

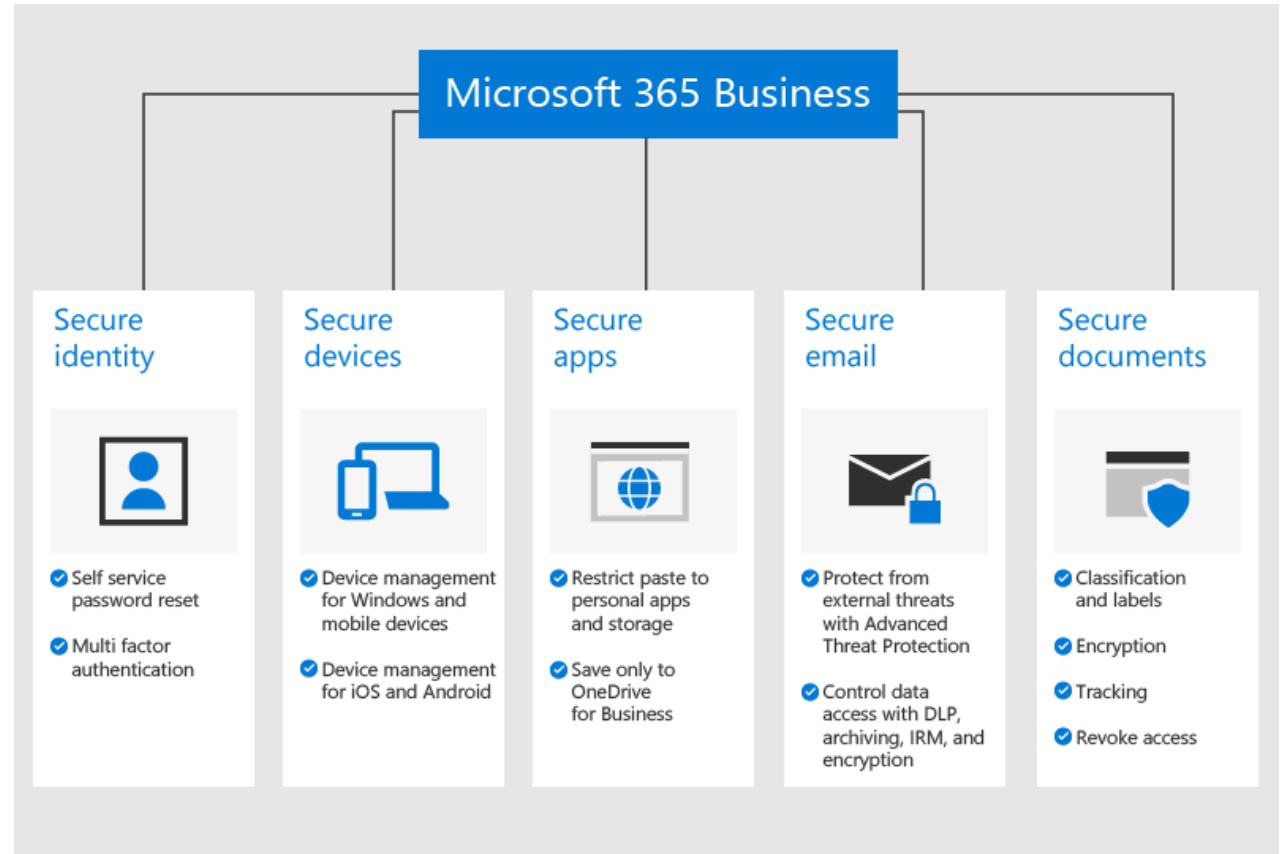
Microsoft 365 Business Premium

Security Deployment

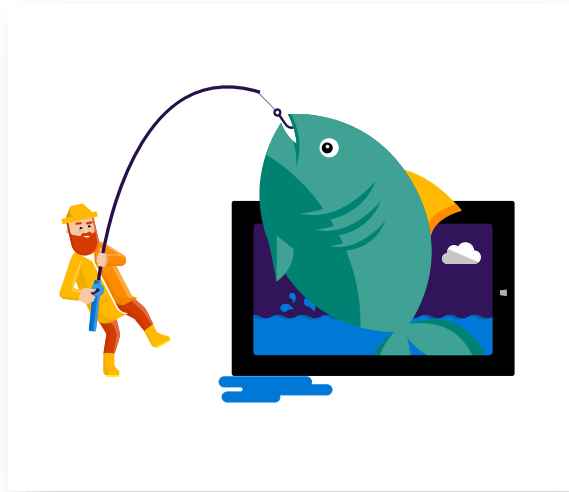


Microsoft 365 Business Premium

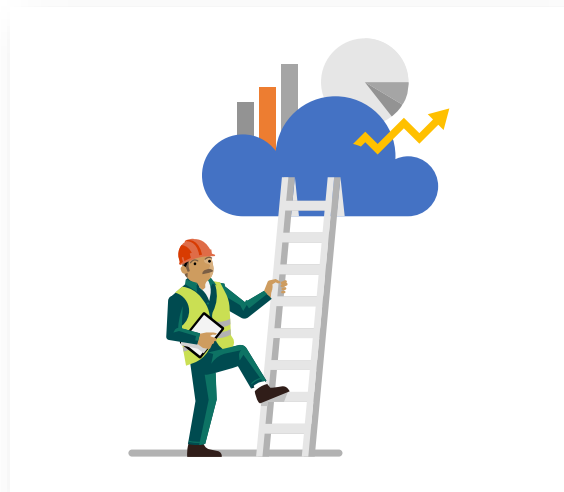
Microsoft 365 Business Premium은 직원의 수가 300명 미만인 비즈니스를 위한 포괄적인 구독 서비스입니다. 좋아하는 Office 생산성 앱 및 서비스와 Microsoft Teams와 같은 공동 작업 도구를 고급 보안 및 장치 관리 기능과 통합 합니다.



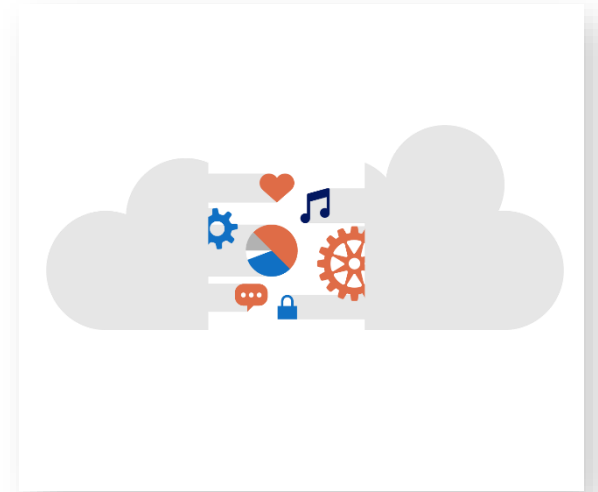
사이버위협 대응과 비즈니스 데이터 보호



Protect users against
cyberthreats like phishing



Safeguard confidential
business data



Get visibility into
cloud app use

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 사용자에게 대한 보다 강력한 보호 프로필입니다.

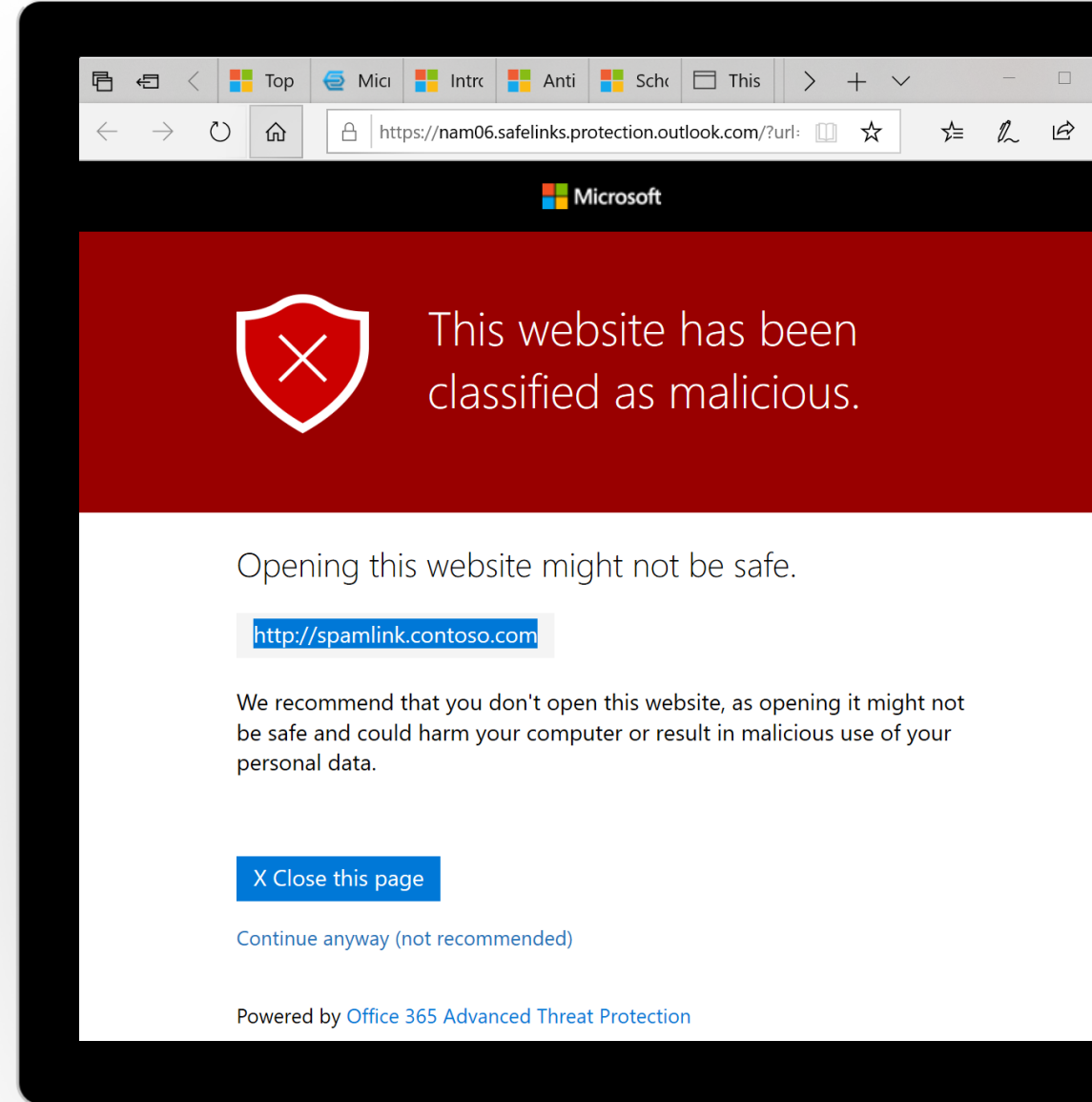
- ✓ 악성 메일에 대한 보다 공격적인 작업
- ✓ 대량 보낸 사람에 대한 제어 강화
- ✓ 더욱 공격적인 기계 학습

엄격한 보호 기능이 켜져 있습니다.

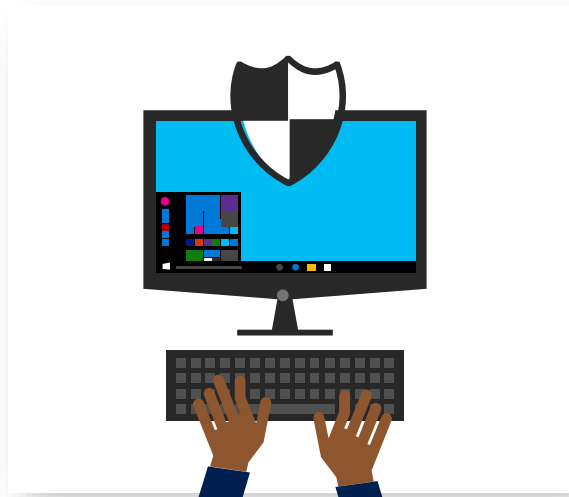
[보호 설정 관리](#)

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)



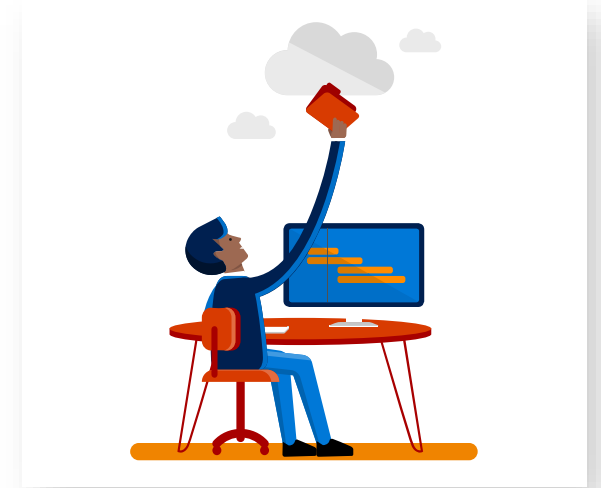
안전한 ID 관리와 접근관리



비밀번호 분실, 탈취로
부터 사용자 계정 보호

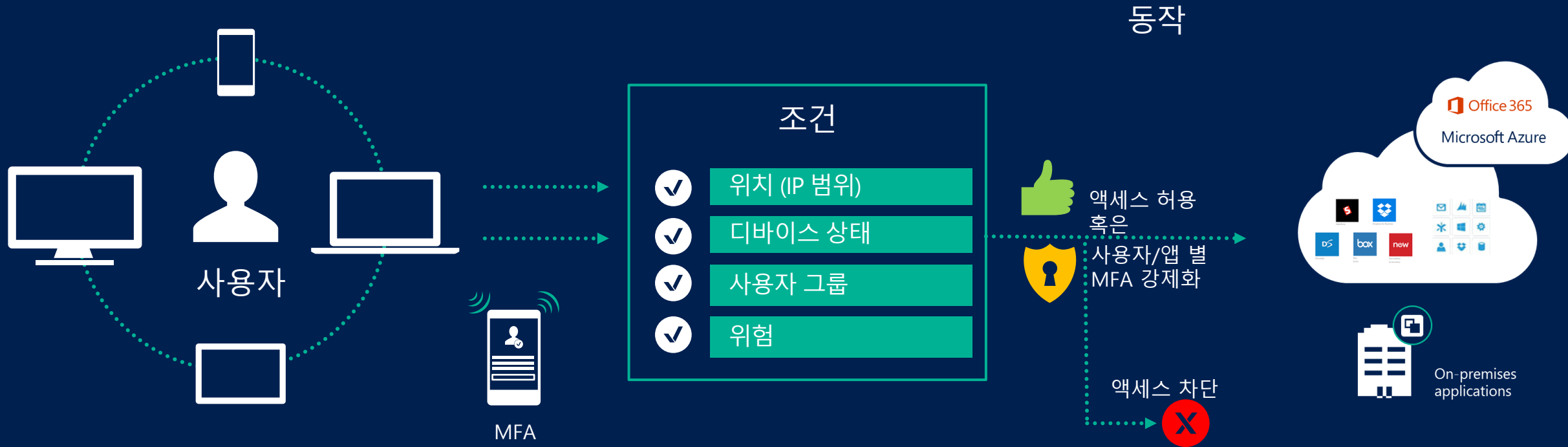


업무용 앱의 안전한
접근

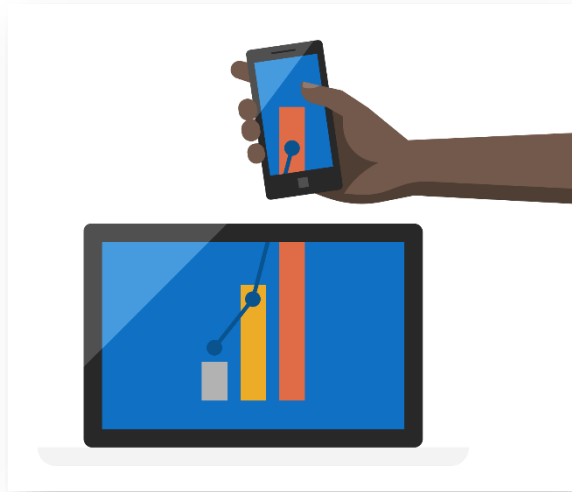


원격 PC로 부터
안전한 접속

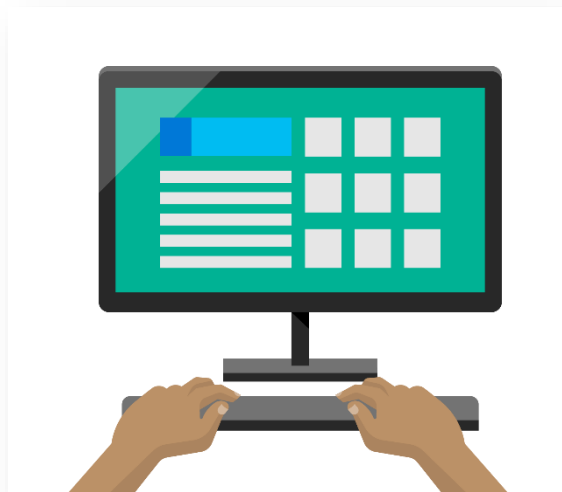
Identity 기반 identity-driven 보안



회사의 데이터에 액세스하는 장치 보안 및 관리



모바일 기기에서
회사데이터 관리



Windows
PC 보안 관리



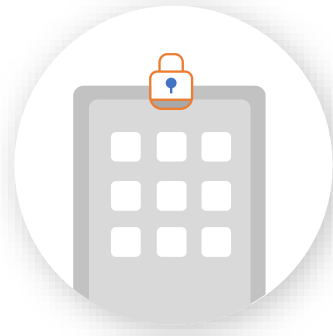
Autopilot을 이용한
자동 배포

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



장치의 등록 및 준수상태
확인

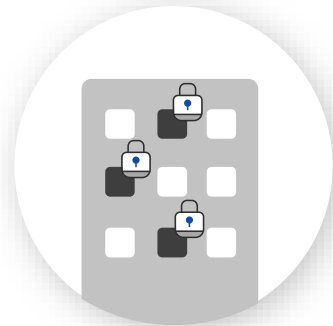


설정, 인증서, 프로필
관리



원격 장치 데이터 삭제

Mobile Application Management (MAM)



모바일 앱 배포



개인 기기에 회사 데이터
저장 금지



앱 설정 및 업데이트 관
리



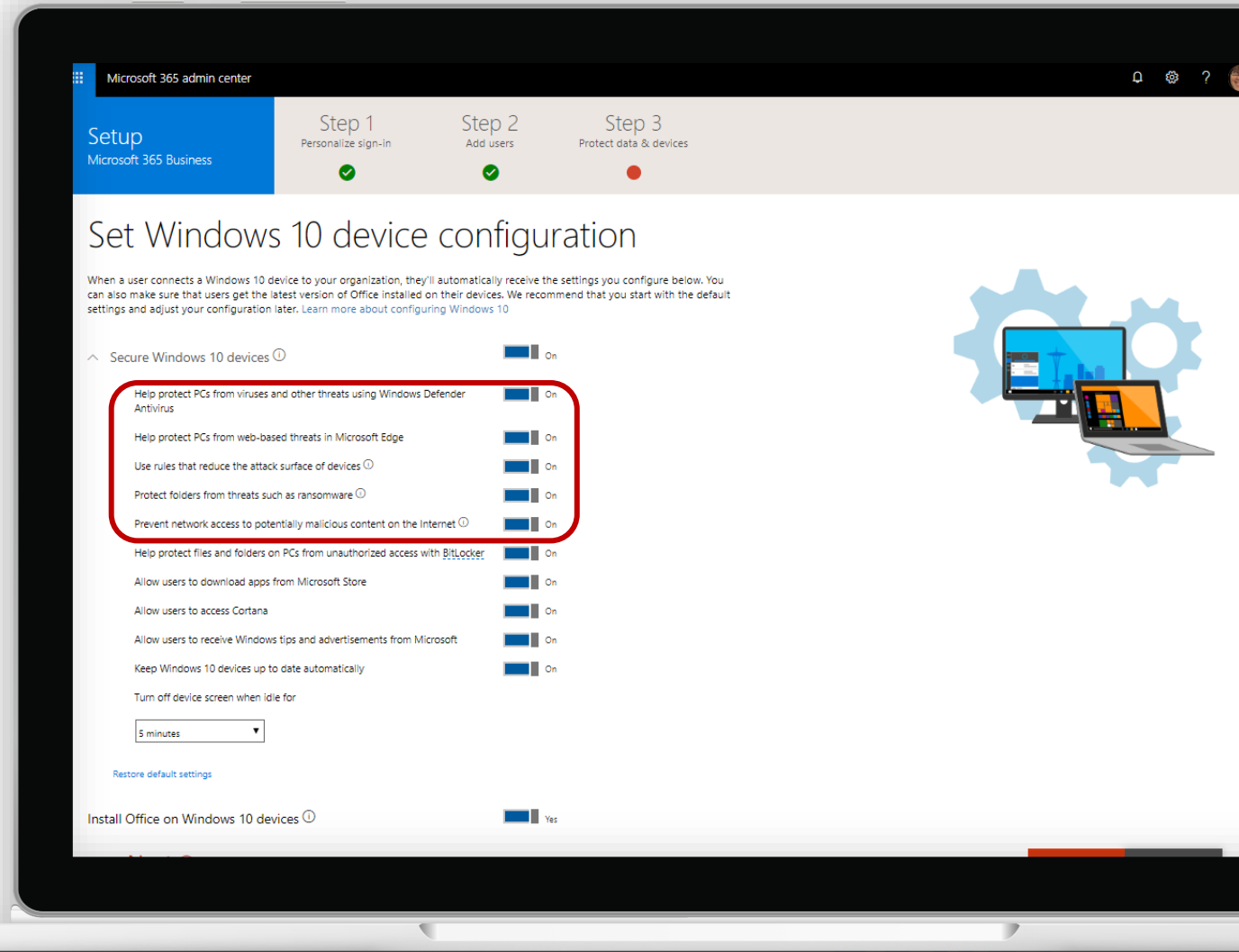
모바일 앱 데이터 내에서
회사데이터 보호

MAM회사 데이터 보호



Windows devices 장치 보안

- ▶ Windows 10 devices 자동 업데이트 설정
- ▶ Microsoft Defender protections 강제 활성화
- ▶ BitLocker encryption 활성화를 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 켜 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

감사 로그 검색

활동
모든 활동 결과 표시

× 모두 지우고 모든 활동 결과 표시

키워드를 입력하여 활동을 검색합니다.

검색

초대 및 액세스 요청 활동
초대 수락
초대 철회됨
액세스 요청 생성됨

결과 547개의 결과가 검색됨

날짜 사용자
2015년 9월 21일 16시... admin@...
2015년 9월 21일 16시... admin@contoso.com
2015년 9월 21일 16시... admin@contoso.com
2015년 9월 21일 16시... admin@contoso.com
2015년 9월 21일 16시... v-temp@contoso.com
2015년 9월 21일 16시... ping@contoso.com
2015년 9월 21일 16시... admin@contoso.com

검색이 완료되면 검색된 결과의 수가 표시됩니다.

파일에 액세스함
파일에 액세스함
파일 다운로드됨
파일에 액세스함
파일 수정됨
파일 이름 변경됨

항목 자세한 정보
admin_contoso_com_SThum... 사용자 사진/프로필 p...에서 확인함
Office 365 활동 보고서 실행... 문서에서 확인함
Office 365 활동 보고서 실행... 문서에서 다운로드함
IT 부서 급여.docx IT_Execs_Only에서 확인함
올림픽 (생물).xlsx 문서에서 수정함
배움 감사 - Exchange2.pptx 배움 감사_Final 이름이 변경됨

▽ 결과 필터링 ↓ 결과 내보내기

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score
Secure Score: 46%
178/122 points achieved

Actions to review
Regressed 0 To address 63 Planned 3 Risk accepted 3 Recently added 0 Recently updated 0

Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Microsoft Defender Application Guard managed mode	+1.1%	Risk accepted	Device
Block credential stealing from the Windows local security author...	+1.1%	To address	Device
Use advanced protection against ransomware	+1.1%	To address	Device
Block execution of potentially obfuscated scripts	+1.1%	To address	Device
Block Office applications from injecting code into other processes	+1.1%	To address	Device
Block executable content from email client and webmail	+1.1%	To address	Device
Encrypt all BitLocker-supported drives	+1.1%	To address	Device
Turn on PUA protection	+1.1%	Risk accepted	Device
Block ... from creating child processes	+1.1%	To address	Device

Breakdown by: Category

- Identity: 63%
- Data: No data to show
- Device: 45%
- Apps: 100%
- Infrastructure: No data to show

Comparison
Your score: 46%
Organizations like yours: No data to show
Custom comparison: 24%

Resources
Read about Secure Score capabilities
Do more with the Secure Score API

History Messages from Microsoft Need help? Give feedback

Microsoft 365 POC

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.



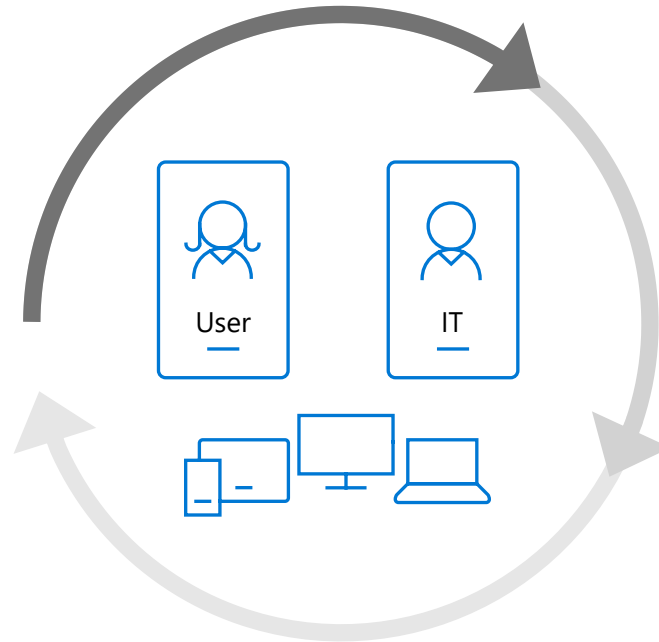
Device Lifecycle

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

Support & Retire

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



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

Protect

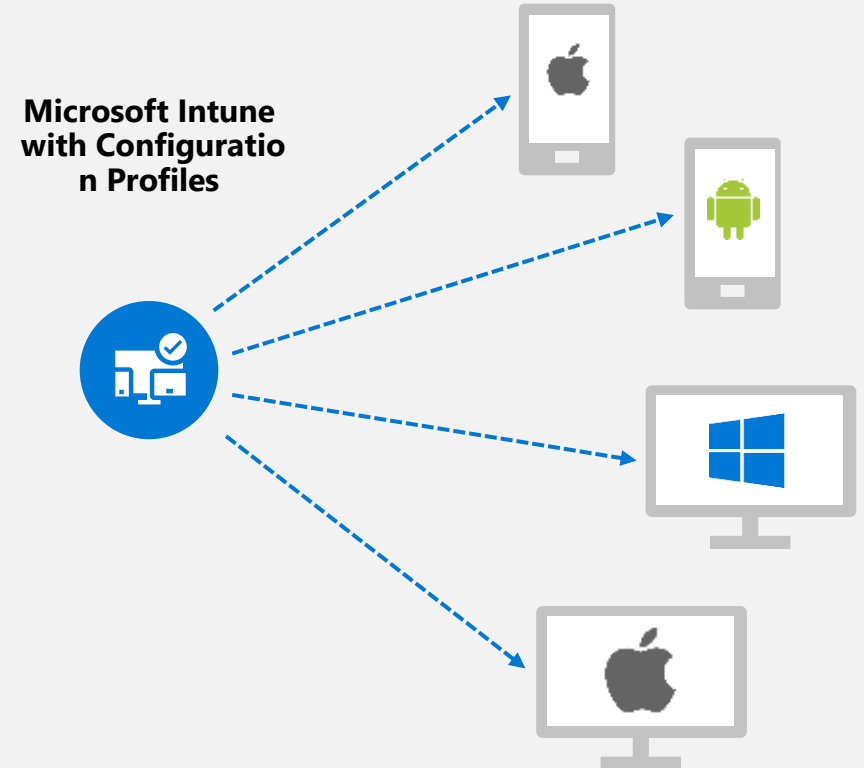
- ✓ Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- ✓ Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- ✓ Report on device and app compliance

What are Configuration Profiles?

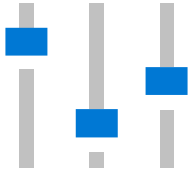
Microsoft Intune provides **Configuration Profiles** which includes **settings** and **features** that can be enabled or disabled on different devices within your organization.

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.

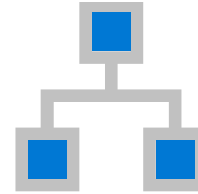
Examples: Airprint, notifications and lock screen messages.



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.



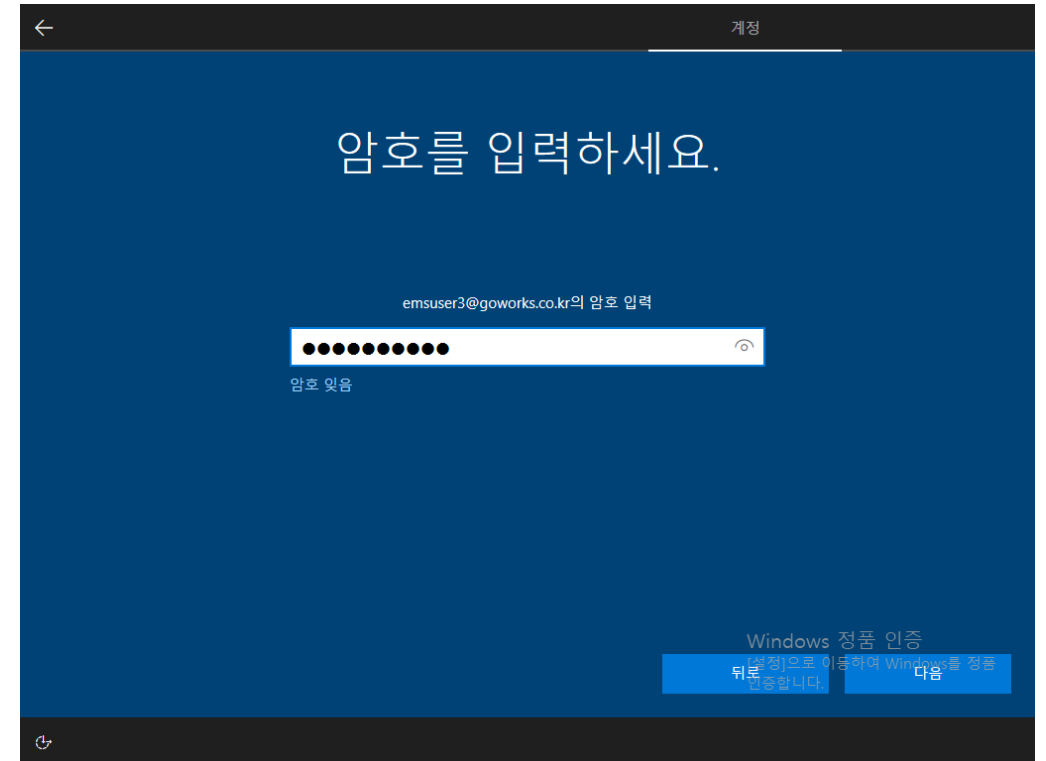
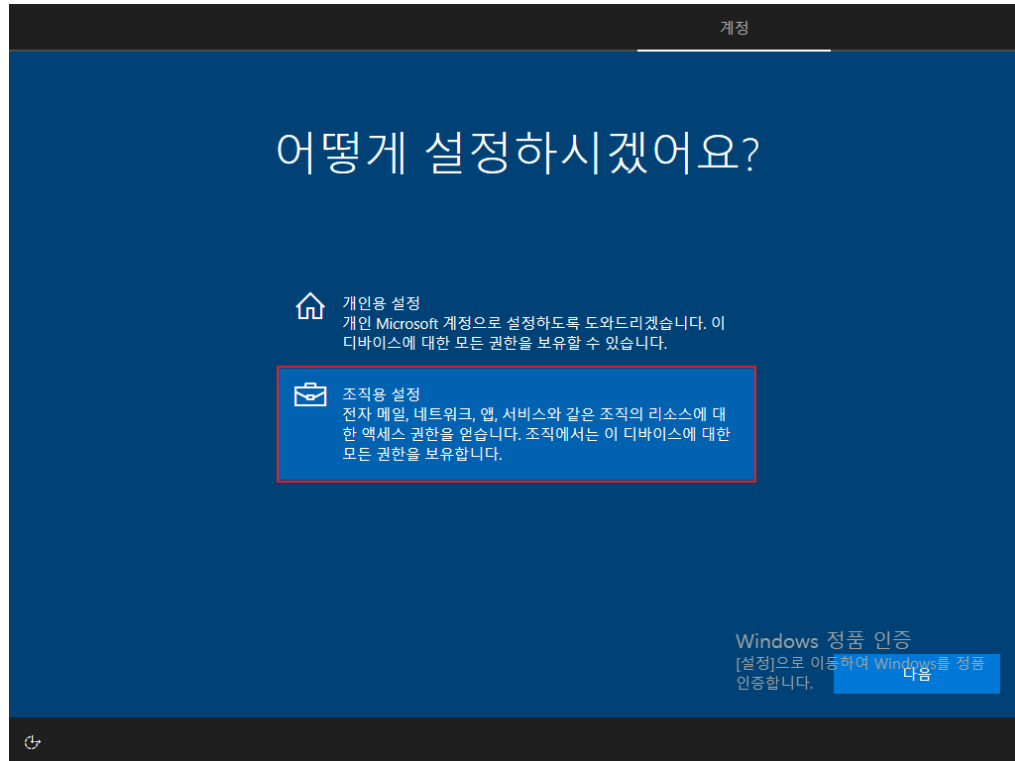
Custom

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.



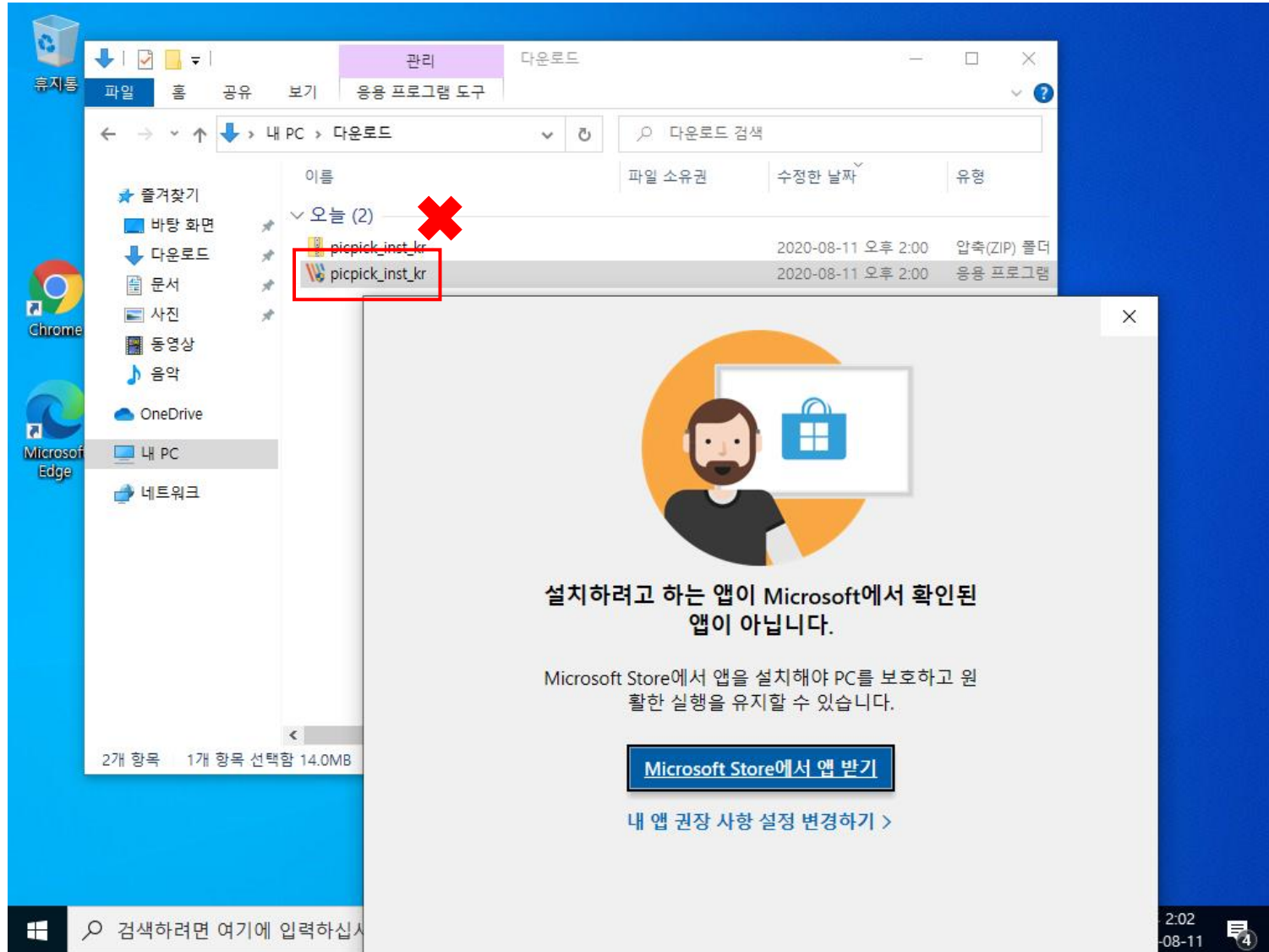
사용자 Windows 10 설정

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

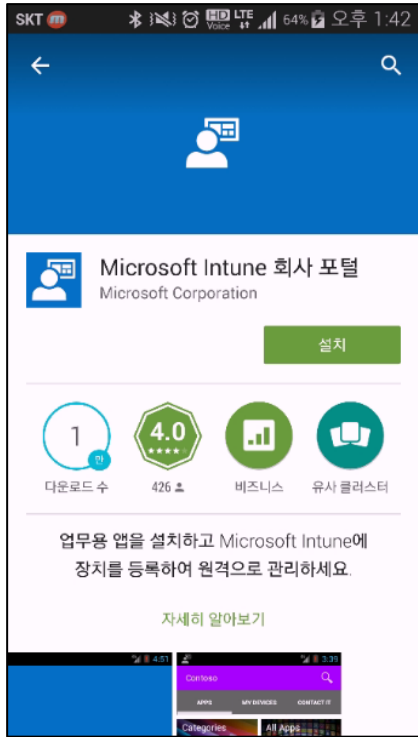
The screenshot displays a Windows 10 desktop environment. On the left, the Start menu is open, showing a list of installed applications including Microsoft Teams, Azure Information Protection 뷰어, Word, PowerPoint, Outlook, OneNote, Publisher, Access, 비즈니스용 Skype, and Excel. The Task View button is visible at the bottom of the Start menu. In the center, a context menu is open over the Start menu, listing various system services and executables such as Microsoft OneDrive Setup, Google Chrome Installer, and Windows Update. On the right, a Microsoft Word window is open, displaying a license agreement titled '라이선스 계약에 동의' (Agree to the license agreement). The agreement lists included Office 365 apps (Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access, and Skype) and includes a '수락' (Accept) button. The Windows taskbar at the bottom shows the search bar, task view button, and several pinned application icons. The system tray in the bottom right corner displays the date and time as '오전 10:37 2020-08-11'.

사용자 Windows 10 설정

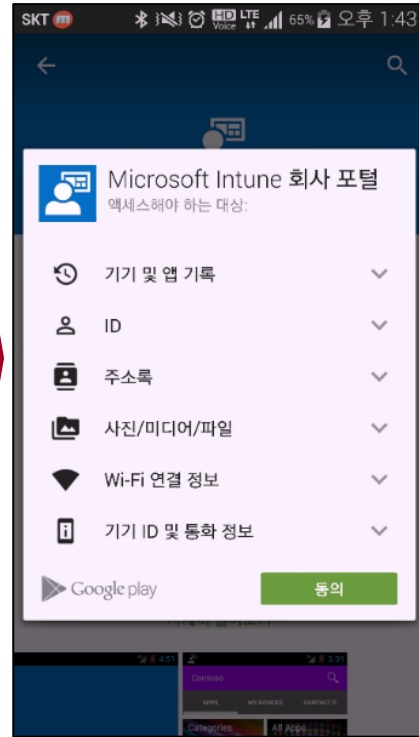
- 사용자는 PC에 일반적인 프로그램을 설치할 수 없습니다.
관리자의 설정에 따라 Windows 앱 스토어에서 인가된 앱만 설치하거나, 중앙에서 배포되는 앱만 사용할 수 있습니다.



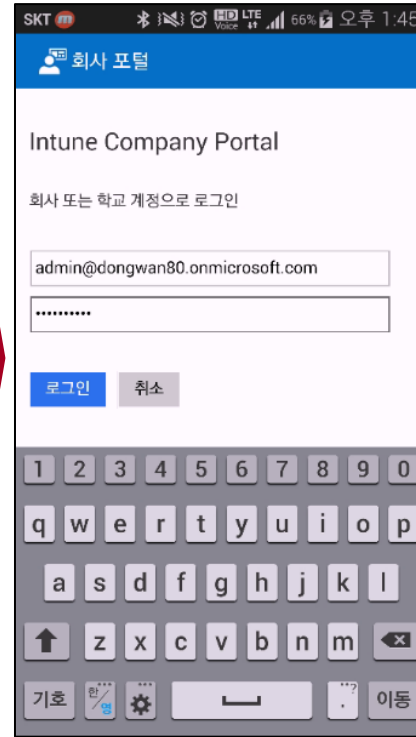
모바일 장치 등록



구글플레이에서
회사포털 검색



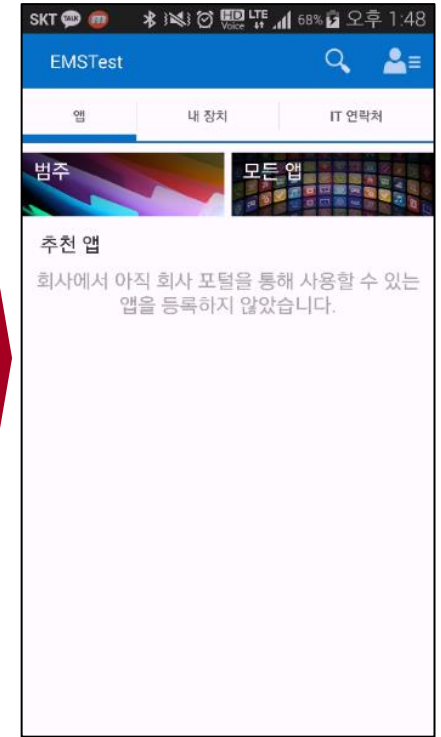
회사포털 설치



회사 계정 로그인

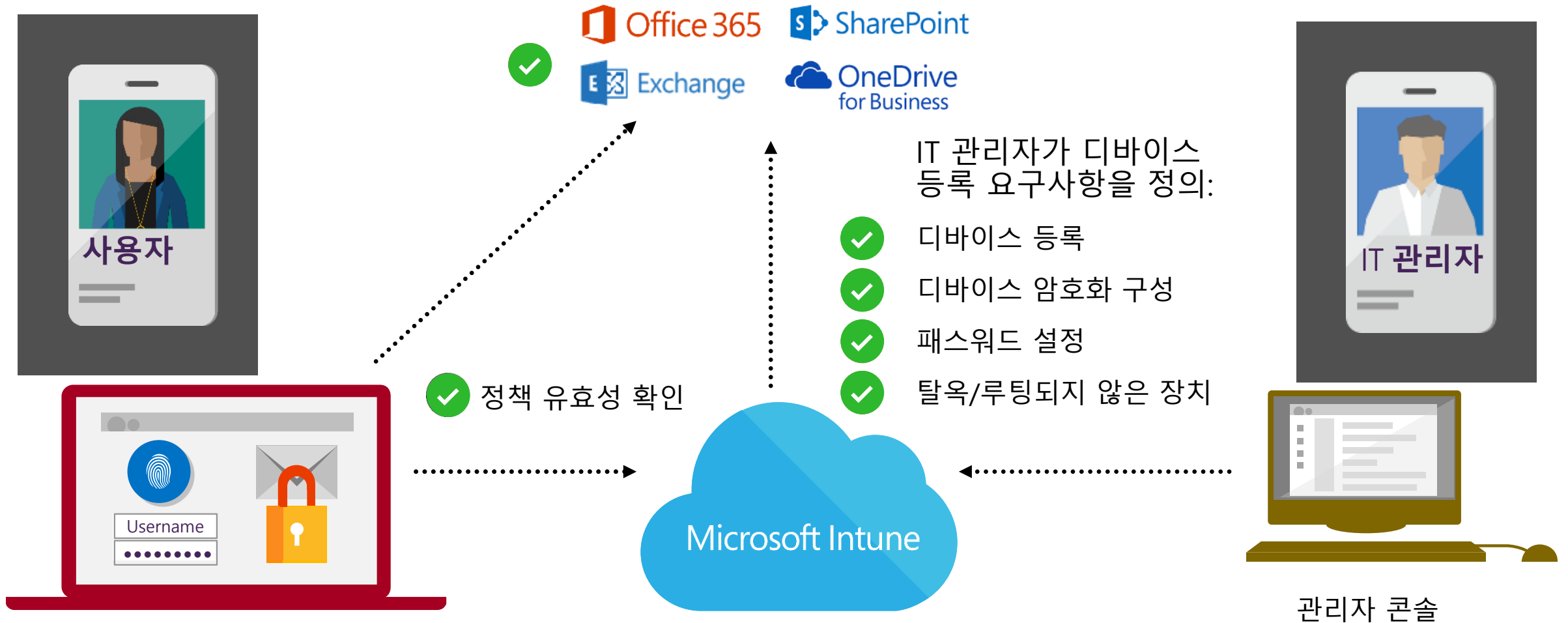


장치 등록



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.

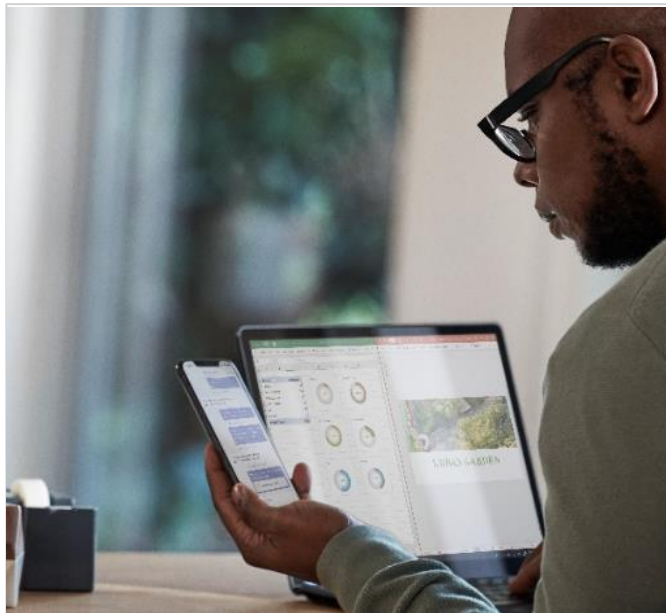
특징

- 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

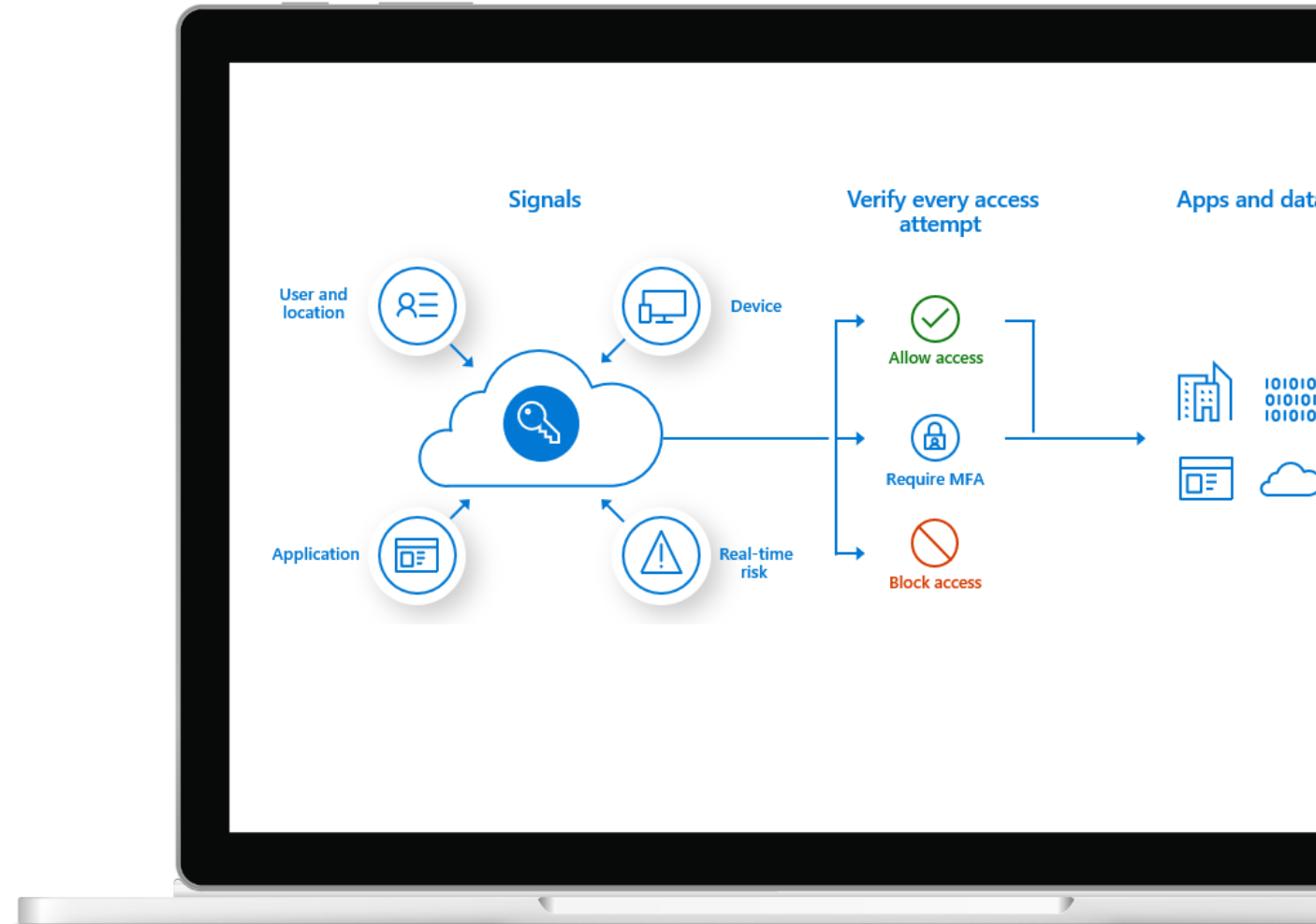
Requirement for Azure MFA can also be based on

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

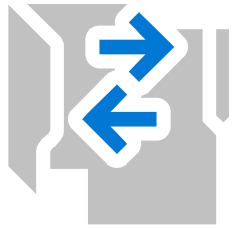
User registration for second factor at next sign in after enablement of Conditional Access policy

Requires Azure Active Directory Premium P1 license

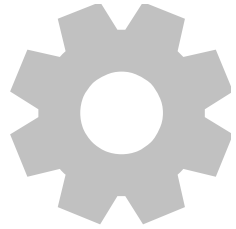
- Or any license that also includes both MFA and Conditional Access, such as Azure Active Directory Premium P2, Microsoft 365 Business, Microsoft 365 E3 or Microsoft 365 E5



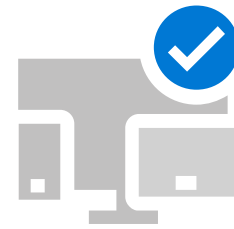
Self-Service Password Reset (SSPR)



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.

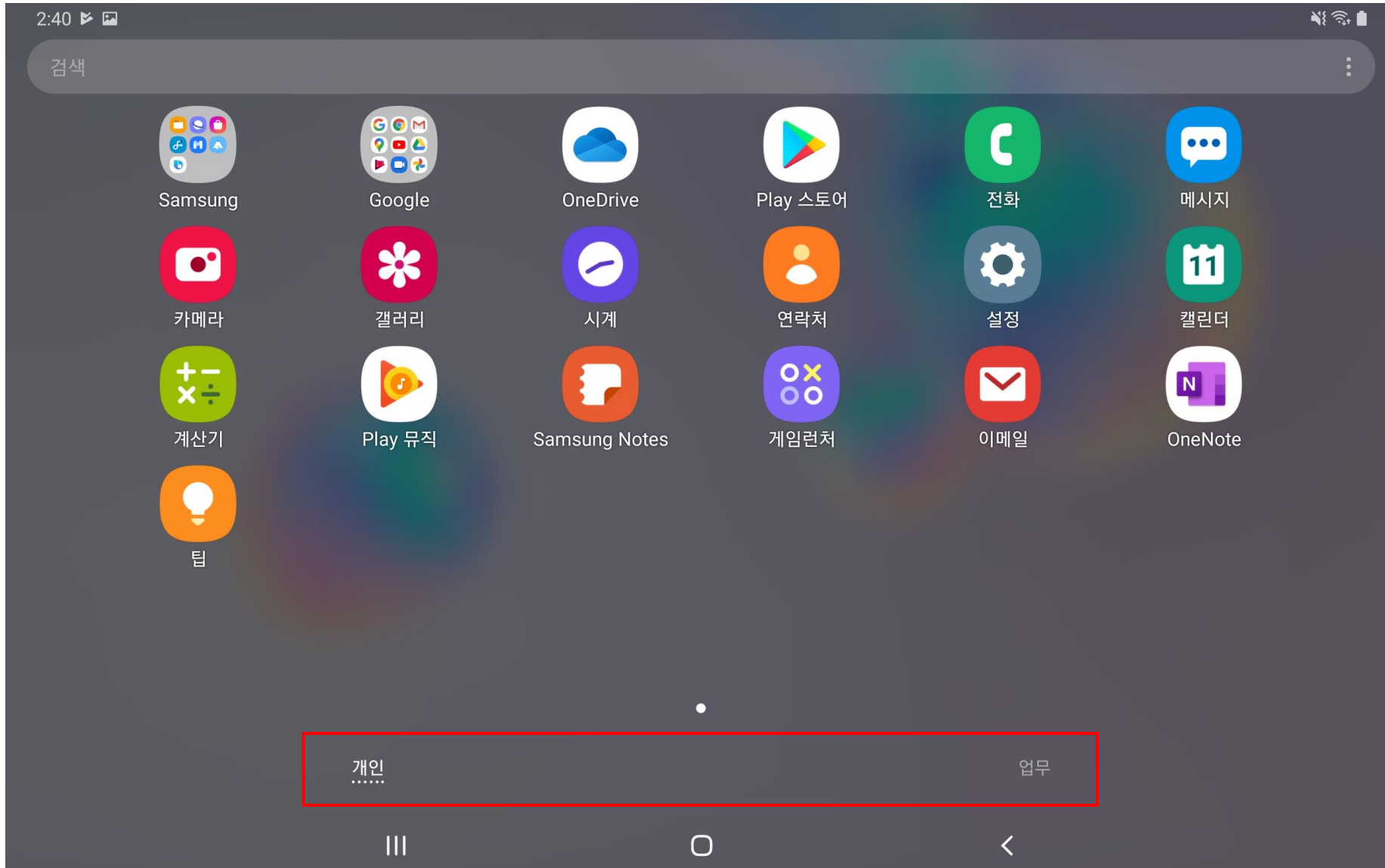
특징

- 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.



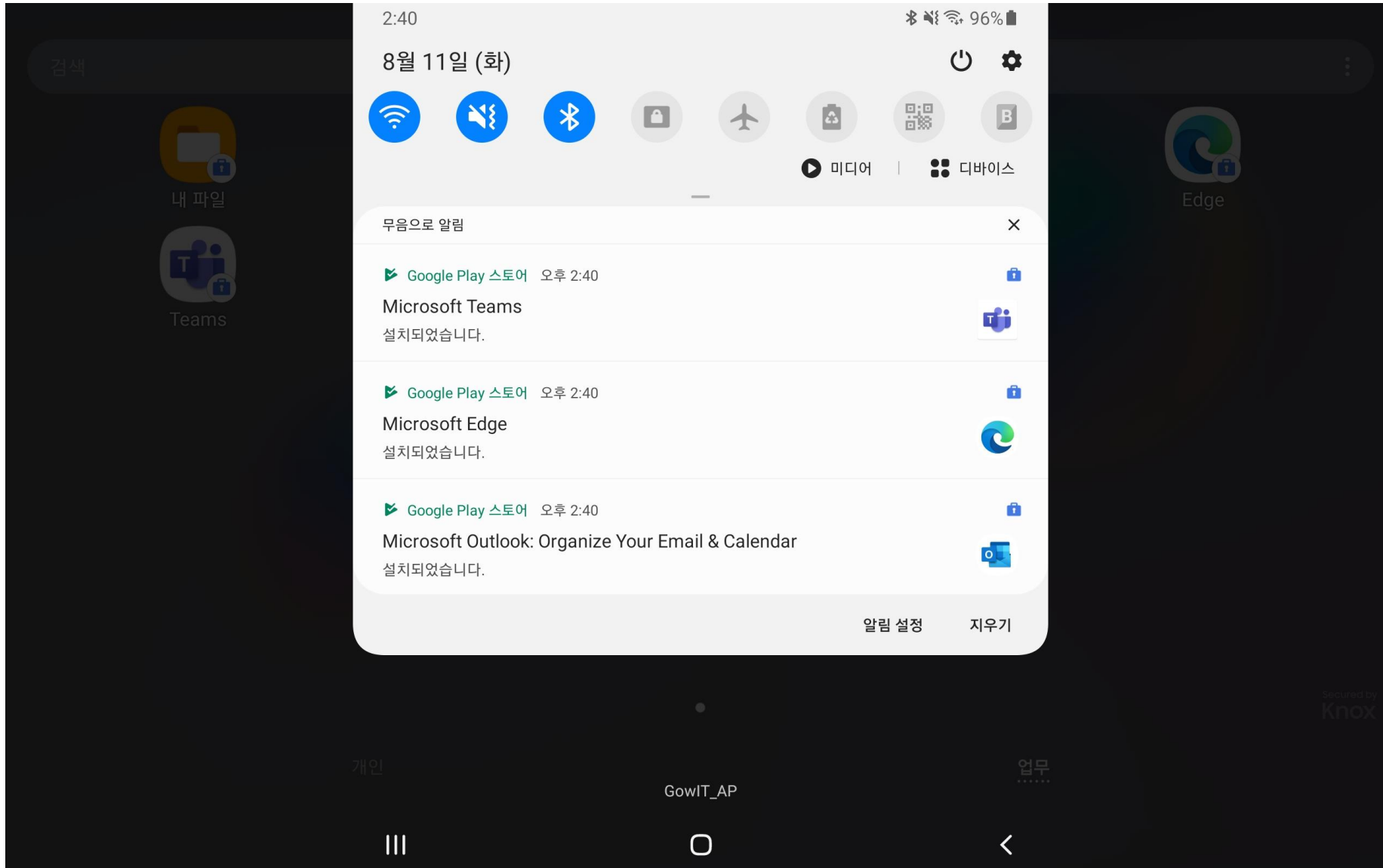
사용자 회사 모바일 장치 등록

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



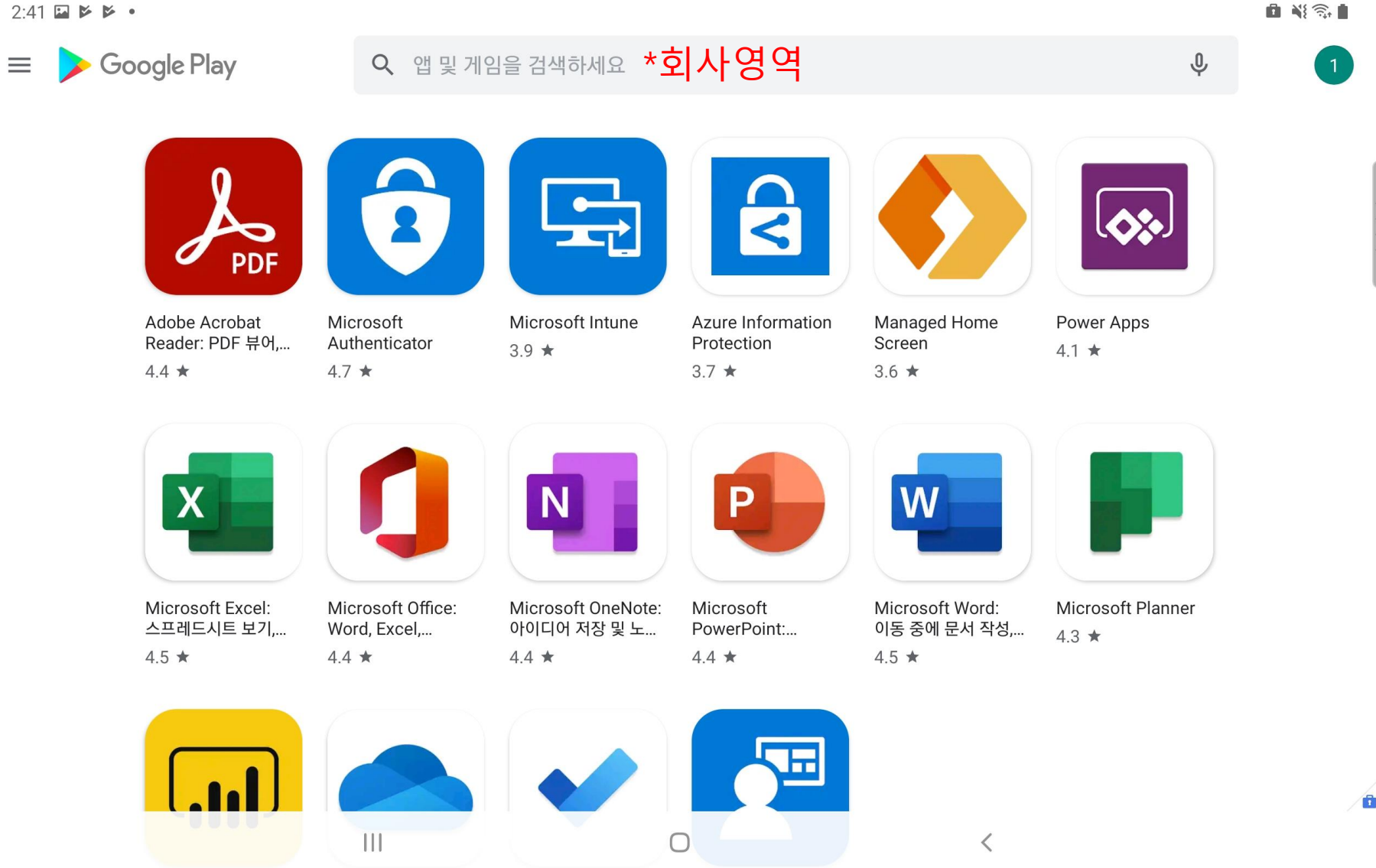
사용자 회사 모바일 앱 다운로드

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



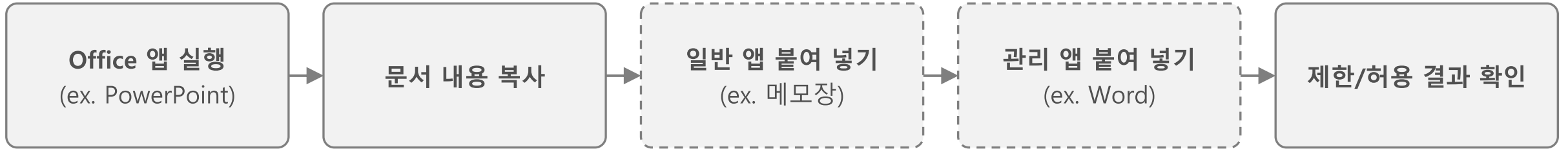
사용자 회사 모바일 앱 다운로드

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

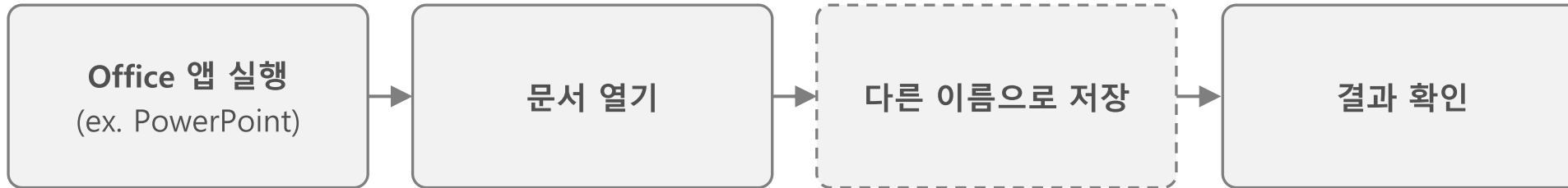


앱 데이터 보호

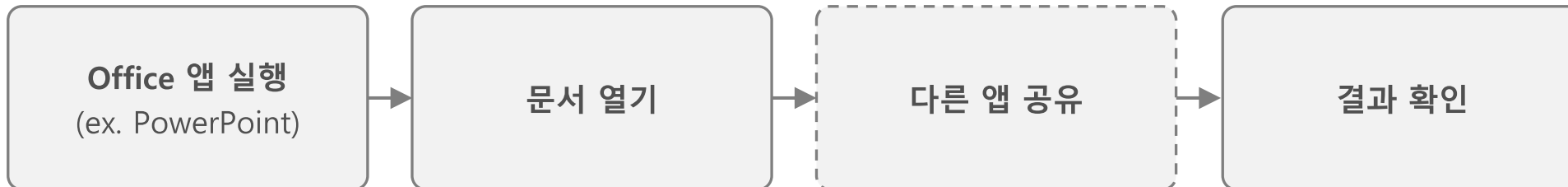
앱 허용/차단 - 클립보드



다른 이름으로 저장(Android)

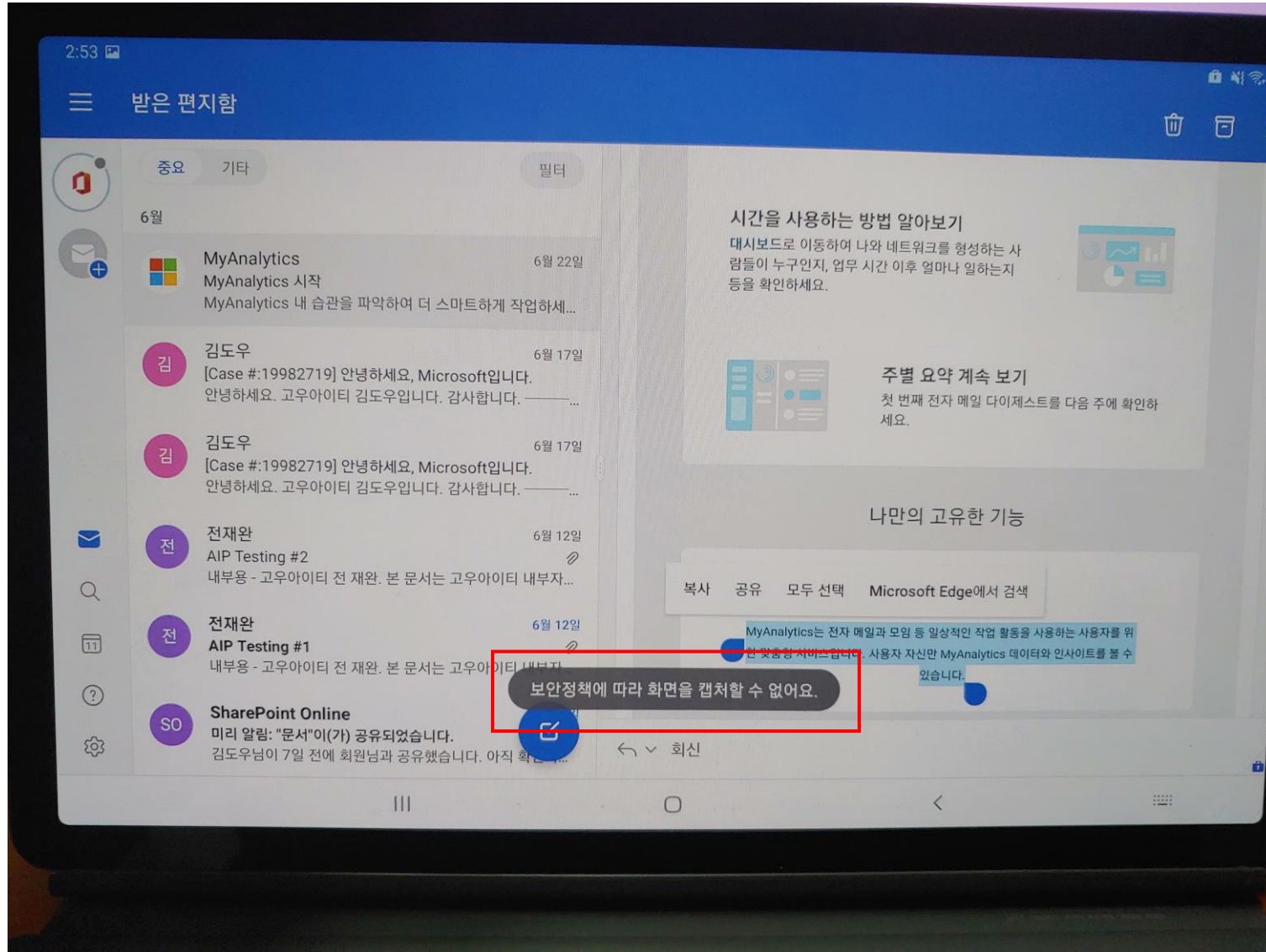


앱 허용/차단 - 공유



사용자 회사 모바일 앱 사용(등록)

- 일반적으로 사용자는 회사 앱을 실행할 경우, 스크린 캡처를 할 수 없도록 정책이 구성되어 있습니다. 해당 가이드에서는 사용자의 원활한 사용을 위하여, 일시적으로 캡처를 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)

The screenshot shows a mobile application interface divided into two main sections: a top light green section for the company area and a bottom white section for the personal area. A red 'X' is placed over the Microsoft logo in the company area, indicating a restriction. A red arrow points from a text box in the company area to a text box in the personal area.

***회사영역** (Company Area):

- 나만의 고유한 기능
- Outlook
- 복사 공유 모두 선택 Microsoft Edge에서 검색
- MyAnalytics는 전자 메일과 모임 등 일상적인 작업 활동을 사용하는 사용자를 위한 맞춤형 서비스입니다. 사용자 자신만 MyAnalytics 데이터와 인사이트를 볼 수 있습니다.

***개인영역** (Personal Area):

- Samsung Notes
- 카테고리 미지정
- 제목
- 개인 영역에서는 개인이 사용한 클립보드(복사, 붙여넣기)한 항목만 복사됩니다.

사용자 회사 모바일 앱 사용(데이터 공유)

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

나만의 고유한 기능

*회사영역

복사 공유 모두 선택 Microsoft Edge에서 검색 Outlook

MyAnalytics는 전자 메일과 모임 등 일상적인 작업 활동을 사용하는 사용자를 위한 맞춤형 서비스입니다. 사용자 자신만 MyAnalytics 데이터와 인사이트를 볼 수 있습니다

EMSUser
4월 23일 오후 7:39
안녕하세요. 고우아이티입니다.

← 회신

나
5월 23일 오후 6:49
dkssudgktpdy

← 회신

*회사영역

MyAnalytics는 전자 메일과 모임 등 일상적인 작업 활동을 사용하는 사용자를 위한 맞춤형 서비스입니다. 사용자 자신만 MyAnalytics 데이터와 인사이트를 볼 수 있습니다.

Teams

사용자 회사 모바일 앱 사용(데이터 공유)

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

*개인영역

Smart View

새 노트 작성 Samsung Notes 드라이브에 저장 리마인더

메시지 블루투스 연락처 > 나 이메일

모든 앱

드라이브에 저장 리마인더 메시지 블루투스

새 노트 작성 업무 연락처 > 나 이메일

*회사영역

나
오후 3:05

MyAnalytics는 전자 메일과 모임 등 일상적인 작업 활동을 사용하는 사용자를 위한 맞춤형 서비스입

← 회신

나
오후 3:06

개인 영역에서는 개인이 사용한 클립보드(복사, 붙여넣기)한 항목만 복사됩니다.

← 회신

GoCloud
by GowIT

이미지 첨부 중...

시나리오 4: PC 데이터 보호

PC 에서 데이터를 보호하고 유출을 방지할 수 있습니다.

목적

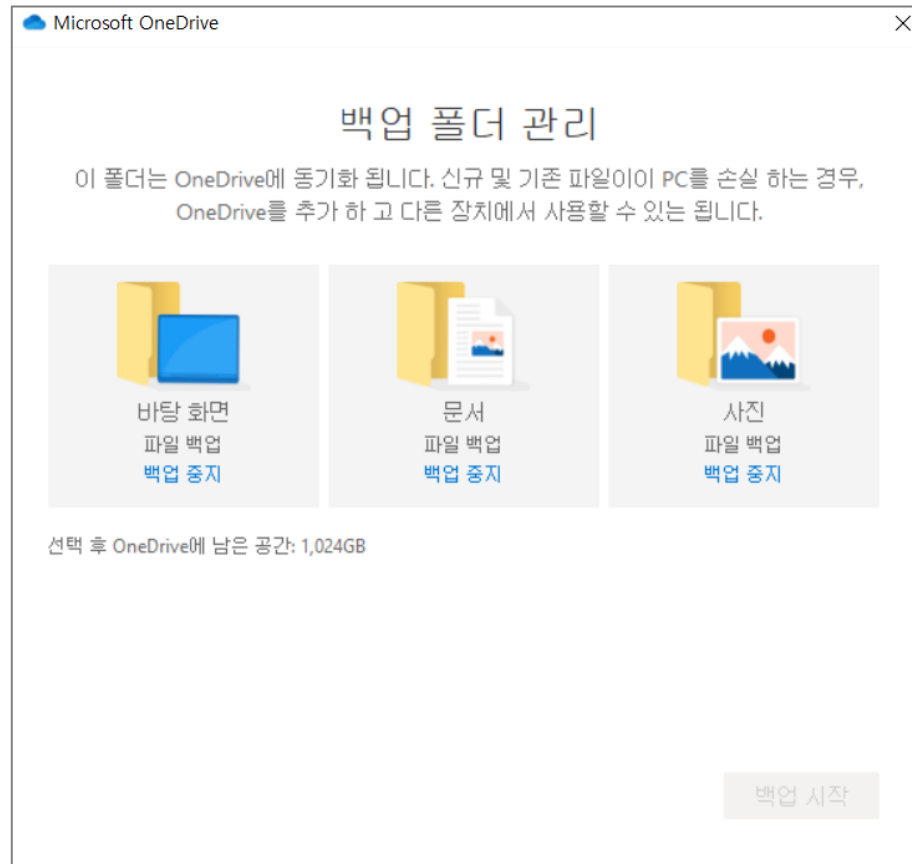
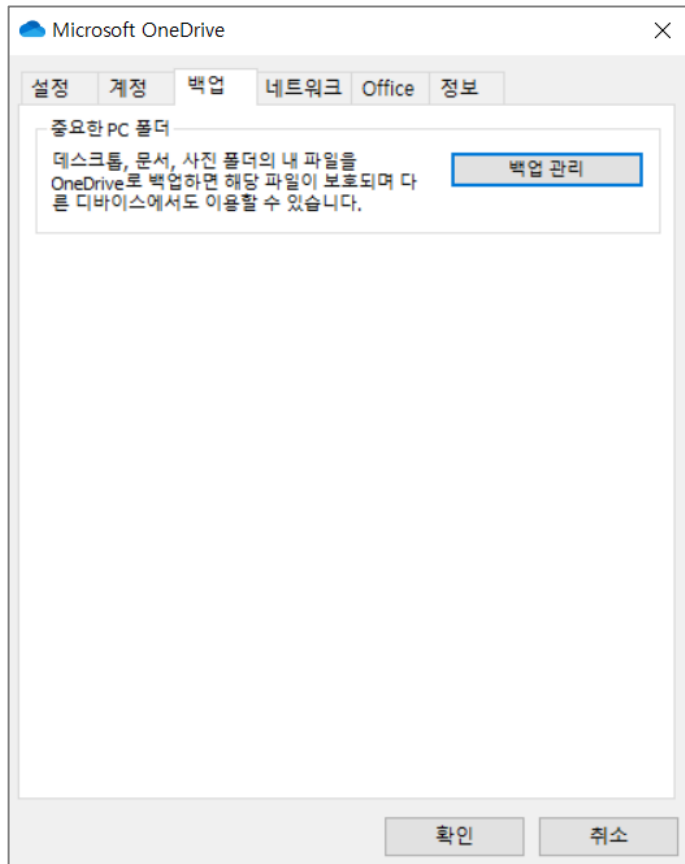
- 개인이 작성하는 문서를 랜섬웨어등의 공격으로 부터 보호할 수 있습니다.
- 조직의 데이터를 외부로 유출을 방지할 수 있습니다.

특징

- 개인 PC의 주요 데이터를 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



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

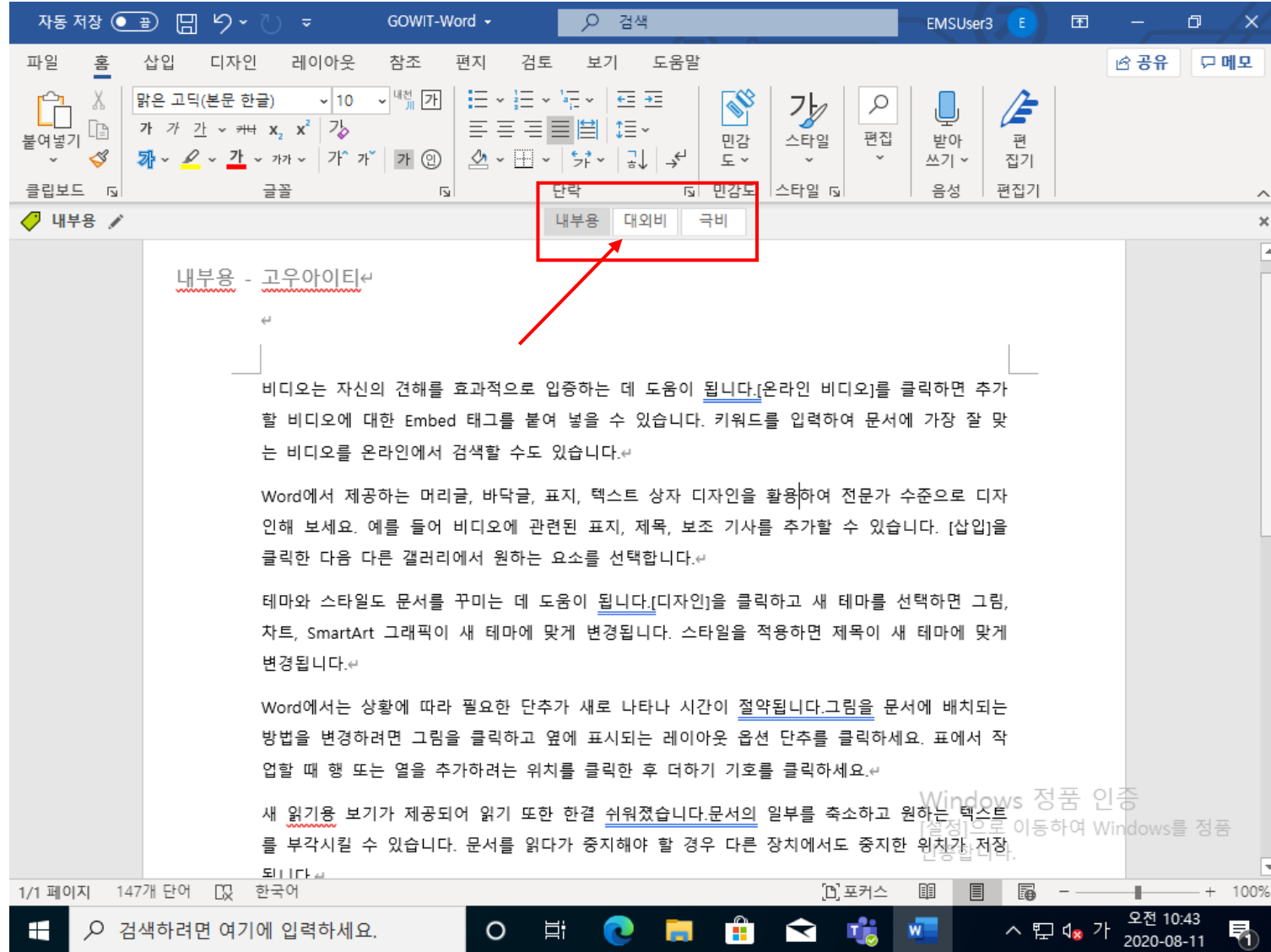


반출용

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

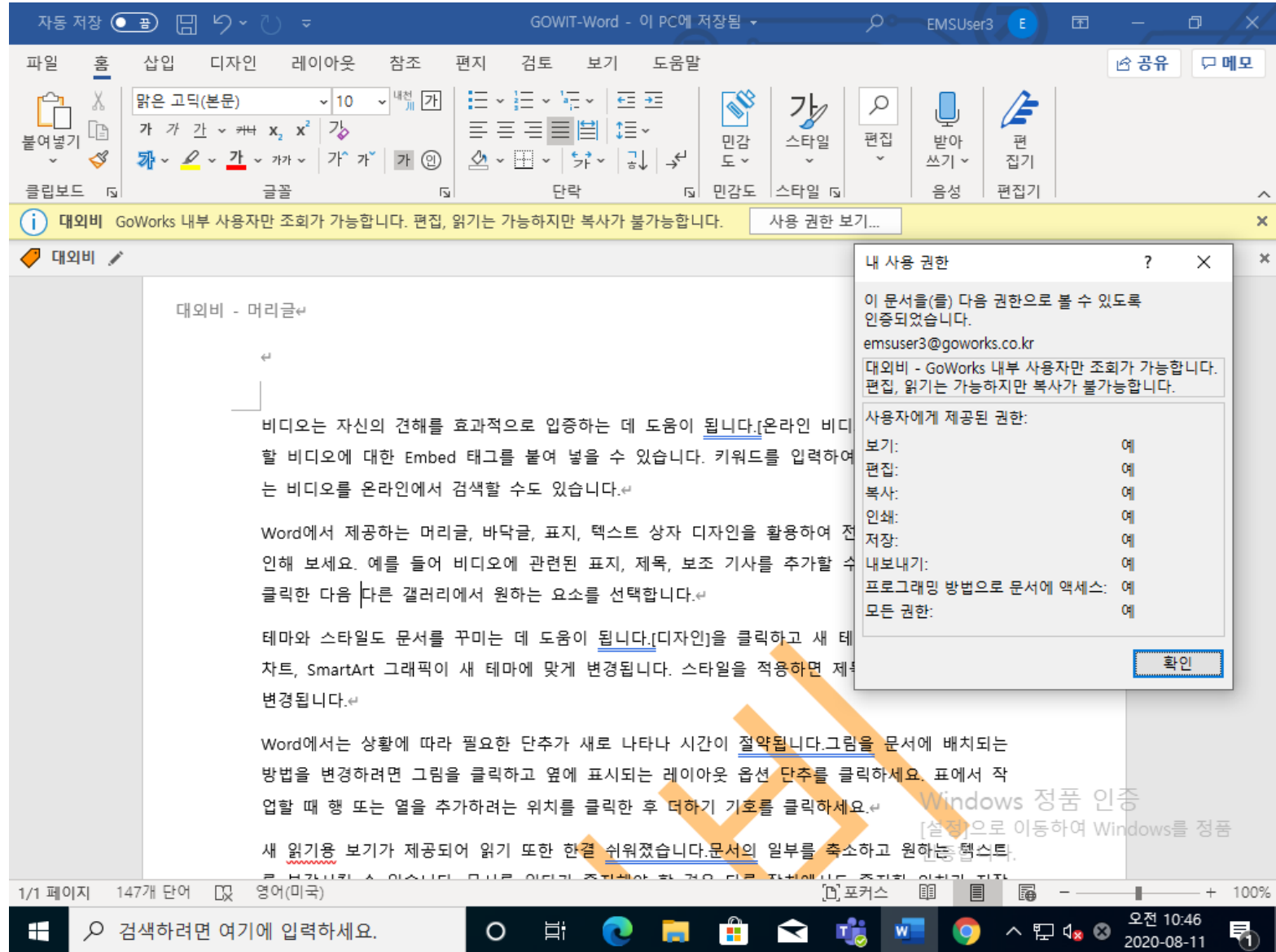
사용자 문서 보안 업무 환경

- 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

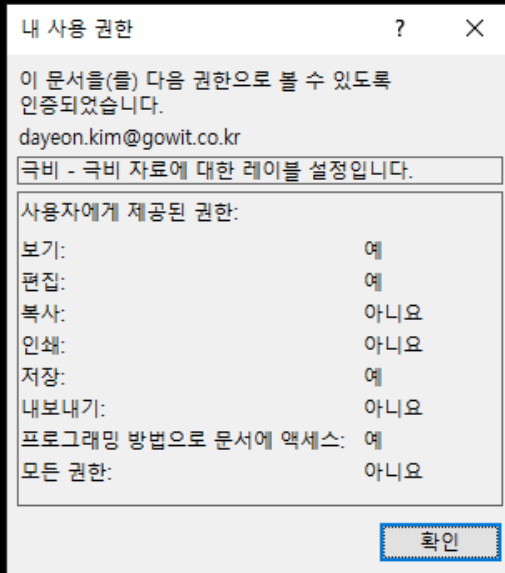
- 사용자는 기본 지정된 레이블 외에 다른 레이블을 지정하여 저장하면, 레이블에 따른 권한 및 암호화가 적용된 것을 확인할 수 있습니다.



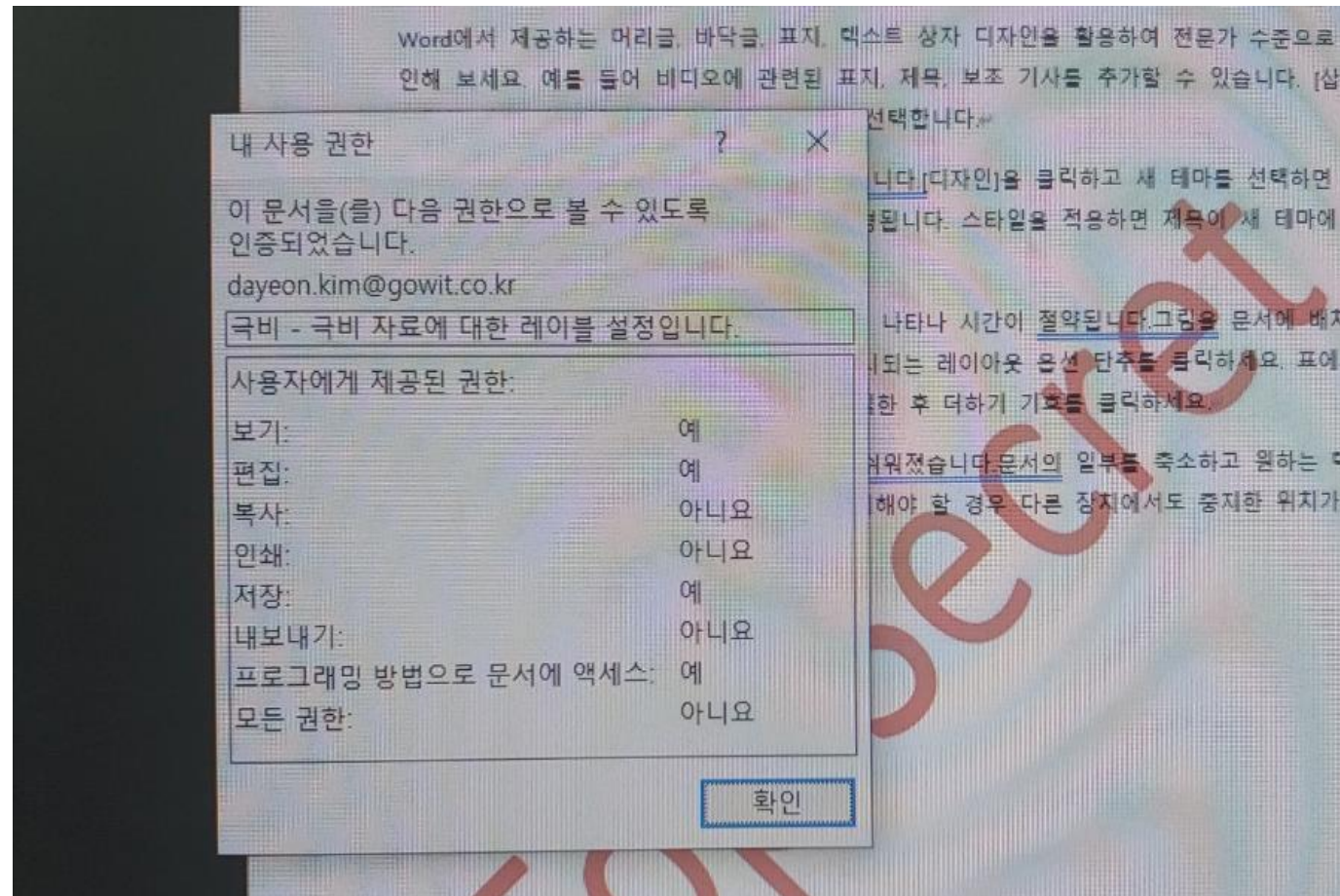
사용자 문서 보안 업무 환경

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

스크린 캡처 시

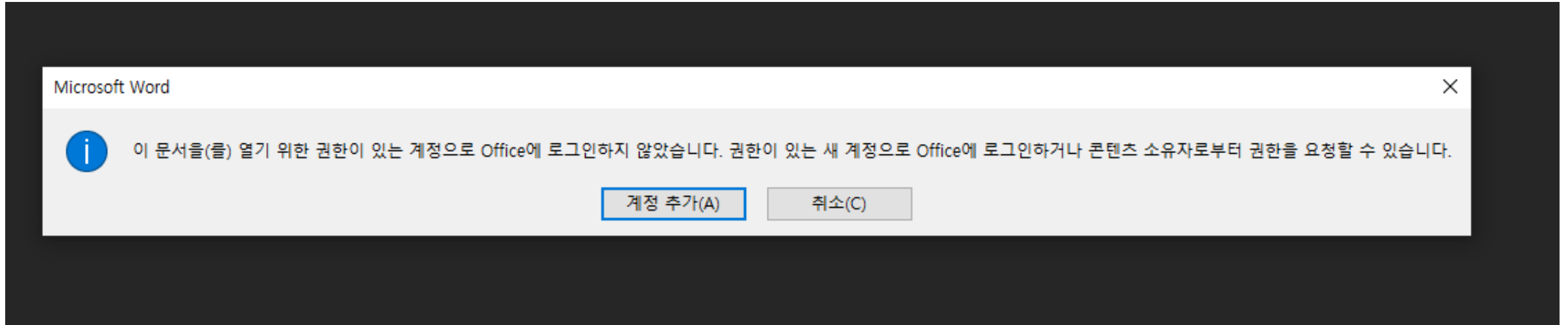


실제 화면



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.

대시보드 > 고우아이티

고우아이티 | 로그인

Identity Governance | 애플리케이션 목록 | 라이선스 | Azure AD Connect | 사용자 지정 도메인 이름 | 모바일(MDM 및 MAM) | 암호 재설정 | 회사 브랜딩 | 사용자 설정 | 속성 | 보안

모니터링 | **로그인** | 감사 로그 | 프로비저닝 로그(미리 보기) | 로그 | 진단 설정 | Workbooks | 사용자 및 인사이드

다운로드 | 데이터 내보내기 설정 | 문제 해결 | 새로 고침 | 열 | 피드백이 있나요?

날짜: 지난 24시간 | 날짜 표시 형식: 로컬 | 필터 추가

날짜	요청 ID	사용자	애플리케이션	상태	IP 주소	위치
2020. 8. 26. 오후 6:1...	c7d40fcb-5851-4b8b...	김도우	Microsoft Teams We...	성공	106.249.251.242	Bujeon-Dc
2020. 8. 26. 오후 6:0...	5cfb6d1c-d035-47fc...	Cheolho Jung	PowerApps	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	4c481c7c-68bf-4721...	김종진	Office 365 Exchange ...	성공	115.138.107.61	
2020. 8. 26. 오후 6:0...	12bd0f86-d23a-4d6...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	6458eee7-4a9e-482...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	e49711ba-116b-48b...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	a9c7e364-1a43-4cb0...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	ec6e960f-b0a7-4da2...	bc012d92-a26d-419...	GoWorksV3(DEV)	중단됨	106.249.251.242	
2020. 8. 26. 오후 6:0...	6495e8ba-7785-4a9...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	3a34746c-62a3-4e0f...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	c283d9c8-5f23-48ac...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	e1c1bcc-6348-46e3...	이창영	Office365 Shell WCS...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	dfd3cdc-35f9-4cf0...	송영식	Office Online Client ...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	0ceb4a6-bc02-4f4a...	송영식	Microsoft Office We...	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	22d92aad-9466-4cf9...	유창우	Windows Sign In	성공	106.249.251.242	
2020. 8. 26. 오후 6:0...	f6b9be5d-479f-4369...	이재훈	GoWorks Demo	성공	106.249.251.242	

대시보드 > 고우아이티

고우아이티 | 감사 로그

Identity Governance | 애플리케이션 목록 | 라이선스 | Azure AD Connect | 사용자 지정 도메인 이름 | 모바일(MDM 및 MAM) | 암호 재설정 | 회사 브랜딩 | 사용자 설정 | 속성 | 보안

모니터링 | 로그인 | **감사 로그** | 프로비저닝 로그(미리 보기) | 로그 | 진단 설정 | Workbooks | 사용자 및 인사이드

다운로드 | 데이터 내보내기 설정 | 새로 고침 | 열 | 피드백이 있나요?

날짜: 지난 24시간 | 날짜 표시 형식: 로컬 | 서비스: 모두 | 범주: 모두 | 활동: 모두 | 필터 추가

날짜	서비스	범주	활동	상태	상태 이유	대상
2020. 8. 26. 오후 4:5...	Core Directory	UserManagement	Update user	Success		Kyungbael
2020. 8. 26. 오후 4:1...	Core Directory	UserManagement	Update user	Success		dayeon.kir
2020. 8. 26. 오후 12:...	Core Directory	Device	Update device	Success		MyPad
2020. 8. 26. 오전 11:...	Core Directory	Device	Update device	Success		DESKTOP-
2020. 8. 26. 오전 10:...	Core Directory	UserManagement	Update user	Success		Jinho.Ha@
2020. 8. 26. 오전 10:...	Core Directory	UserManagement	Update user	Success		hanyoung_
2020. 8. 26. 오전 9:3...	Core Directory	Device	Update device	Success		samsungSI
2020. 8. 26. 오전 9:1...	Core Directory	DirectoryManagement	Set Company Inform...	Success		고우아이티

세부 정보

활동	대상	수정된 속성	행위자(시작한 사람)	자세한 정보
활동			유형	애플리케이션
날짜	2020. 8. 26. 오후 12:22:06		표시 이름	Microsoft.Intune
활동 형식	Update device		앱 ID	
상관 관계 ID	2496a48b-cf5d-40d2-a093-5dd987771136		서비스 사용자 ID	fc3e5beb-4bc5-4ff5-9595-4d7d6393e17d
범주	Device			

모니터링

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

The screenshot displays the Office 365 Security & Compliance Center interface. On the left is a navigation pane with various security and compliance tools. The main content area shows the 'Audit Log Search' page. At the top, there is a breadcrumb '홈 > 감사 로그 검색' and a title '감사 로그 검색'. Below the title is a descriptive paragraph explaining the search functionality. A search bar contains the text '검색' and a '지우기' button. Below the search bar is a table with columns for '작업', '날짜', 'IP 주소', '사용자', '작업', '항목', and '세부 정보'. The table is currently empty, and a message box above it states '모든 작업 결과를 표시하려면 모두 선택 취소하세요.' The navigation pane on the left includes items like '레코드 관리', '정보 거버넌스', '감독', '위협 관리', '메일 흐름', '데이터 개인 정보 보호', '검색', '콘텐츠 검색', '감사 로그 검색', '생산성 앱 검색', 'eDiscovery', '데이터 조사', and '보고서'.

홈 > 감사 로그 검색

감사 로그 검색

사용자가 문서를 삭제했는지 또는 관리자가 누군가의 암호를 재설정했는지 확인해야 하나요? Office 365 감사 로그를 검색하면 조직의 사용자 및 관리자가 어떤 작업을 수행했는지 찾을 수 있습니다. 전자 메일, 그룹, 문서, 사용 권한, 디렉터리 서비스 등에 관련된 활동을 찾을 수 있습니다. [감사 로그 검색 방법에 대해 자세히 알아보기](#)

검색 지우기 결과

작업 날짜 IP 주소 사용자 작업 항목 세부 정보

모든 작업의 결과 표시

× 모든 작업 결과를 표시하려면 모두 선택 취소하세요.

검색

파일 및 페이지 활동

파일에 액세스함	파일에 대해 보존 레이블 변경됨
레코드로 표시된 삭제된 파일	파일 체크인됨
레코드 상태가 잠김으로 변경되었습니다.	레코드 상태가 잠금 해제로 변경되었습니다.
파일 체크 아웃됨	파일 복사됨
파일 체크 아웃 취소됨	파일 삭제됨
휴지통에서 파일 삭제됨	2단계 휴지통에서 파일 삭제됨
문서 민감도 불일치 감지됨	파일에서 맬웨어 검색됨
파일 다운로드됨	파일 수정됨
파일 이동됨	파일의 모든 부 버전이 재생됨
파일의 모든 버전이 재생됨	파일의 버전이 재생됨

모니터링

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

경고 정책

경고 정책을 사용하여 조직의 사용자 및 관리자 활동, 멀웨어 위협 또는 데이터 손실 인시던트를 추적합니다. 경고를 받을 활동을 선택한 후에는 조건을 추가하고 경고를 트리거할 시점을 결정하고 알림을 받을 사람을 지정하여 정책을 조정합니다. 경고 정책에 대한 자세한 정보

[+ 새 경고 정책](#) [필터](#)

<input type="checkbox"/>	이름	심각도 ...	유형	범주	수정된 날짜	상태
<input type="checkbox"/>	파일에서 멀웨어 검색됨	● 높음	사용자 지정	데이터 손실...	20. 8. 25. 오후 4:36	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Suspicious email sending pattern...	● 보통	시스템	위협 관리	-	<input type="checkbox"/>
<input type="checkbox"/>	Unusual volume of sensitive file ...	● 보통	시스템	데이터 손실...	-	<input type="checkbox"/>
<input type="checkbox"/>	Elevation of Exchange admin priv...	● 낮음	시스템	사용 권한	-	<input type="checkbox"/>
<input type="checkbox"/>	Email messages containing malw...	● 정보	시스템	위협 관리	-	<input type="checkbox"/>
<input type="checkbox"/>	Malware campaign detected and ...	● 낮음	시스템	위협 관리	-	<input type="checkbox"/>
<input type="checkbox"/>	Email reported by user as malwar...	● 정보	시스템	위협 관리	-	<input type="checkbox"/>
<input type="checkbox"/>	Unusual volume of file deletion	● 보통	시스템	정보 거버넌스	-	<input type="checkbox"/>
<input type="checkbox"/>	Unusual external user file activity	● 높음	시스템	정보 거버넌스	-	<input type="checkbox"/>

GowIT Office 365 보안 및 준수

홈 > 알림 > 경고 보기

경고 보기

심각도 경고 이름 상태 범주 활동 수 마지막 발생...

<input checked="" type="checkbox"/>	● 보통	Unusual volume of file dele...	활성	정보 거버넌스	30	1일 전
<input type="checkbox"/>	● 보통	Unusual volume of file dele...	활성	정보 거버넌스	41	1일 전
<input type="checkbox"/>	● 보통	Unusual volu...				
<input type="checkbox"/>	● 보통	Unusual volu...				
<input type="checkbox"/>	● 보통	Unusual volu...				
<input type="checkbox"/>	● 보통	Unusual volu...				
<input type="checkbox"/>	● 보통	Unusual volu...				
<input type="checkbox"/>	● 보통	Unusual volu...				

활동 목록

사용자에게 알림 [내보내기](#)

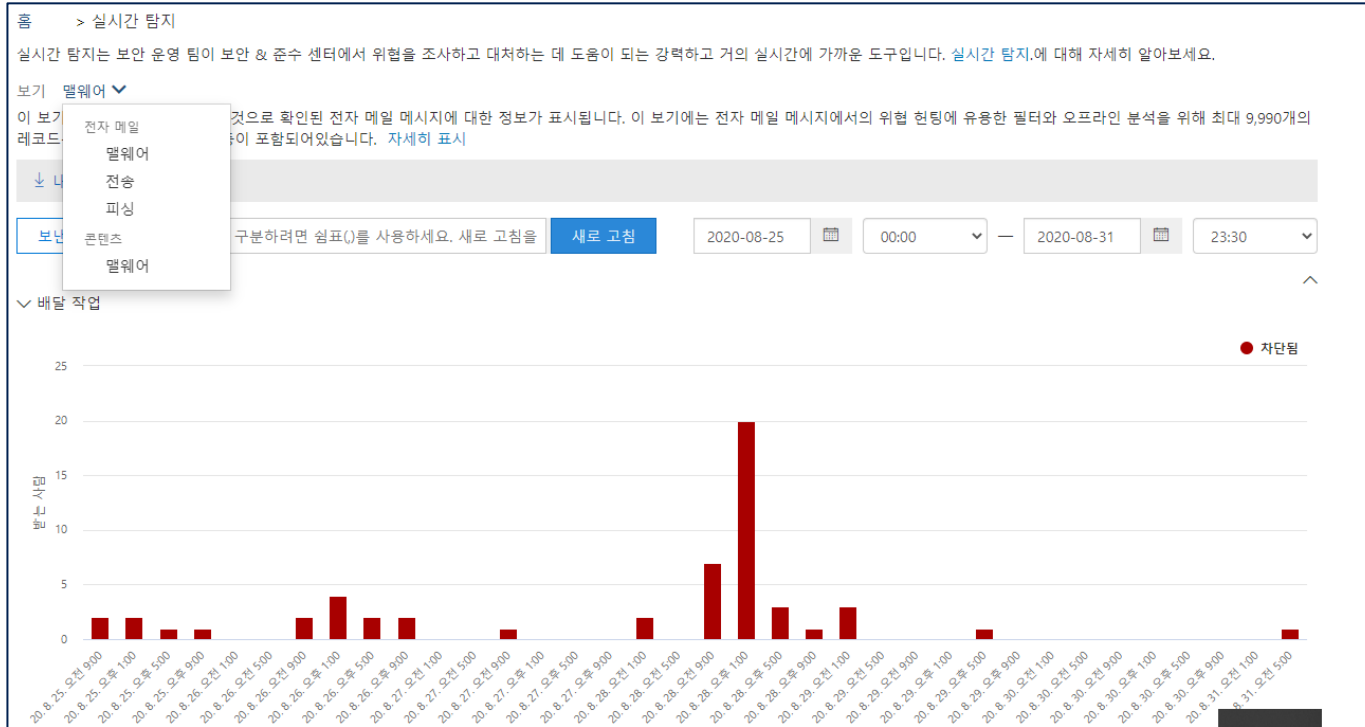
<input type="checkbox"/>	날짜	작업	사용자:	항목	IP 주소
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200725_10401...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200724_19334...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200724_19333...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200503_09421...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200430_12524...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200430_11231...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200425_17422...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200415_16190...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200430_11230...	106.249.251.242
<input type="checkbox"/>	2020. 8. 25. 오전 ...	FileDeleted	jaewan.chon@go...	20200408_10573...	106.249.251.242

46개 항목이 로드되었습니다.

[닫기](#)

모니터링

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



날짜 (UTC +09:00)	제목	받는 사람	보낸 사람	보낸 사람 IP	특수 작업	배달 작업
20. 8. 26. 오후 3:08	Undeliverable: Tota...	yuna.kim@gowit.co...	MicrosoftExchange...	0.0.0.0	-	차단됨
20. 8. 26. 오후 3:08	Total of Three (3) ...	yuna.kim@gowit.co...	yuna.kim@gowit.c...	45.95.171.110	-	차단됨
20. 8. 26. 오후 1:04	Undeliverable: You...	emailadmin@dom...	postmaster@gowit...	0.0.0.0	-	차단됨
20. 8. 26. 오후 1:04	You have Three (3)...	yuna.kim@gowit.co...	emailadmin@dom...	45.95.171.110	-	차단됨
20. 8. 26. 오전 11:57	Undeliverable: Total of Three (3) Messages Pending Delivery On Your e-Mail Portal yuna.kim@gowit.co.kr as of 8/26/2020 2:08:20 p.m.					

항목 7개 중 7개 로드됨

요약	세부 정보	첨부 파일	장치	전자 메일 시간 표시 막대	유사한 전자 메일
받는 사람	yuna.kim@gowit.co.kr				
받은 시간 (UTC +09:00)	2020. 8. 26. 오후 3:08:29				
회신 경로	yuna.kim@gowit.co.kr				
보낸 사람	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@GowITCo.onmicrosoft.com				
보낸 사람 이름	Microsoft Outlook				

완료