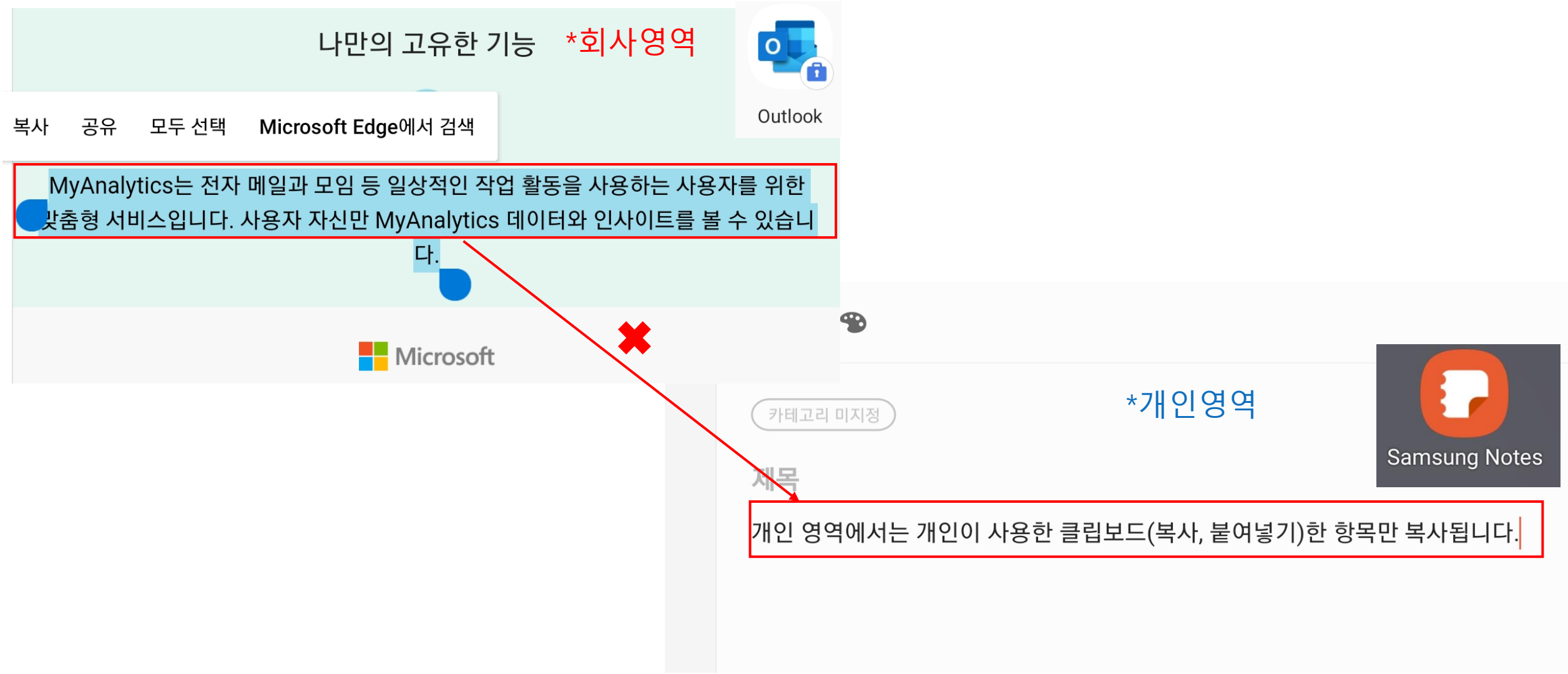
사용자 회사 모바일 앱 사용(등록)

- 일반적으로 사용자는 회사 앱을 실행할 경우, 스크린 캡쳐를 할 수 없도록 정책이 구성되어 있습니다.
  해당 가이드에서는 사용자의 원활한 사용을 위하여, 일시적으로 캡쳐를 활성화 한 상태입니다.



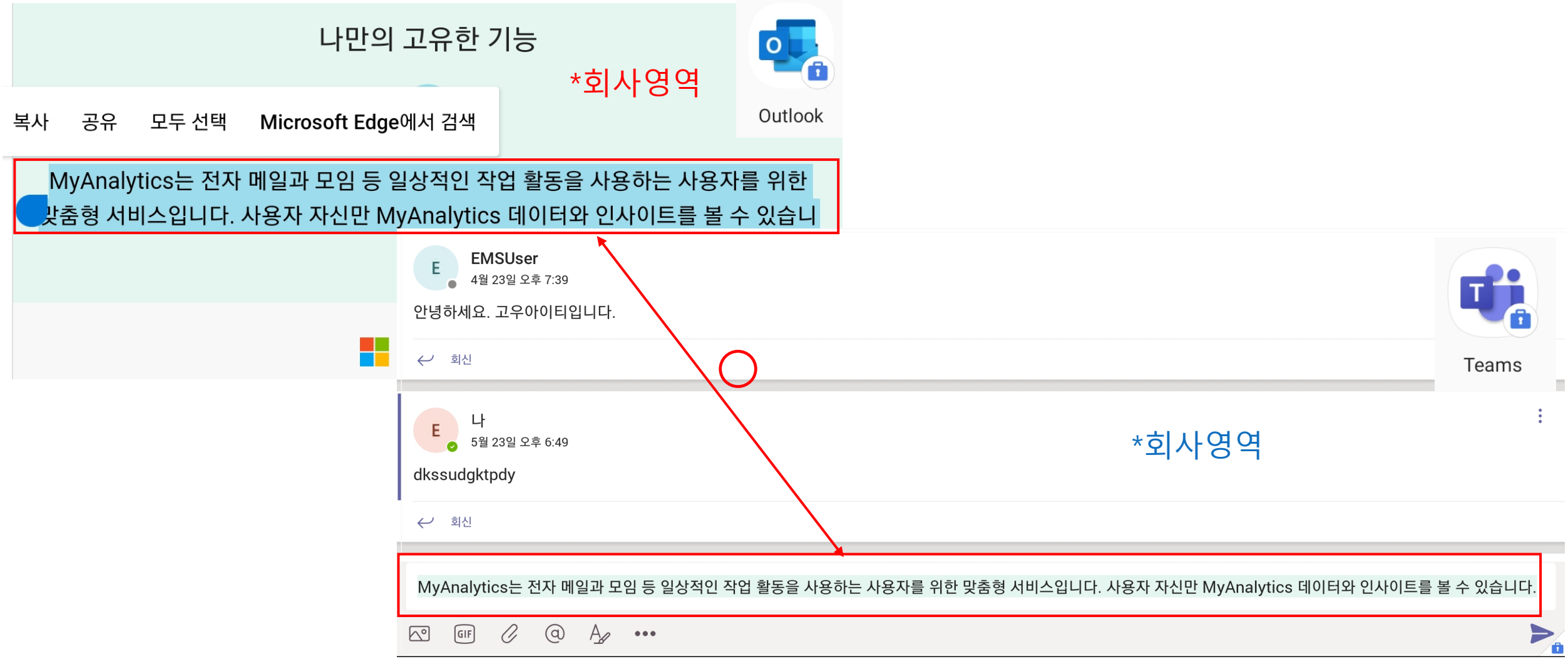
사용자 회사 모바일 앱 사용(데이터 공유)

- 사용자는 회사의 보안 정책에 따라 Outlook, Teams와 같은 모바일 앱에서 회사의 데이터를 개인 영역의 앱(카카오톡, 기본 노트 앱)으로 복사, 붙여넣기를 할 수 없습니다. **(회사 -> 개인 앱 데이터 전송 불가능)**



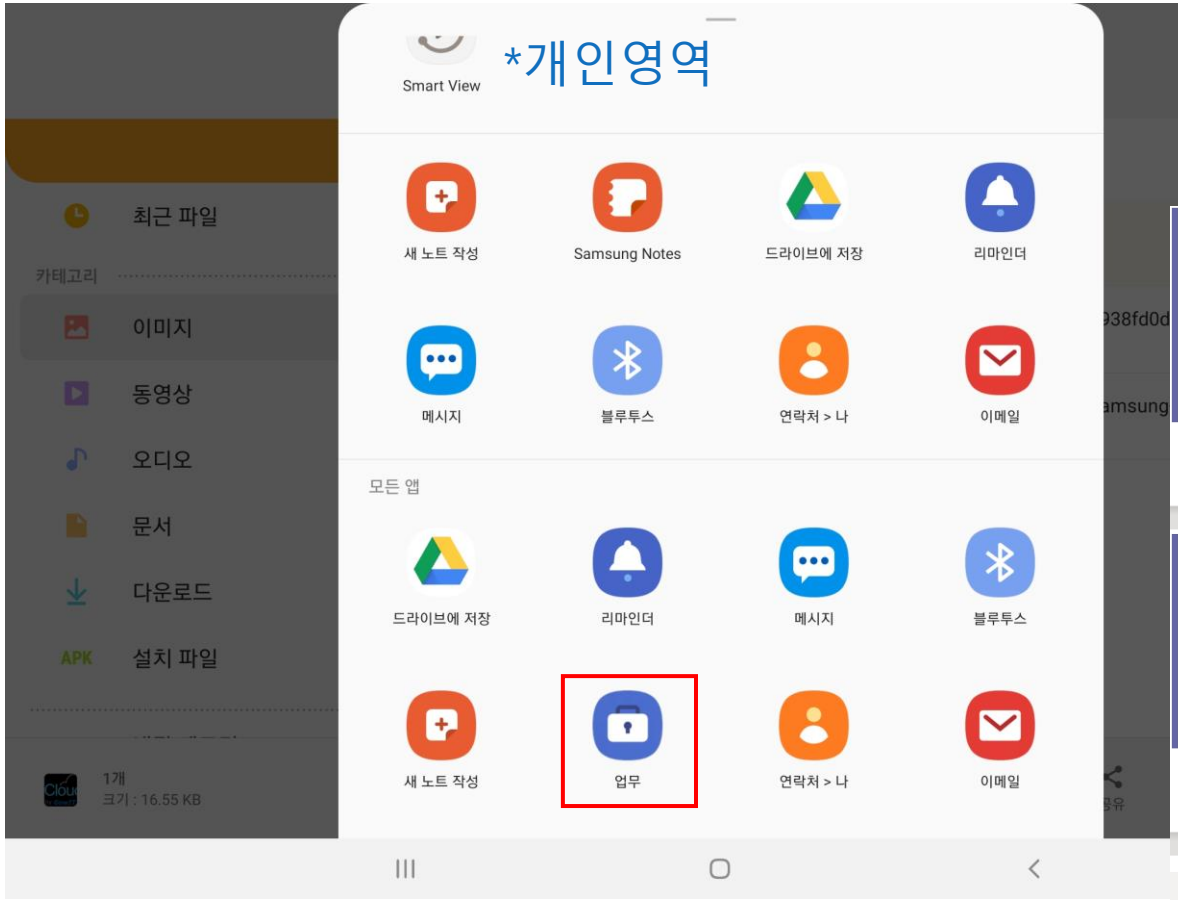
사용자 회사 모바일 앱 사용(데이터 공유)

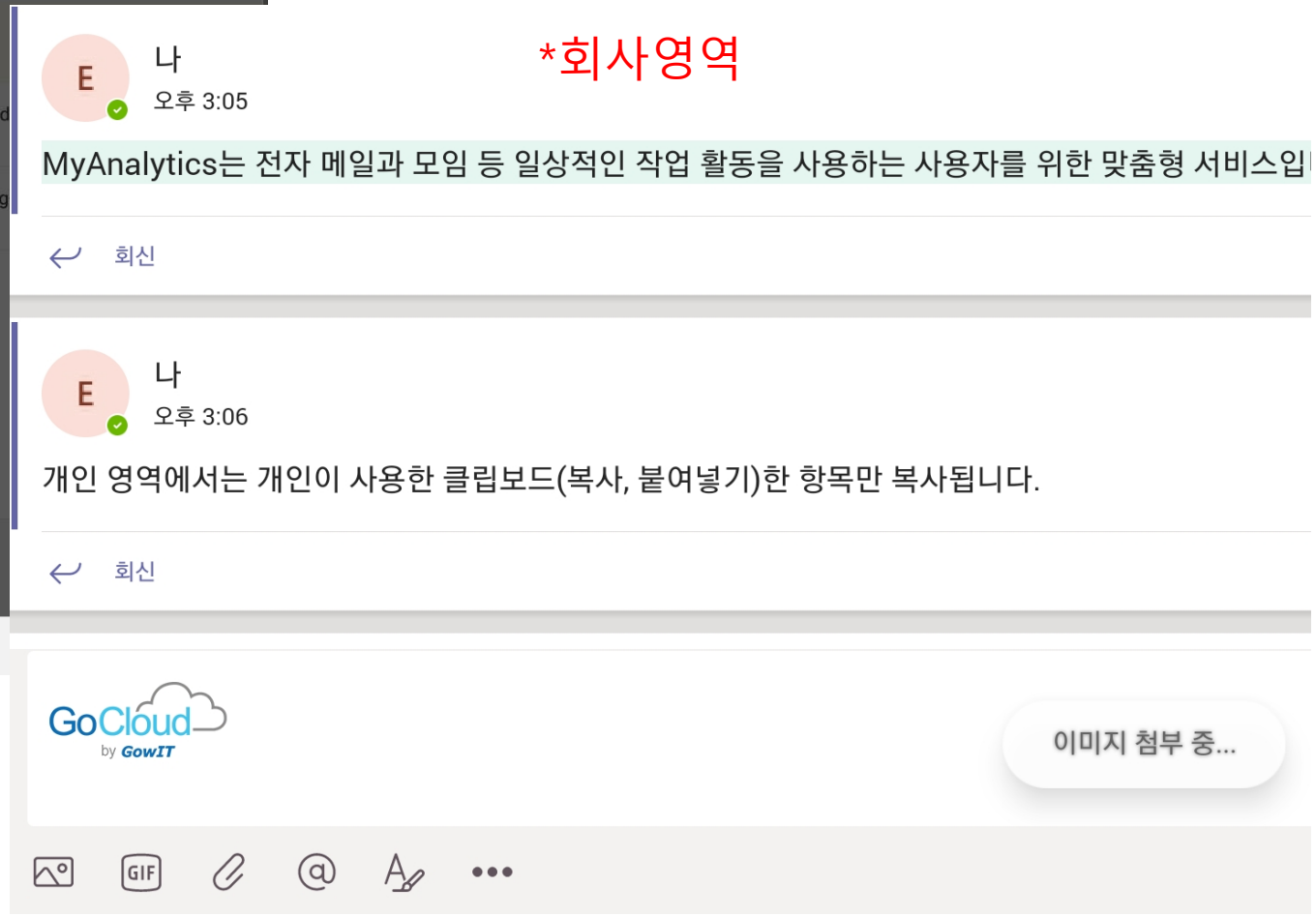
- 회사 영역의 앱 간에는 자유롭게 데이터 복사, 붙여넣기가 가능합니다. **(회사 <-> 회사 앱 간 데이터 전송 가능)**



사용자 회사 모바일 앱 사용(데이터 공유)

- 반대로, 개인 영역의 모바일 데이터는 회사의 앱으로 복사, 붙여넣기가 가능합니다. **(개인 -> 회사 앱 데이터 전송 가능)**





시나리오 4: PC 데이터 보호

PC 에서 데이터를 보호하고 유출을 방지할 수 있습니다.

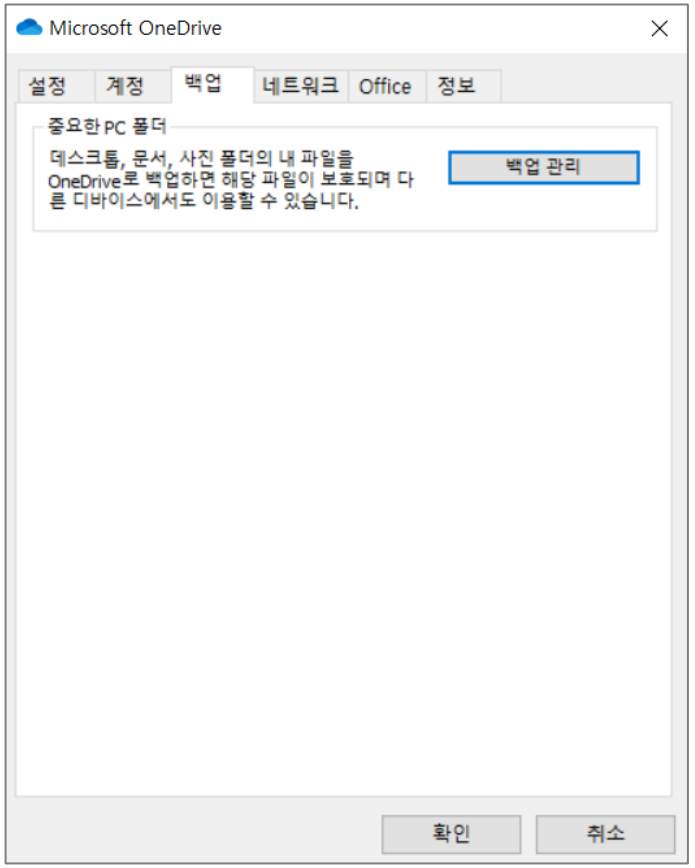
목적

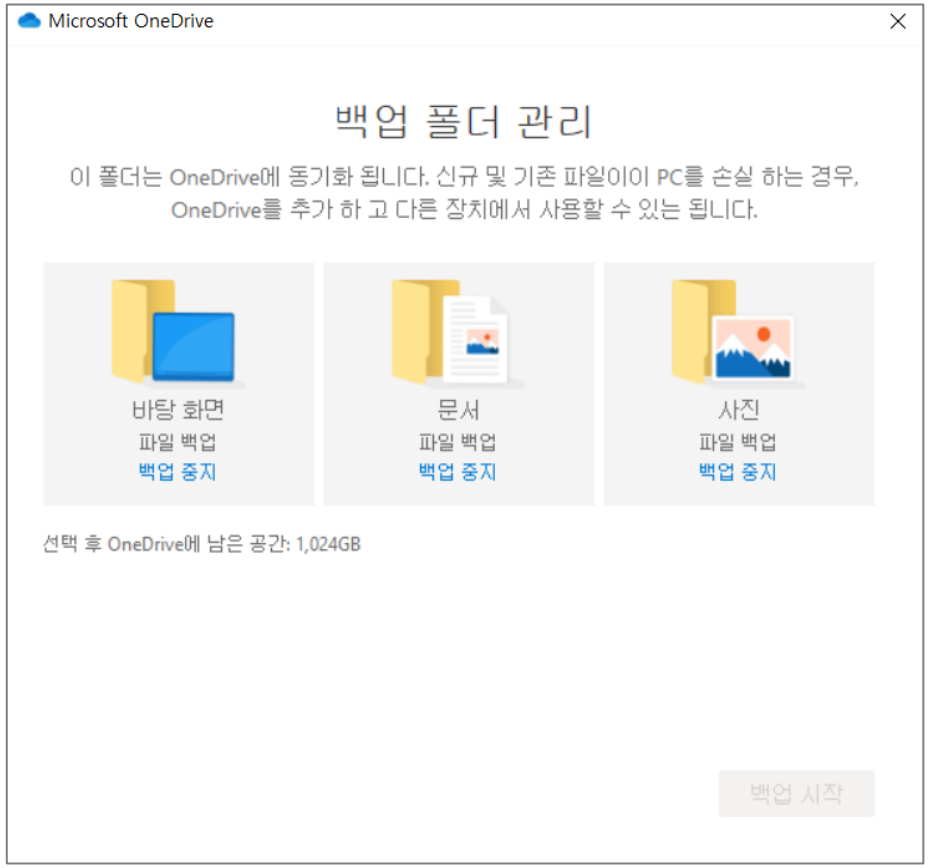
- 개인이 작성하는 문서를 랜섬웨어등의 공격으로 부터 보호할 수 있습니다.
- 조직의 데이터를 외부로 유출을 방지할 수 있습니다.

특징

- 개인 PC의 주요 데이트를 클라우드로 백업할 수 있습니다.
- 클라우드에 보관된 조직의 데이터가 외부로 유출되는 것을 방지할 수 있습니다.
- 라벨을 설정하여 중요 문서에 대한 암호화를 수행하여 중요한 문서가 외부로 유출되는 것을 방지할 수 있습니다.

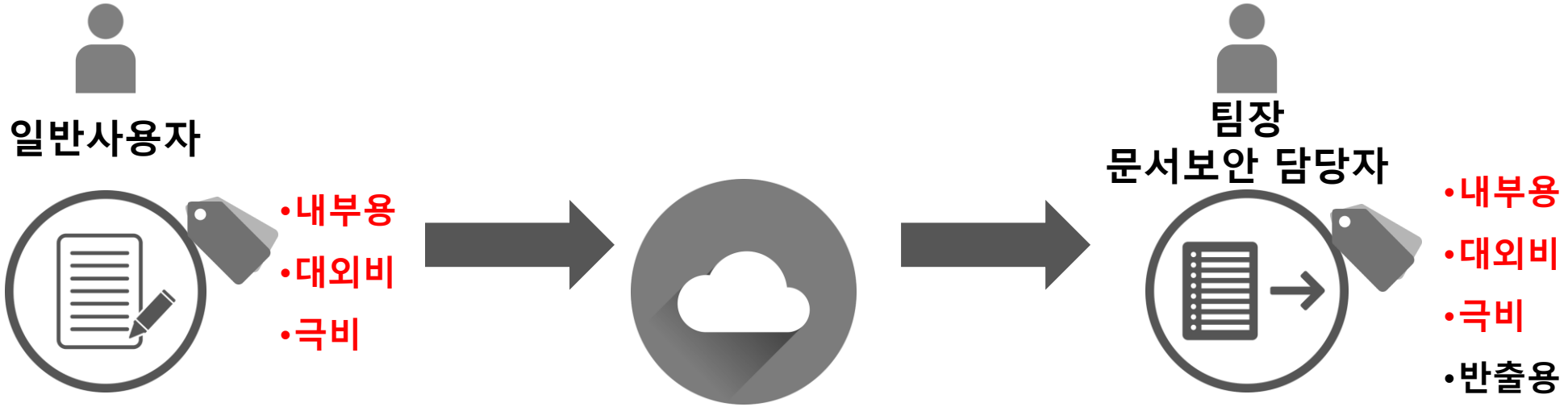
중요한 PC 폴더 백업


Microsoft OneDrive
설정
계정
백업
네트워크
Office
정보
중요한 PC 폴더
데스크톱, 문서, 사진 폴더의 내 파일을 OneDrive로 백업하면 해당 파일이 보호되며 다른 디바이스에서도 이용할 수 있습니다.
백업 관리
확인
취소


Microsoft OneDrive
백업 폴더 관리
이 폴더는 OneDrive에 동기화 됩니다. 신규 및 기존 파일이이 PC를 손실 하는 경우, OneDrive를 추가 하 고 다른 장치에서 사용할 수 있는 됩니다.
바탕 화면
파일 백업
백업 중지
문서
파일 백업
백업 중지
사진
파일 백업
백업 중지
선택 후 OneDrive에 남은 공간: 1,024GB
백업 시작

문서라벨 적용으로 사내 데이터 보호

협력 업체의 사용자와 문서를 안전하게 공유해 봅니다.



- 사용자는 오피스 문서 저장 시 반드시 라벨을 적용하여야 함
- 내부용 문서는 소유자를 제외하고 다른 이름으로 저장, 내보내기 등의 작업을 할 수 없음
- 소유자는 라벨을 최초 적용하여 문서의 권한을 설정한 사람임
- 권한이 지정된 문서는 추적이 가능하고 7일간 오프라인으로 열람이 가능하며 그 이후에는 열람이 불가능함.

- 내부용 문서를 반출하기 위해서는 팀문서 폴더에 파일을 업로드 하고 팀장에서 반출용 문서 변환 요청

- 팀장은 요청된 문서를 반출용으로 변환하고 팀원에게 변환 내용을 통보함
- 시간이 흐름에 따라 지속적으로 팀문서함의 문서 증가
- 일정 시간 후 팀장/담당자는 반출용 문서를 내부용으로 라벨을 변경하면 소유자가 변경.

사용자 문서 보안 업무 환경

- AIP 문서 보호의 라벨은 다음과 같이 문서를 보호 합니다.

내부용

- 라벨이 지정되면 문서에 권한 관리가 적용됨.
- 소유자는 모든 권한가지고 라벨 변경, 문서 내보내기를 포함한 문서에 대한 모든 권한을 소유함
- 소유자는 문서에 권한을 최초 적용한 사람이 소유자가 되며 보안관리자 그룹(팀장)은 문서의 소유자 권한을 가짐
- 그외 사내 사용자 그룹은 제한된 공동편집자 권한을 가짐
- 제한된 공동편집 권한은 권한관리가 적용되지않는 다른 이름 저장, 내보내기 기능을 수행할 수 없음
- 문서에는 머리글, 바닥글에 보안문구가 적용됨
- 출력기능을 이용한 PDF 출력은 가능함

대외비
극비

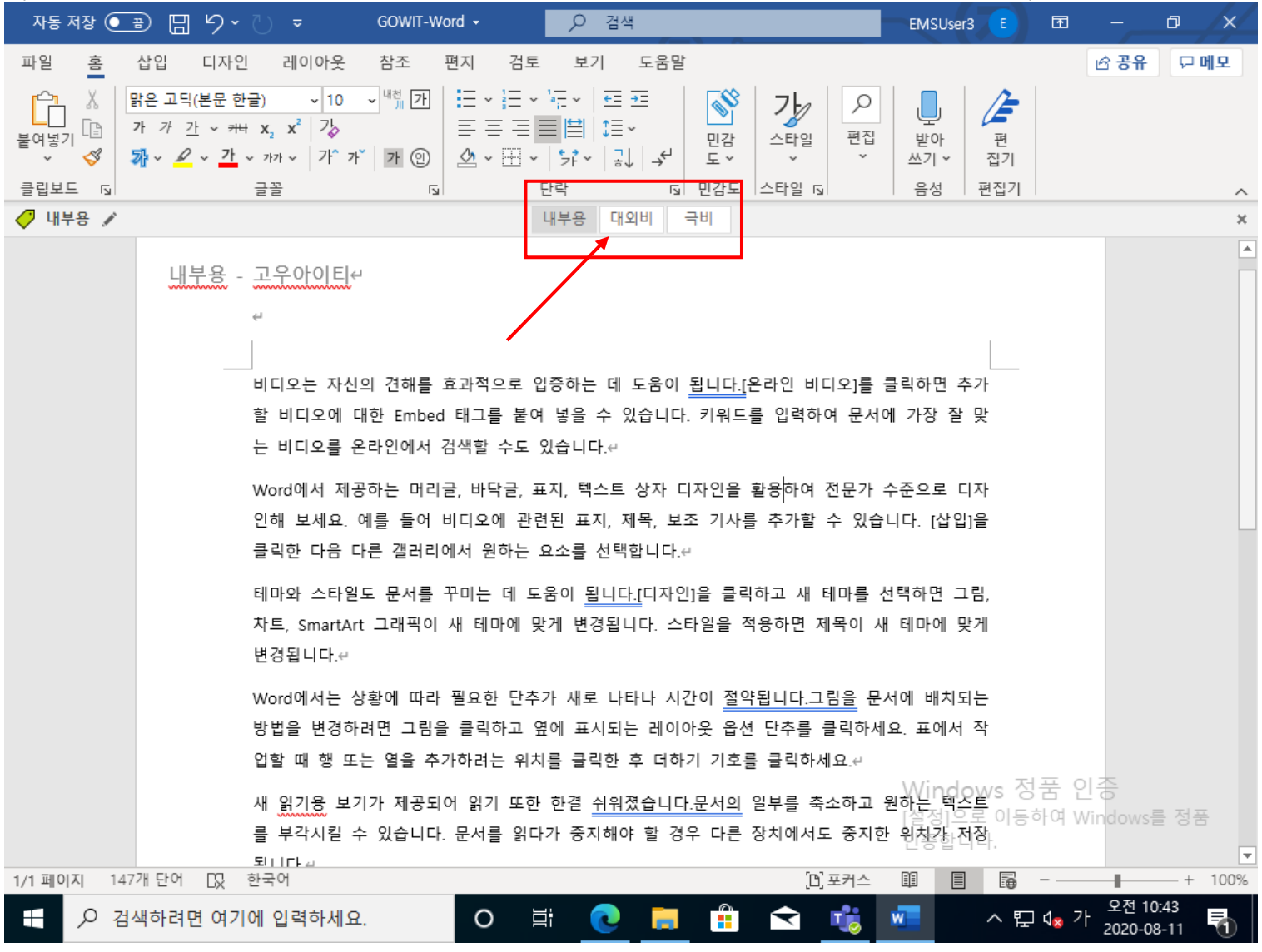
- 소유자와 특정 그룹만 권한을 가짐
- 권한는 보안 정책에 따라 설정 됨
- 문서에는 머리글, 바닥글에 보안문구가 적용됨

반출용

- 라벨은 보안관리 그룹(팀장) 만 적용할 수 있음
- 문서에는 머리글, 바닥글에 보안문구가 적용됨
- 권한관리가 해제되며 외부 인원도 문서열람이 가능함

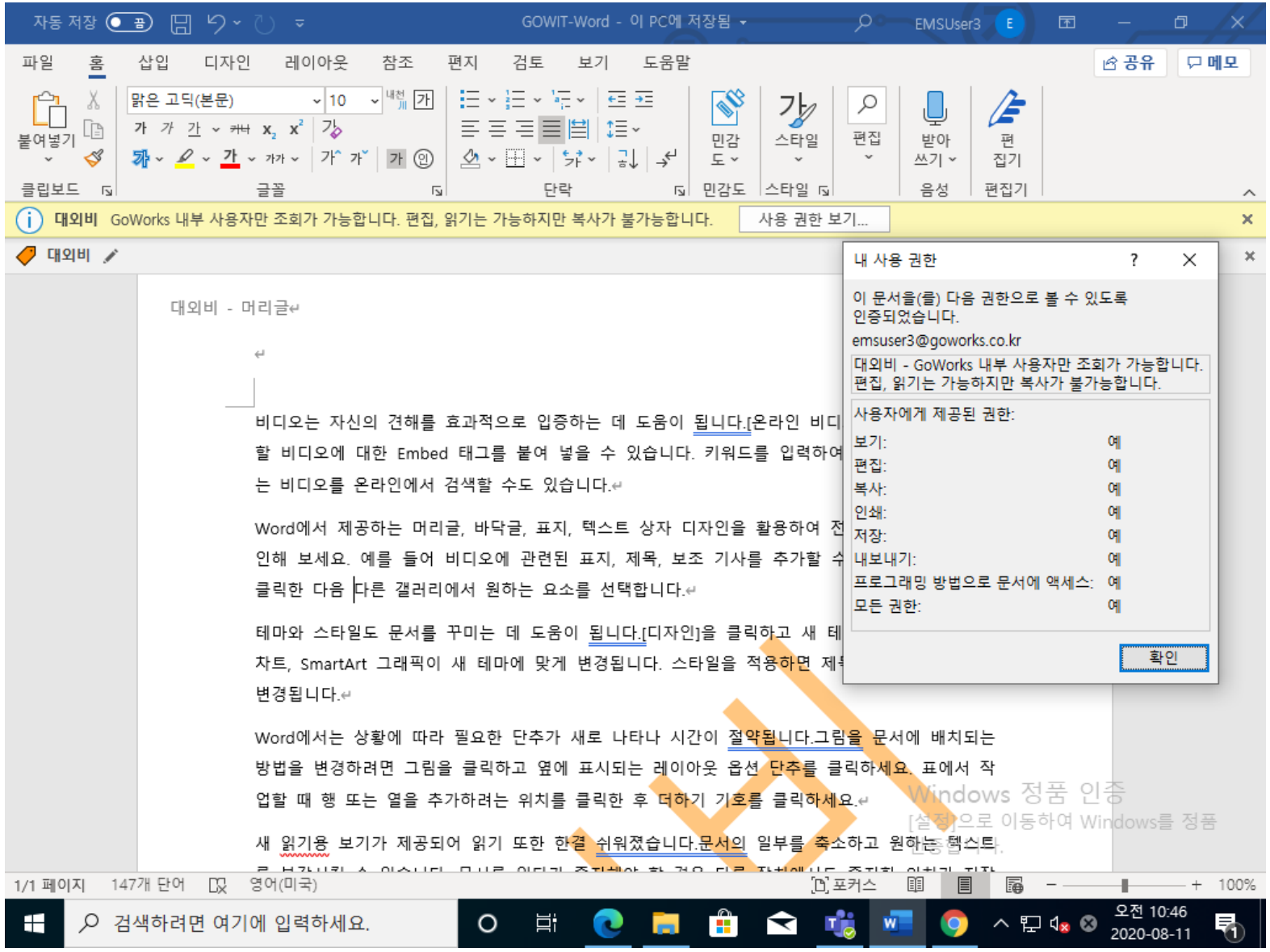
사용자 문서 보안 업무 환경

- 사용자는 중앙에서 배포한 AIP 배포 응용 프로그램(Add-on)을 통해 문서에 레이블이라는 보안 정책을 적용할 수 있습니다.
  레이블을 적용함에 따라, 외부로 파일이 유출되더라도 인가되지 않은 사용자는 조회할 수 없거나, 기타 권한 설정이 가능합니다.



사용자 문서 보안 업무 환경

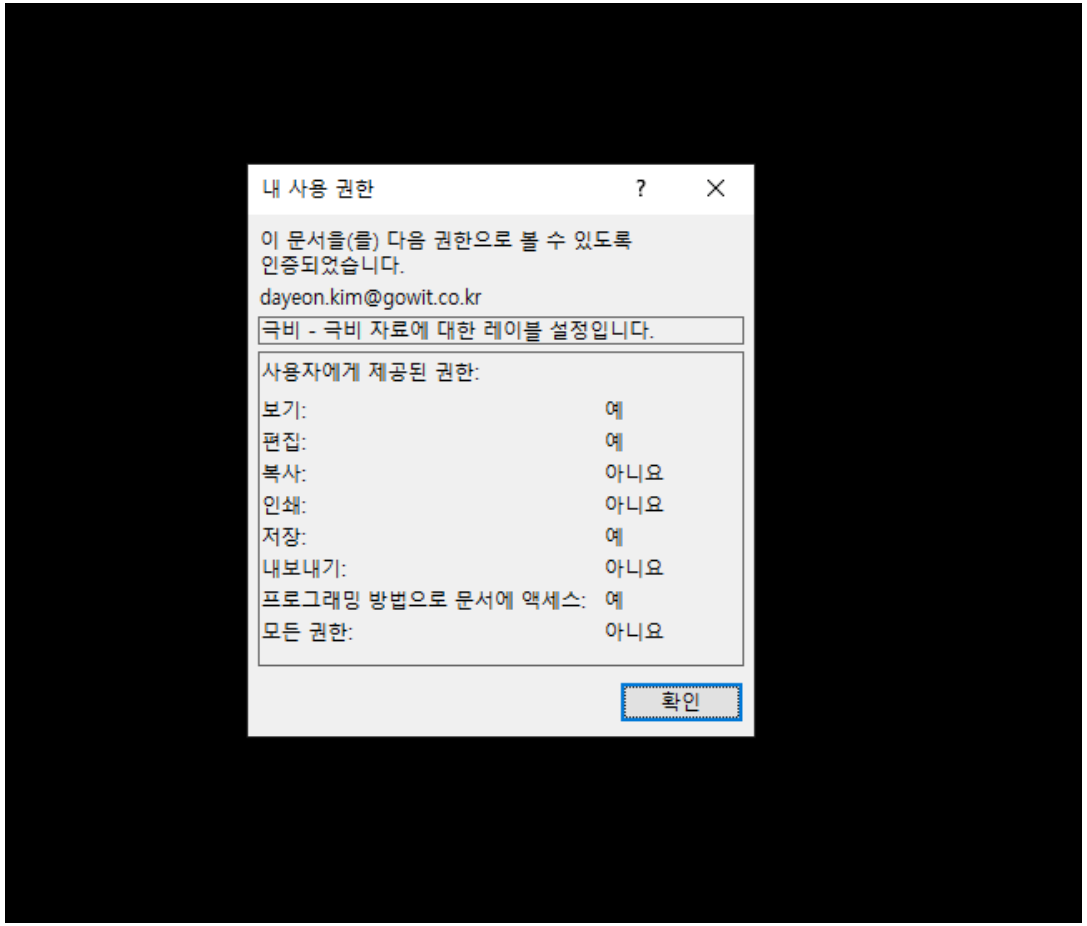
- 사용자는 기본 지정된 레이블 외에 다른 레이블을 지정하여 저장하면, 레이블에 따른 권한 및 암호화가 적용된 것을 확인할 수 있습니다.



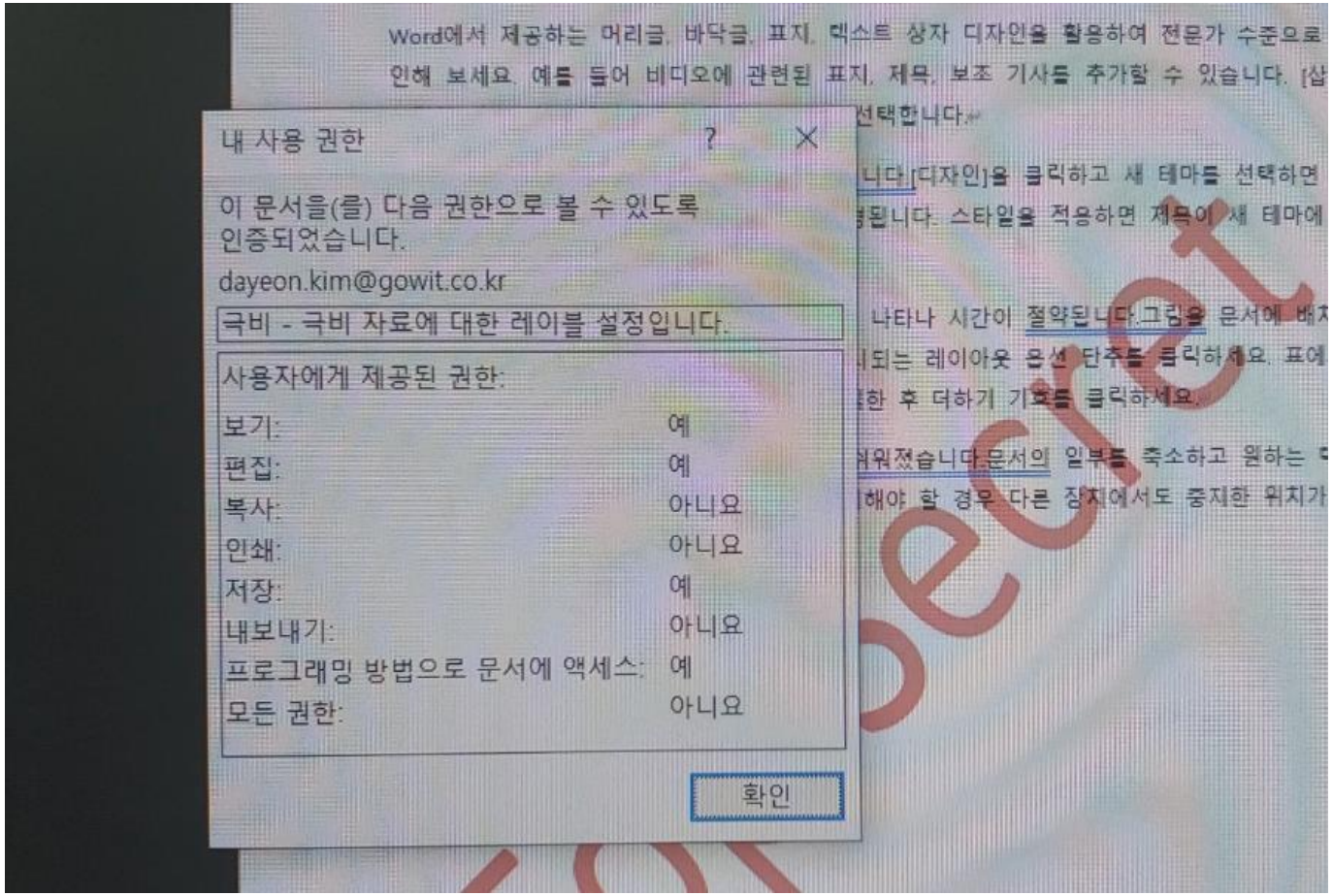
사용자 문서 보안 업무 환경

- 권한이 적용된 레이블을 다른 사용자가 열어볼 경우, 레이블에 따라 적용된 권한을 확인할 수 있습니다.
  뒷배경이 검게 나오는 것은, 사용자에게 "복사" 권한이 없는 상태에서 스크린 캡쳐 시 Office 파일의 작업 영역이 검게 표시됩니다.

스크린 캡쳐 시

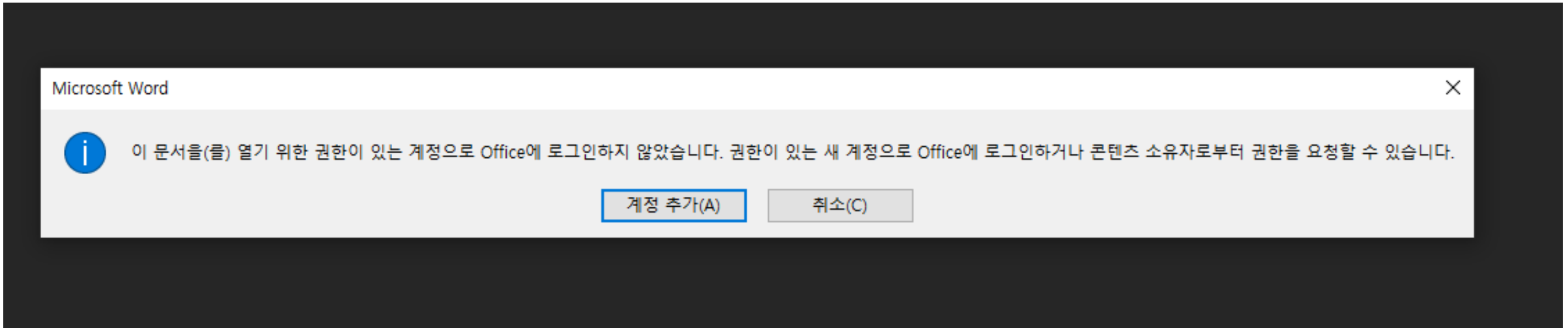


실제 화면



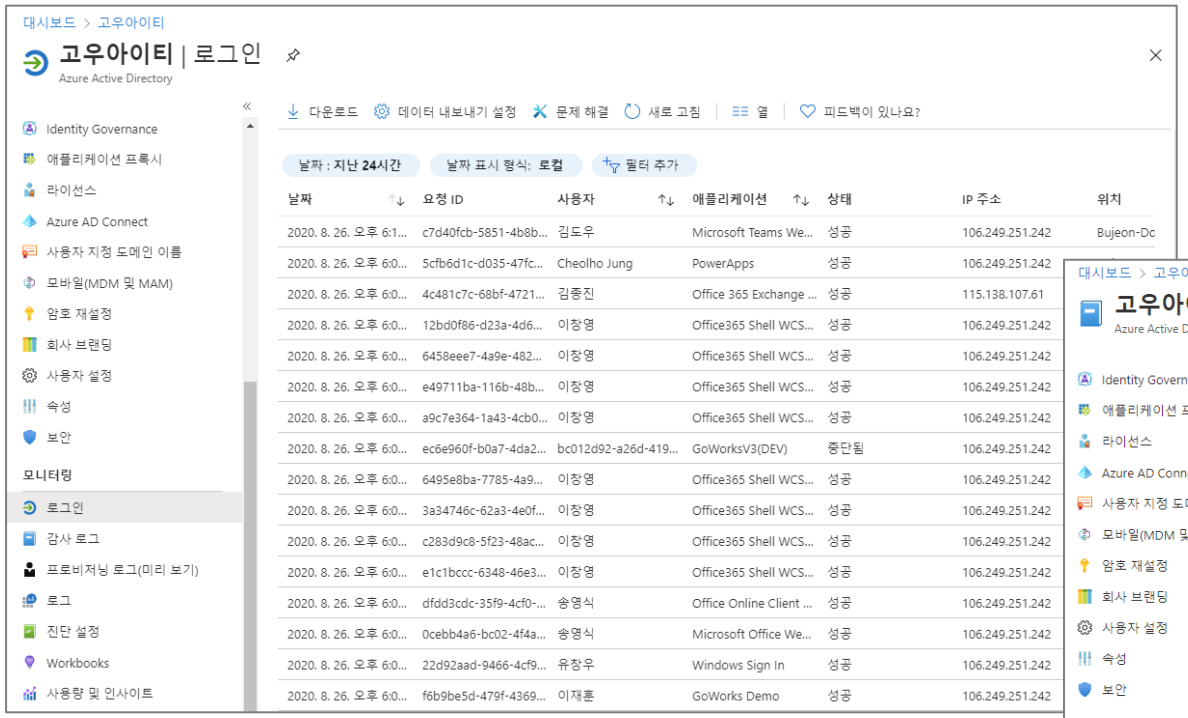
사용자 문서 보안 업무 환경

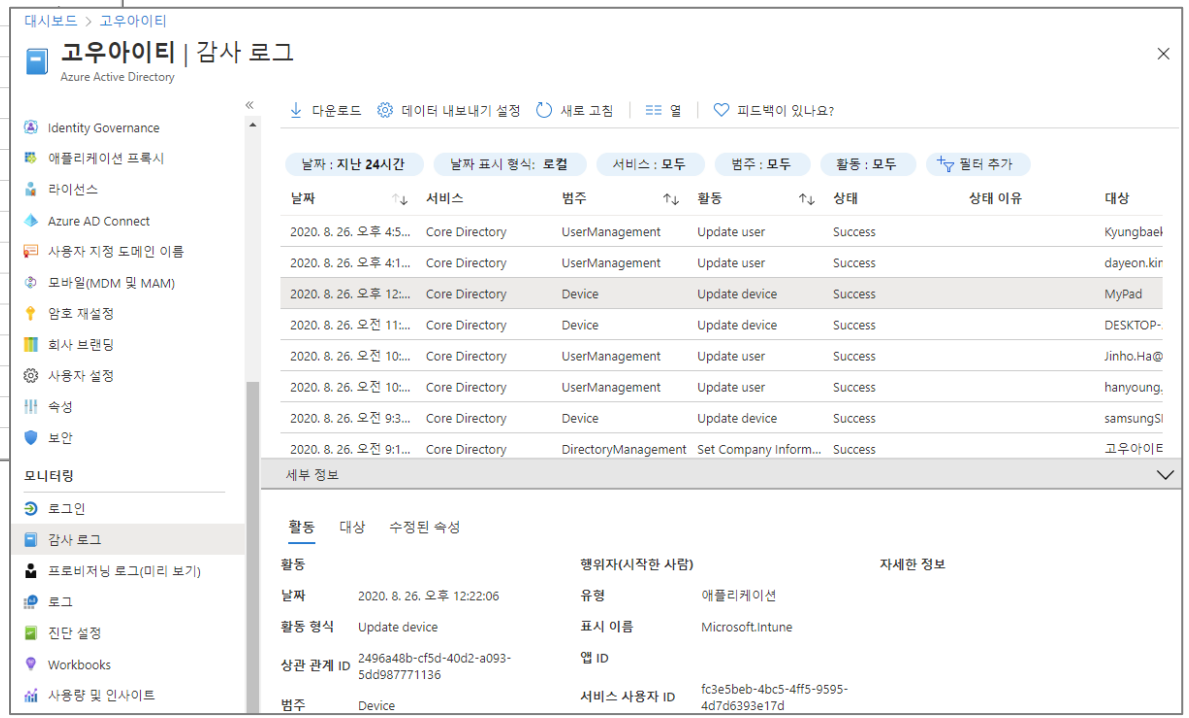
- 권한이 없는 문서를 조회할 경우, 아래와 같이 문서에 접근이 되지 않는 것을 확인할 수 있습니다.



모니터링

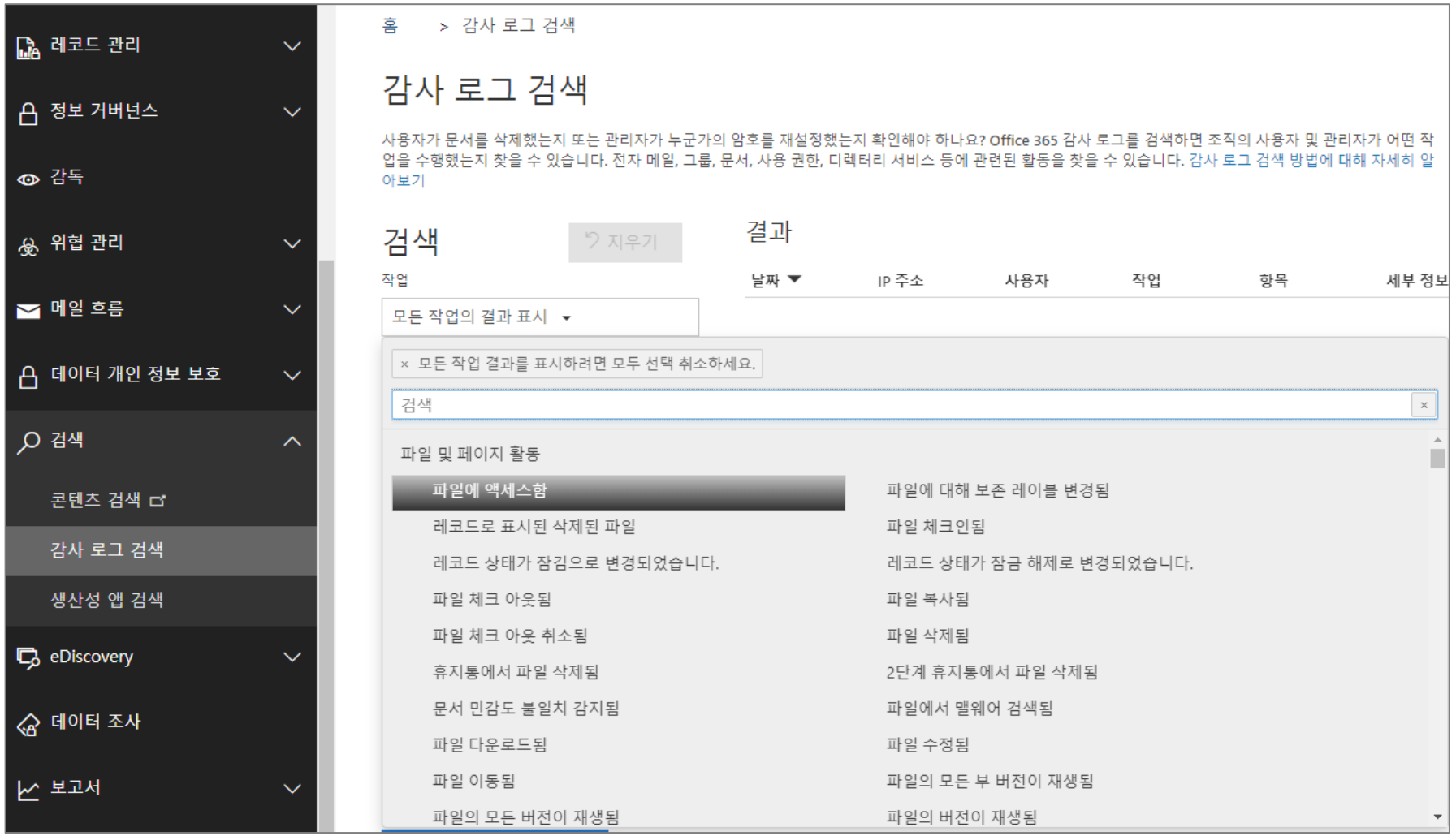
Azure Active directory 관리 대시보드에서 사용자의 로그인 현황을 확인할 수 있습니다.





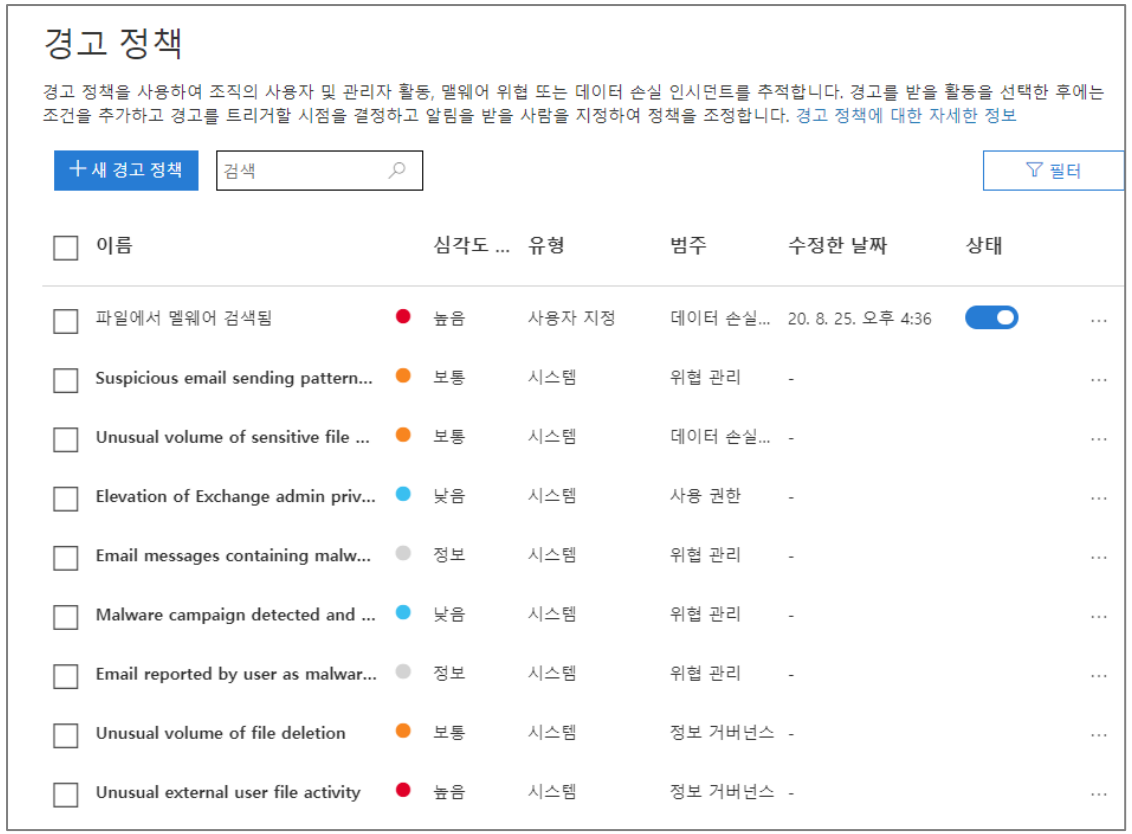
모니터링

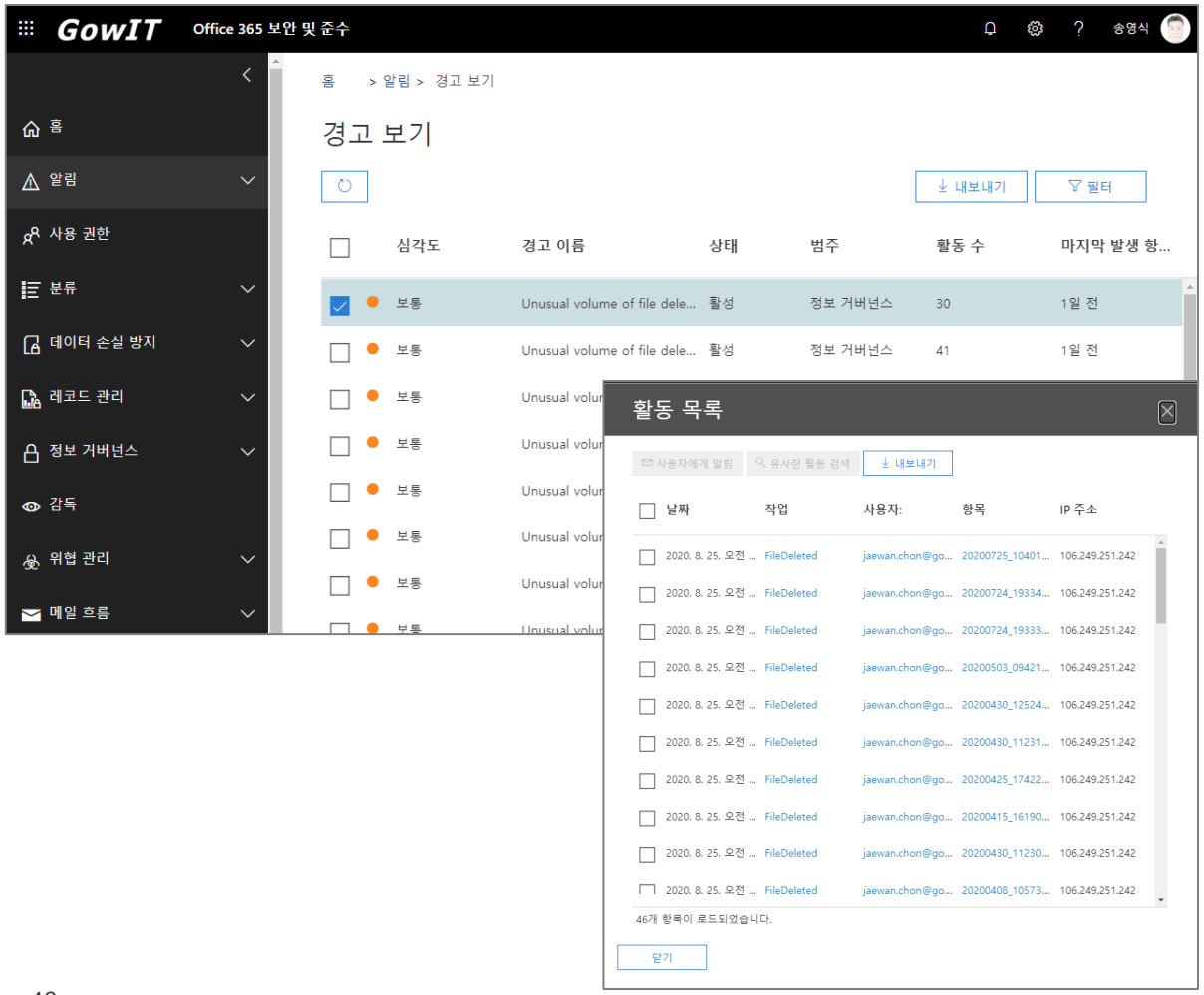
Office365 보안 및 준수 관리 센터에서 조직의 사용자 및 관리자의 작업 수행 현황을 확인할 수 있습니다.



모니터링

Office365 보안 및 준수 관리 센터에서 조직의 비정상적인 활동에 대한 경고현황을 확인할 수 있습니다.





모니터링

Office365 보안 및 준수 관리 센터에서 조직의 위협을 효과적이고 효율적으로 조사하고 대응할 수 있는 보고서를 얻을 수 있습니다.