M. Cloud Bridge
Specialized Consulting Firm in Data & AI

Specialized Consulting Firm in Data & AI Cloud System

Data & BI
Big Data & AI
Data Flow & Automation
Data Infra & Security

[생산성]과 [보안]이 중요한 중소기업을 위한 통합솔루션 Microsoft 365 Business Premium에서 제공되는 보안 기능 알아보기

데이터에 가치를 더하여 고객의 성장에 공헌합니다.
Specialized Consulting Firm in **Data & AI** Cloud System

Copyrightⓒ 2022-2023 by M(Multi) Cloud Bridge Co., Ltd All rights reserved.

M. Cloud Bridge
Multi Cloud Bridge

오늘 전달 드릴 이야기

1. **변화하는 환경에서의 고민과 걱정**

- 우리는 이런 고민과 걱정을 하고 있습니다.
- 협업 시나리오로 알아보는 업무 혁신

2. **보안 시나리오로 알아보는 업무 혁신**

- ID 및 액세스 제어 How To
- 클라우드 컨텐츠 보안 How to(1)
- 클라우드 컨텐츠 보안 How to(2)
- Endpoint 보안 How To

3. **Why Microsoft 365 Premium**

1. 고민과 걱정

" 우리는 이런 고민과 걱정을 하고 있습니다 "

관리자 & 사용자 해결 과제

관리자 해결 과제

- 직원들의 디바이스 관리
- 외부로의 정보 유출
- 랜섬웨어, 피싱 등..

사용자 해결 과제

- 실시간 팀워크
- 원활한 외부 협업
- 어디에서나 미팅 참여

But... 현실은...

이메일 / 문서작업
메신저 / 화상회의
콘텐츠 관리 / 시스템
별로 따로 운영 되어서…

이메일에 사용되는 시간 28%
이메일 읽은 후 다른 일에 다시
몰입하는 데 걸리는 시간
16분

관리자들이 놓치는 정보의 비중
59%
필요한 정보를 찾는데 사용하는
시간 20%

But... 현실은...

기존 팀 프로세서의 어려움은 모든 팀의 요구사항은 다르며, 한가지의 방법으로 모든 협업 요구사항을 만족할 수 있는 방법은 존재하지 않음

A팀

필요한 자료를 찾으려고 한나절 보내는 거 같다.최신파일은?"
당췌 우리 팀원의 행적을 모르겠네"

B부서

"이기종 데이터 원본의 자료도 같이 검색해 보면 좋을 것 같은데 문서 분류를 할 수 없을까?"
"데이터 취합은 막내 일?"

C본부

"품의서 양식은 공유 폴더 어디에 있나요?"
"용량 큰 대용량 첨부 파일은 어떻게 보내야 하는?해답은?"

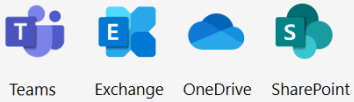
D 프로젝트

"회사와 개인생활이 분리된 메신저를 사용하고 싶다"
"협업 중인 파트너사와의 커뮤니케이션 부분에

우리는 아래와 같은 해답을 제시합니다.

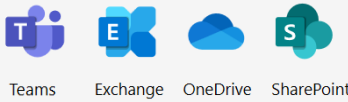
300인 이하 기업을 위한 Microsoft 365 제품

Microsoft 365 Business Basic



$6 per user/month[1]

Microsoft 365 Business Standard

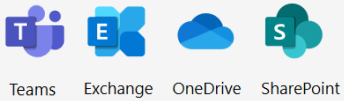


Desktop Apps

$12.50 per user/month[1]

Microsoft 365 Business Premium

Cloud Services

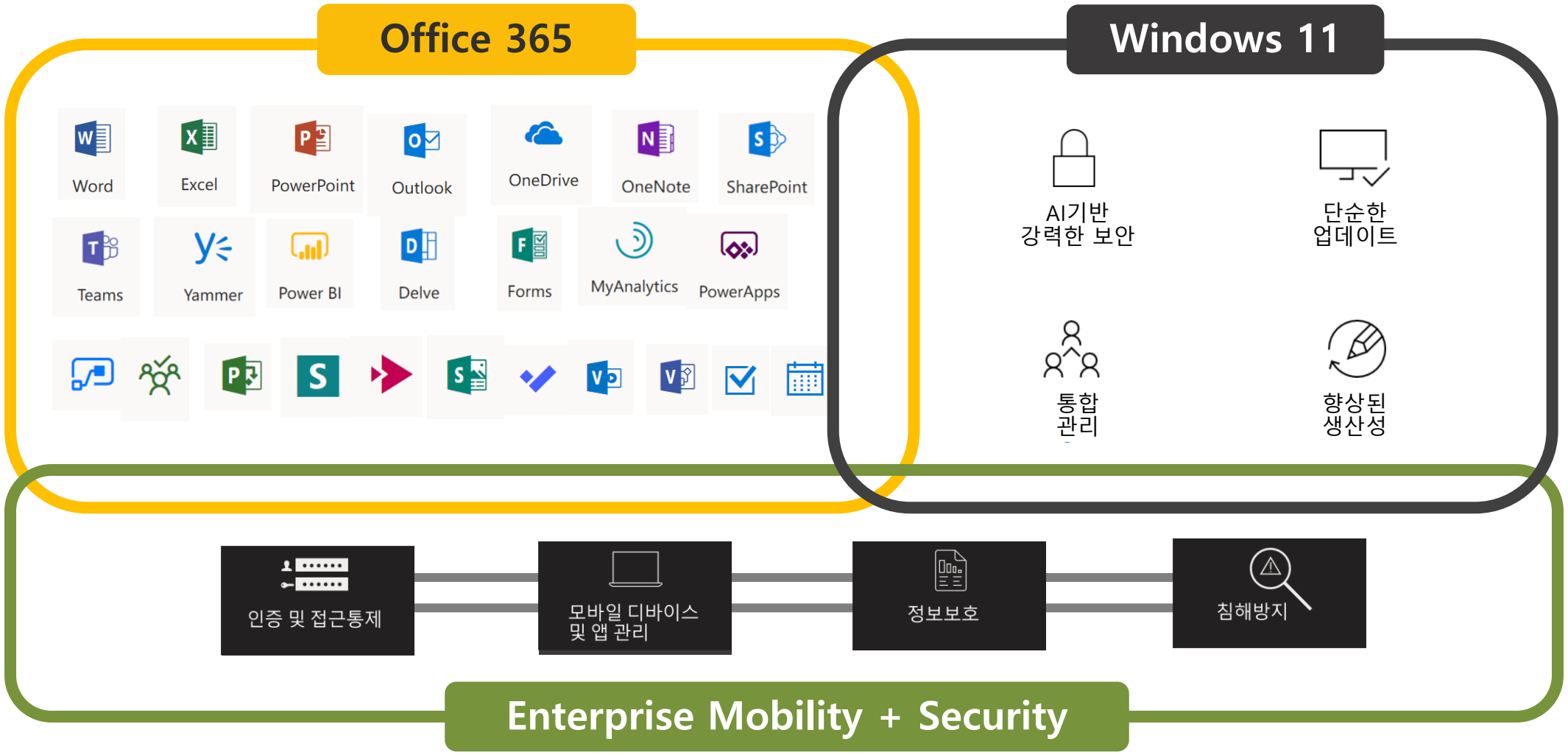


Desktop Apps

Comprehensive Security

$22 per user/month[1]

Microsoft 365 Business Premium



어디서나 비즈니스를 안전하게 운영

Microsoft 365 Business Standard (Office apps and services, Teams) $12.50[1]

+

Microsoft Defender for Business

Microsoft Defender for Office P1

Intune

Azure AD Premium Plan 1

Azure Information Protection Premium P1

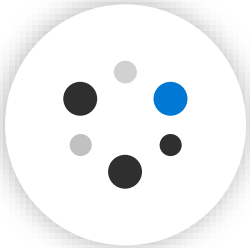
Device Antivirus

Autopilot

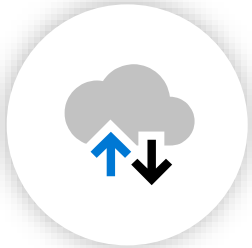
Windows Virtual Desktop license

Windows Upgrade rights

Microsoft 365 Business Premium
$22/사용자/월[1]



실시간 협업, 공동작업



업무용 앱에 대한 보안 액세스 활성화

사이버 위협 및 데이터 손실로 부터 보호

회사 소유 및 개인 장치를 안전하게 보호

어디서나 비즈니스를 안전하게 운영

Microsoft 365 Premium

How To

How To Work?

- 여러 위치에서 일하는 직원

보안을 어떻게 유지할 수 있나요?

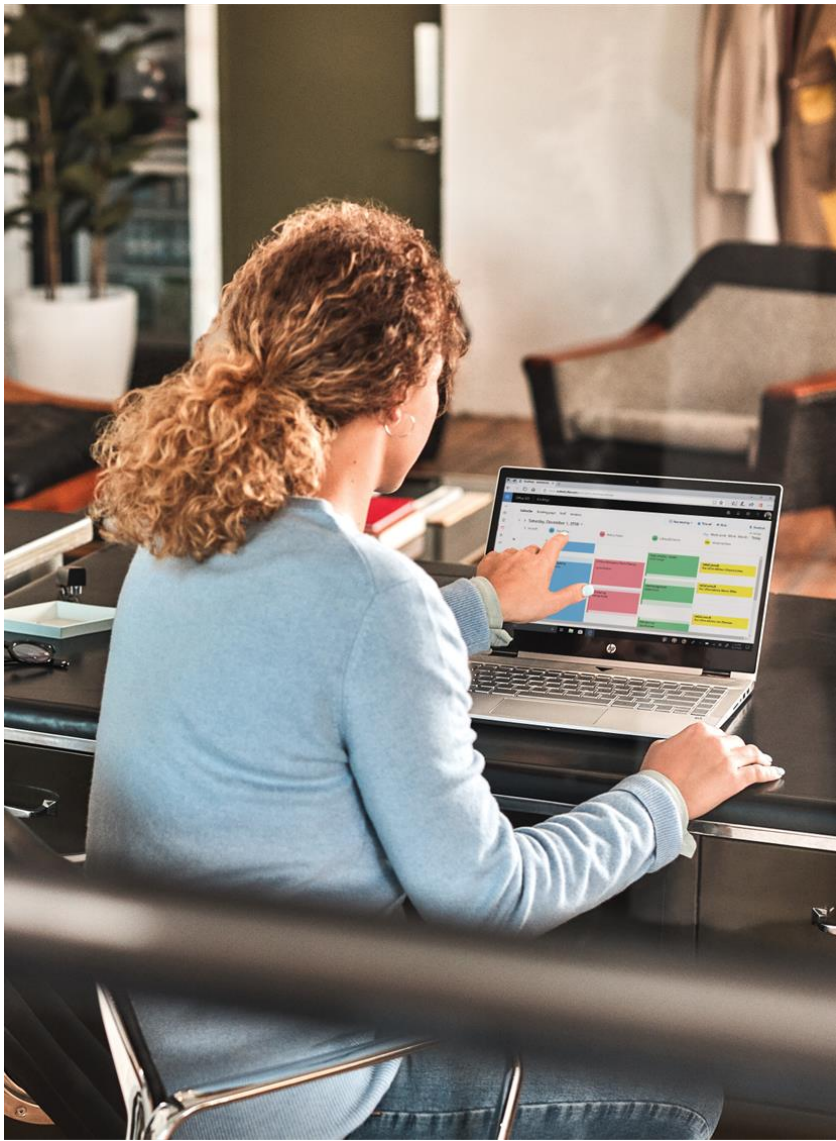
- 다양한 개인 및 모바일 장치

비용을 어떻게 줄일 수 있나요?

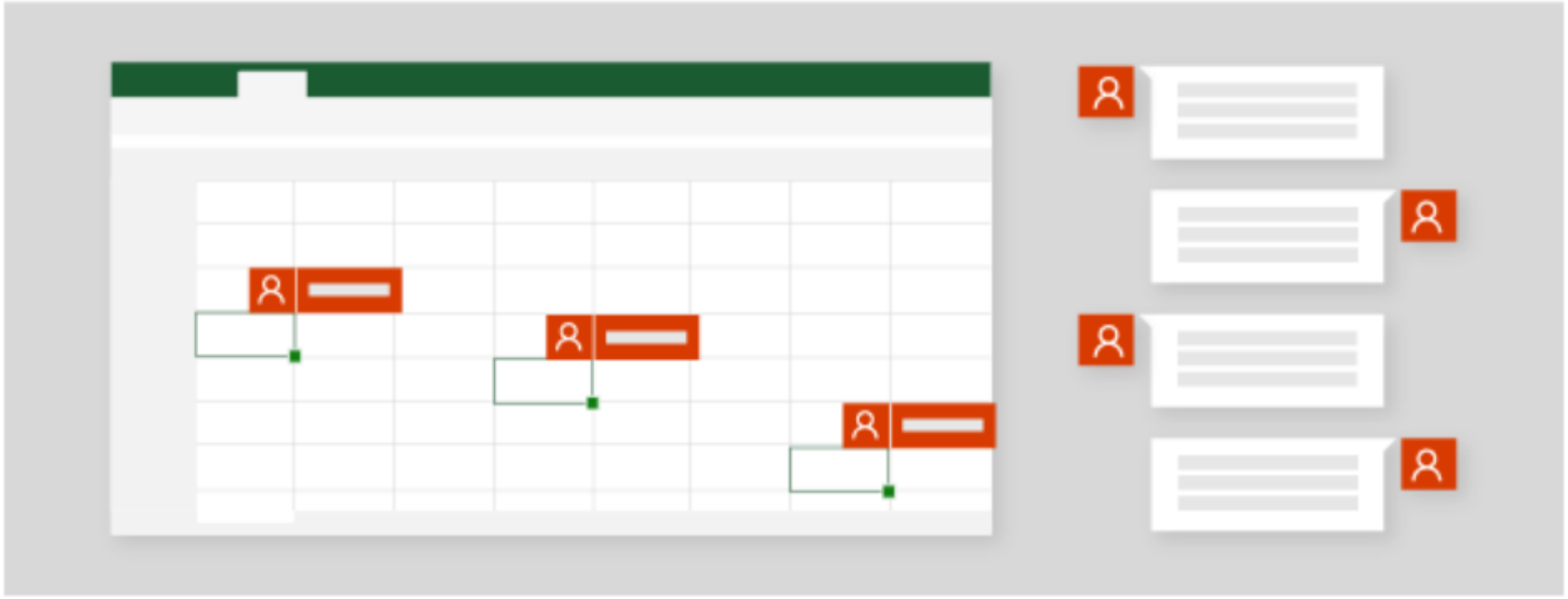
- 피싱 및 랜섬웨어 증가

2. 협업 시나리오 업무 혁신

“ 팀워크 방식의 업무 시나리오는 How To”



문서 협업, 문서 공동 편집

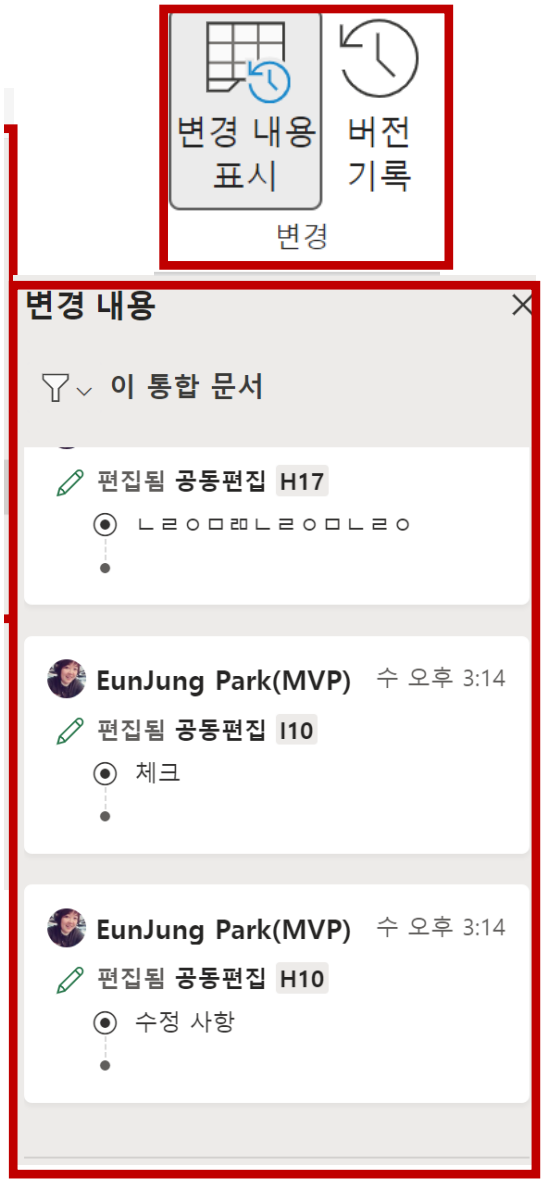


OneDrive

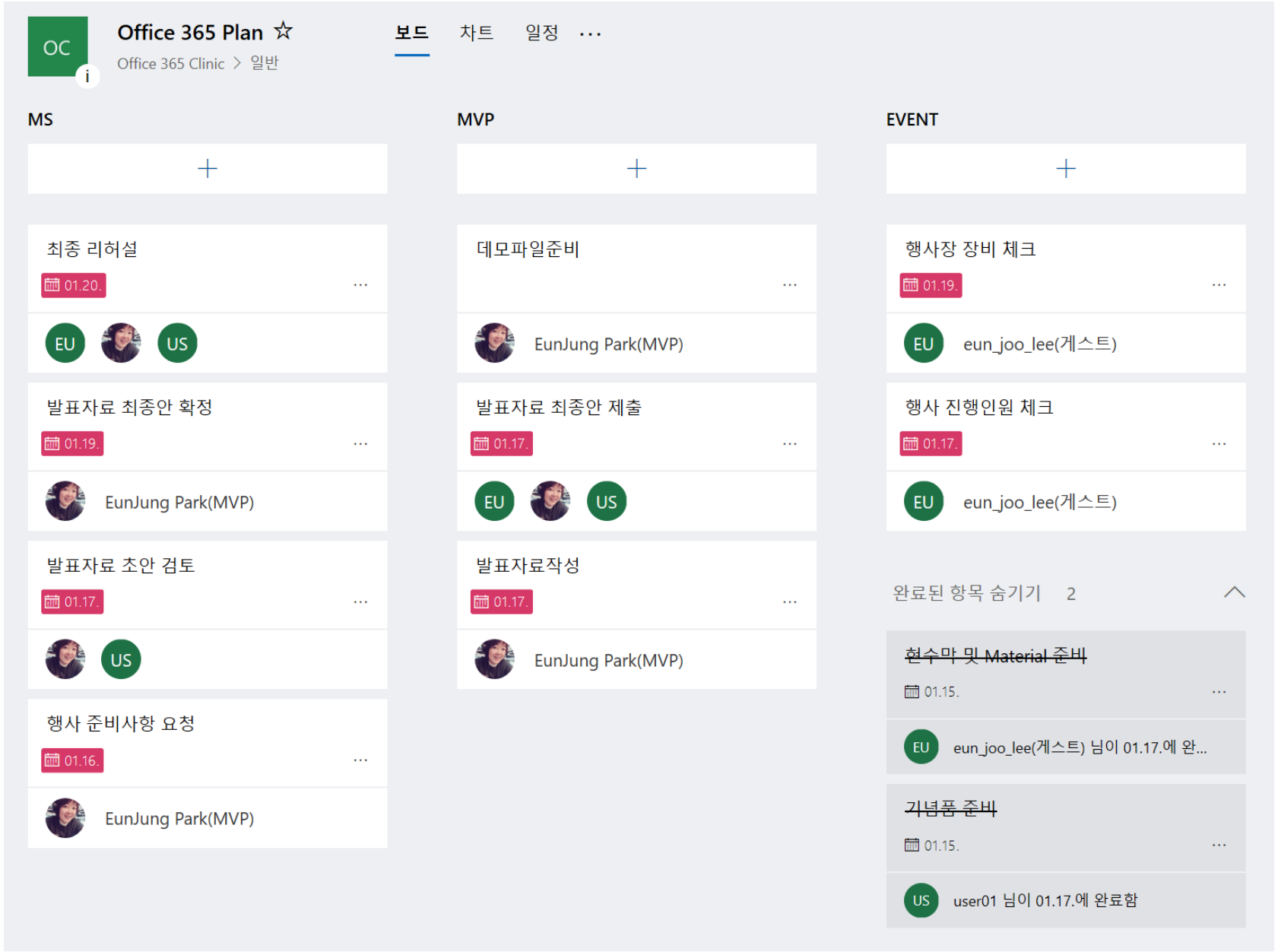
SharePoint

문서 협업, 문서 공동 편집

- Requirements.Final.docx
- Requirements.FinalFinal.docx
- Requirements.ThisIsReallyFinal.docx
- Requirements.v1.docx
- Requirements.v2.docx
- Requirements.v3.docx



프로젝트 진행률 및 하나의 화면에서 산출물 공유..

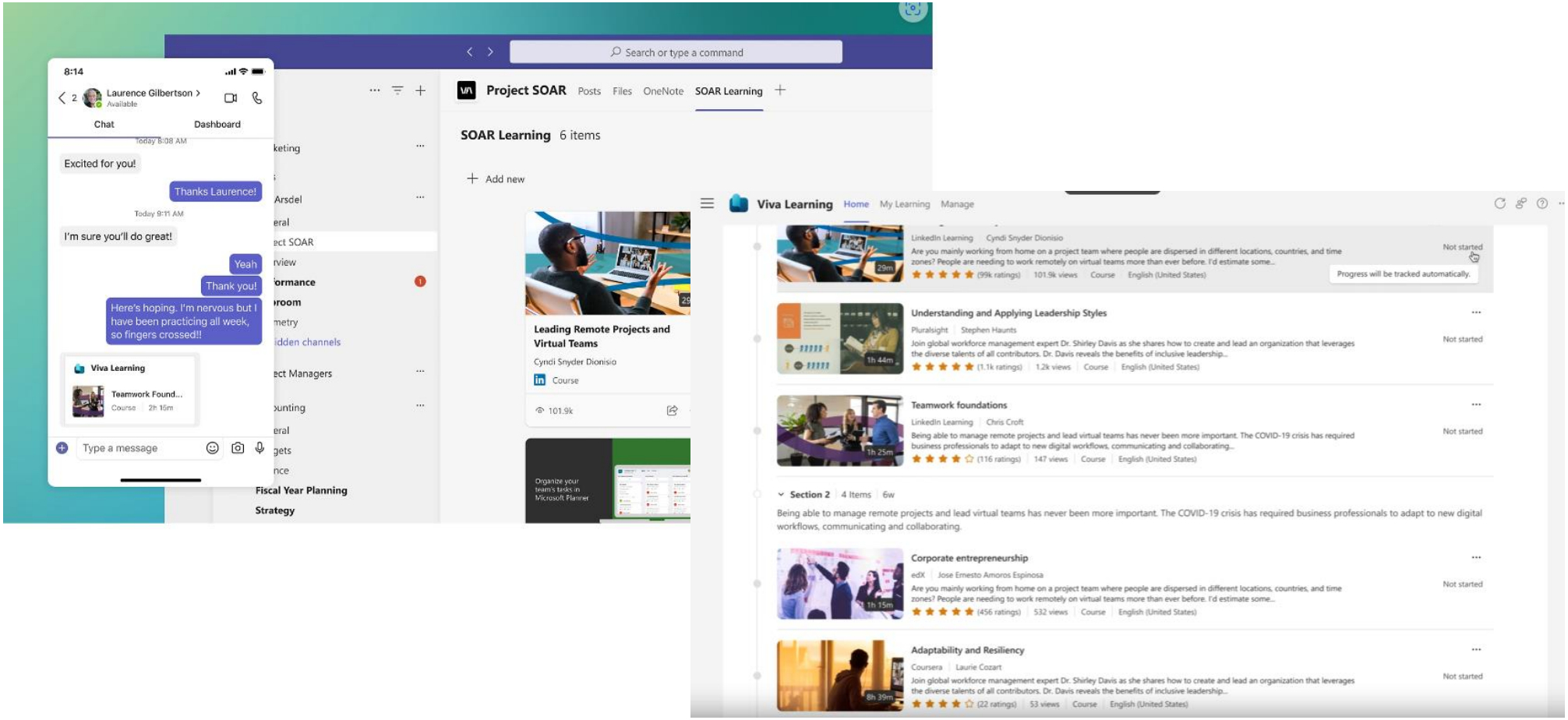


업무에 필요한 여러가지 시나리오 프로세스 자동화

Question

우리가 업무를 하면서 엑셀을 활용하여 데이터를 계산하고 엑셀 워크시트의 데이터 값을 다른 엑셀로 복사하는 업무를 합니다.
엑셀을 자동화 할 수 있는 작업 기능은 어떤 부분이 있을까요? 또한 엑셀1 시트의 값을 복사 하여 다른 엑셀 워크시트에 붙여 넣는 작업을 자동화 가능할까요?
인터넷 검색을 통해 시청률 등에 대한 순위표를 엑셀로 저장 가능할까요? 또한 메일로 보내는 흐름 생성도 가능할까요? 사용중인 Invoice App을 실행하여 송장 정보를 입력하는 활동을 자동화, 그리고 레코더 기능을 이용하여 녹화하여 자동화!!

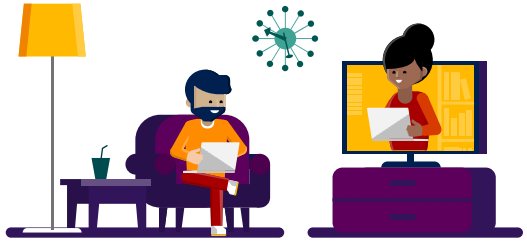
지속가능, 언제 어디서나 활용가능한 역량 강화 방안



동료, 고객, 파트너와 협업

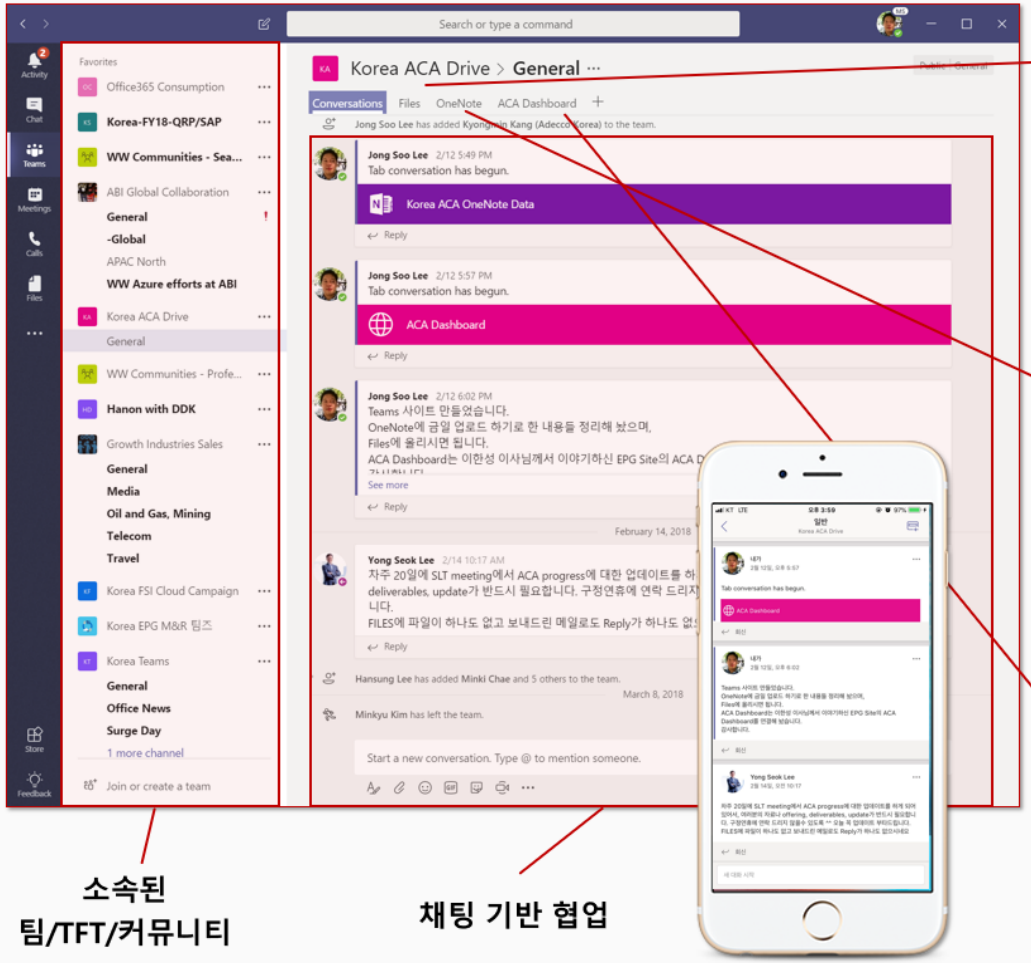
실시간 팀워크

어디에서나 미팅,업무 참여

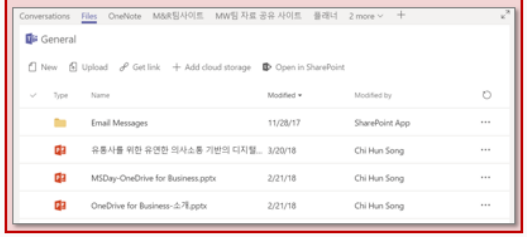


원활한 외부 협업

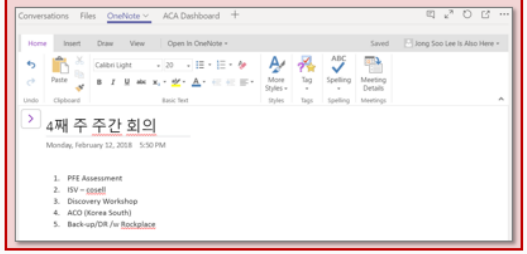
동료, 고객, 파트너와 협업



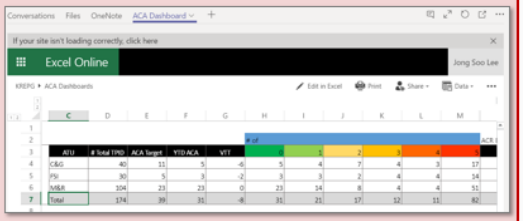
관련 파일/문서



회의록 등 공동작업 문서



필요에 따른 추가 (대쉬보드/일정/웹페이지)



기업을 위한 기능

- PC / 모바일 (안드로이드, iOS) 지원
- 다국어 지원 (한글/중국어 포함 19개 언어)
- 보안 (디바이스 / 컨텐츠 보안)
- 검색 / 컨텐츠 연계

손쉬운 연계/확장

- BI / 분석
- 영업관리(CRM), 고객관리
- R&D 등을 위한 개발툴
- 뉴스 / 소셜
- 프로젝트 관리

"한곳에서 대화,콘텐츠,앱을 사용,업무능률을 높이는 채팅 기반의 디지털 허브"

보안은 중소기업의 주요과제

+300%

지난해 랜섬웨어 공격, 50% 이상이 중소기업을 표적으로 삼았습니다

1 in 4

중소기업 4곳 중 거의 1곳이 작년에 보안 침해를 당했다고 밝혔습니다

70%

중소기업의 70% 이상이 사이버 위협이 점점 더 비즈니스 위험으로 변하고 있다고 생각합니다

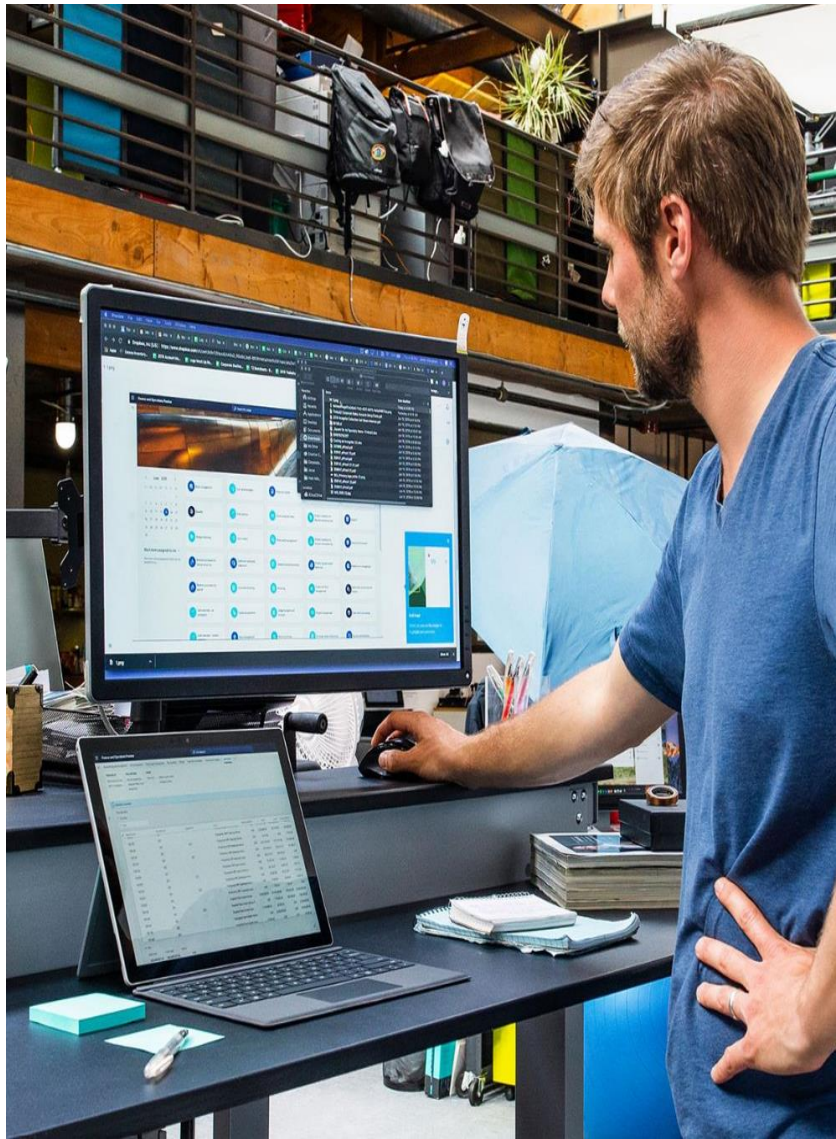
90%

중소기업은 적합한 사이버 보안 솔루션을 제공한다면 새로운 MSP 고용을 고려할 것입니다

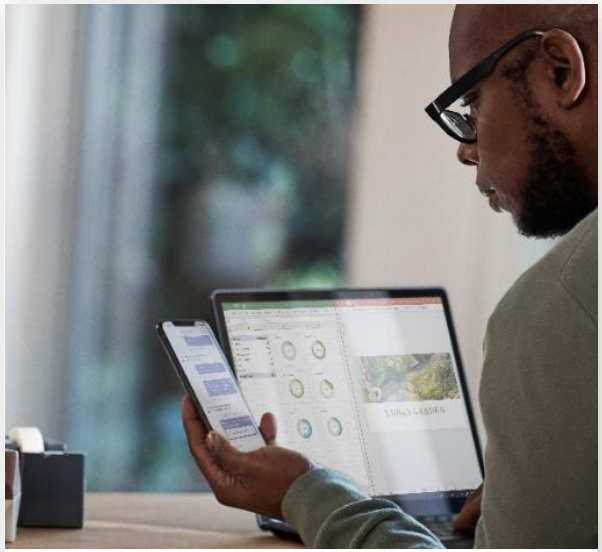
1. Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report
2. Microsoft commissioned research, April 2019, US SMBs 1-300 employees

보안 시나리오로 알아보는 업무 혁신

ID 및 액세스 제어 How To



MFA를 통해 비밀번호 분실 또는 도난 방지



우리는 광범위한 다단계 인증 옵션을 지원합니다.

비밀번호 없는 기술 포함

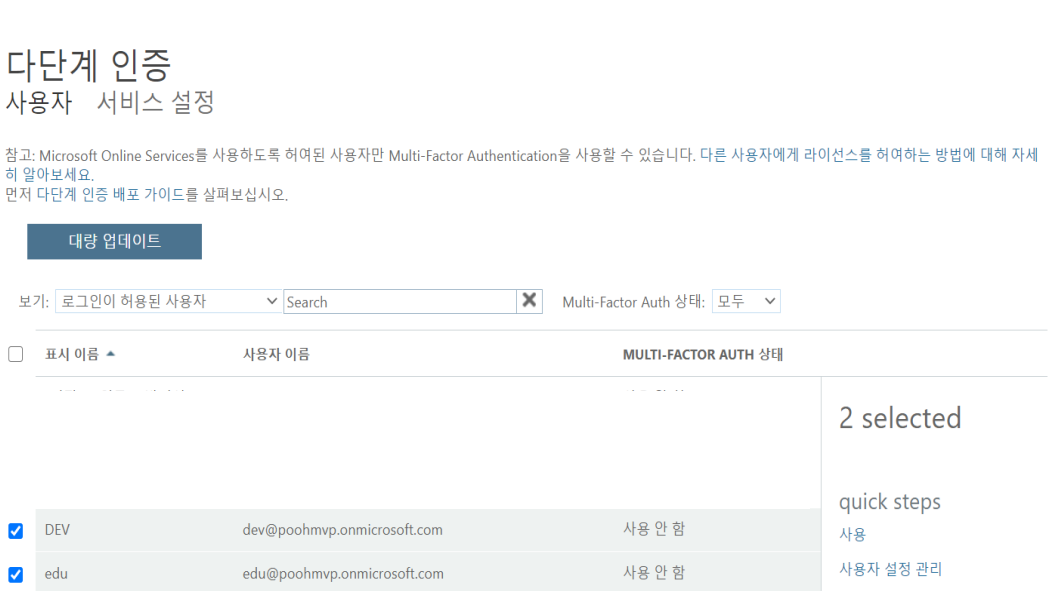
- Microsoft Authenticator
- Windows Hello
- FIDO2 security key
- Biometrics

- Push notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, voice

다단계 인증은 **ID** 공격의 **99.9%**를 방지합니다.

MFA를 통해 비밀번호 분실 또는 도난 방지

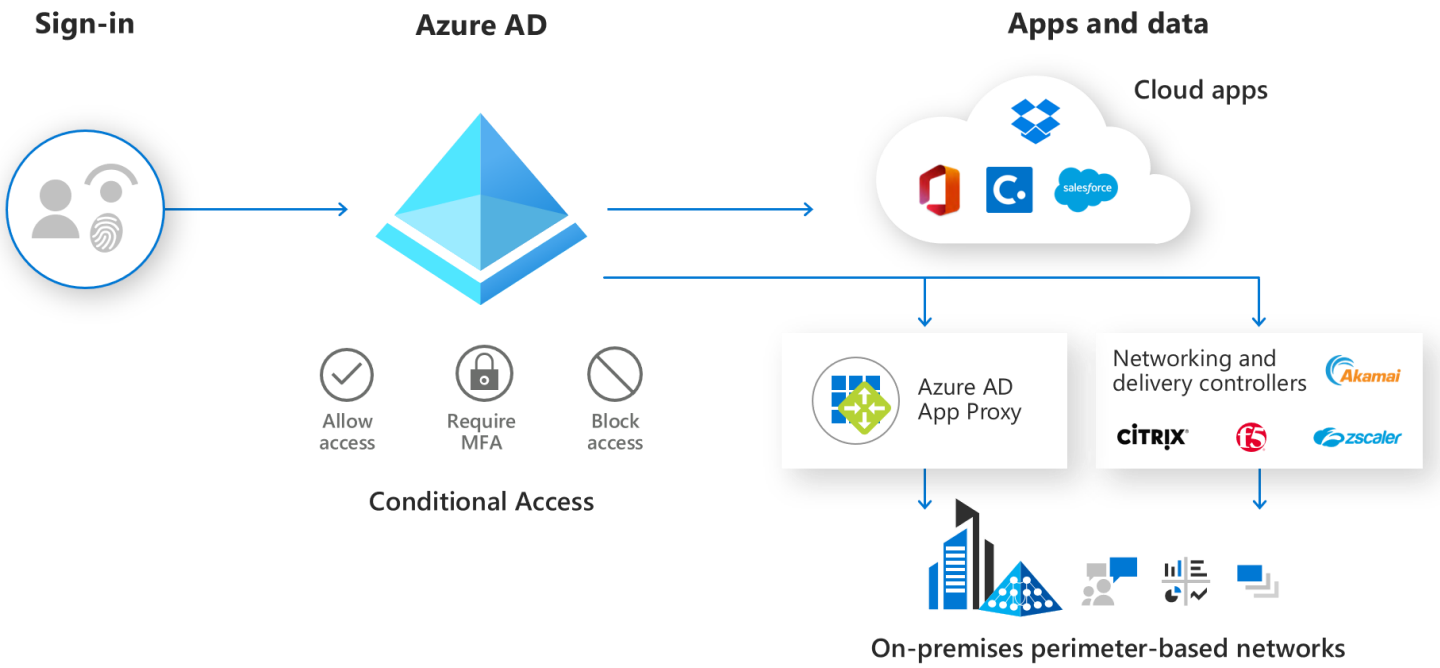
- 인증방법 - 모바일 앱을 통한 일람, 모바일 앱 또는 하드웨어 토큰의 확인, 휴대폰에 문자메시지 전송, 휴대폰에 전화 걸기



참고!Microsoft 365 Business, E3 또는 E5 -> 기본 MFA 인증 사용
Azure AD 조건부 액세스(Azure AD Premium P1)
위험 기반 조건부 액세스(Azure AD Premium P2)

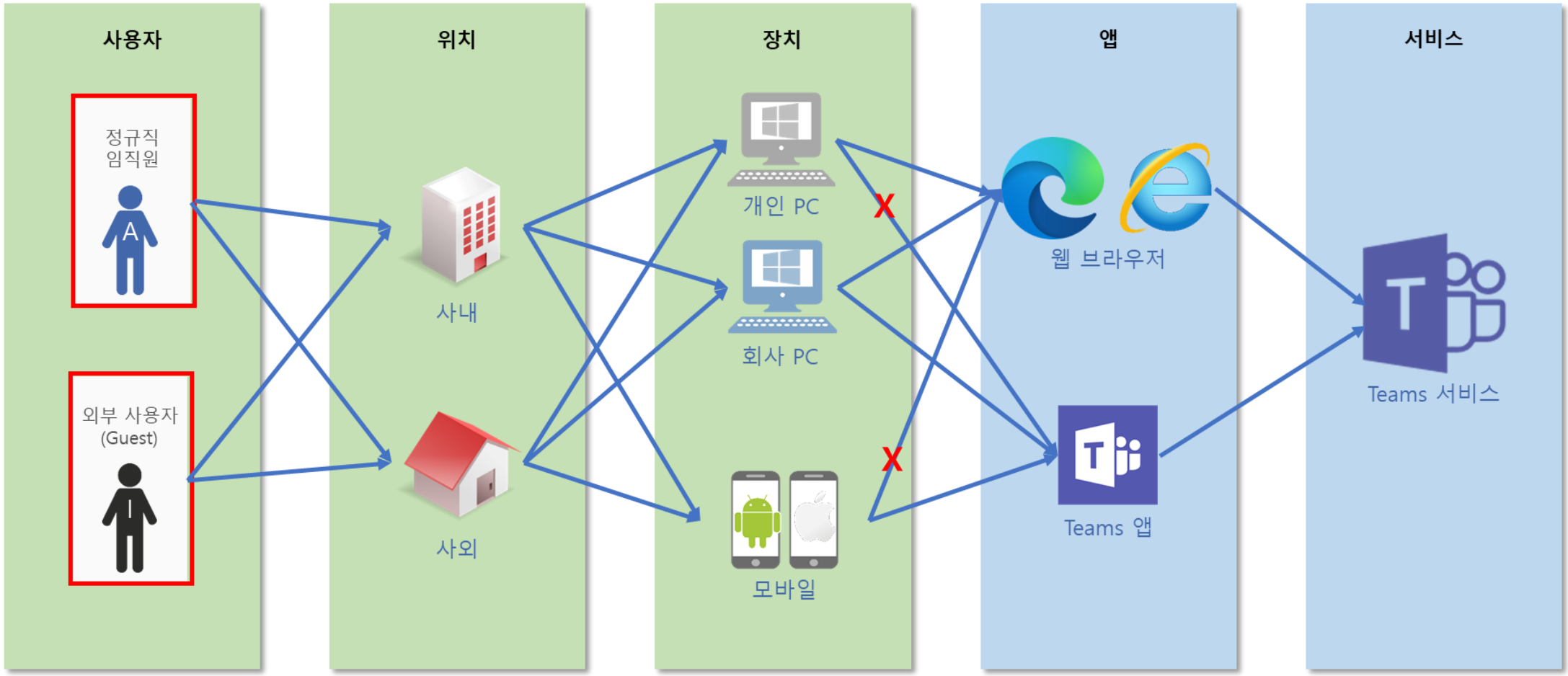
Entra ID를 사용하여 업무용 앱에 안전하게 액세스

- 앱 프록시를 사용하면 직원들이 네트워크에 대한 광범위한 액세스를 열지 않고도 온프레미스 앱에 원격으로 액세스할 수 있습니다
- 조건부 액세스를 사용하여 "어디에서, 언제, 누가" Office 앱에 연결하는지 제어
- 보안 그룹에 사용자를 자동으로 추가/제거하고 동적 그룹을 통해 IT 오버헤드를 줄입니다.



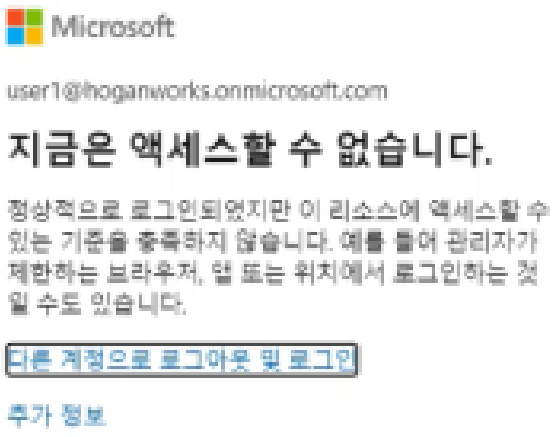
How To – 접근 제어- Teams 모든 구성원

- 사용자에 대한 Teams 접근 제어 예시



How To : MFA

How To : 조건부 액세스



인증 구성에 따른 권장 수준

부적절: 암호

123456

qwerty

password

iloveyou

Password1

양호: 암호
기타...

sms

음성

적절: 암호
기타...

Microsoft Authenticator

소프트웨어
토큰 OTP

하드웨어 토큰 OTP
(미리 보기)

최적: 암호 없음

Windows Hello

Microsoft Authenticator
(미리 보기)

FIDO2 보안 키
(미리 보기)

셀프서비스 암호 재설정(SSPR)

✓ Enter 관리센터 SSPR(셀프 서비스 암호 재설정)은
관리자나 지원 센터의 관여 없이도 사용자가 암호를 변경하거나
재설정 할 수 있는 기능을 제공합니다.
✓ 사용자의 계정이 잠겨 있거나 암호를 잊어 버린 경우 프롬프트를 따라
스스로 차단 해제하고 작업으로 돌아 갈 수 있습니다.

사용자가 디바이스 또는 애플리케이션에 로그인 할 수 없을 때
지원 센터 호출 및 생산성을 줄입니다.

How To : SSPR
셀프서비스 암호 재설정

엠클라우드브리지 Multi CLOUD BRIDGE

위험 보고서

Microsoft Entra 관리 센터 | 리소스, 서비스 및 문서 검색(G+/) | eunjung@M365x48165... CONTOSO

홈 > Identity Protection

Identity Protection | 위험한 로그인

검색

- 대시보드(미리 보기)
- 개요
- 자습서
- 문제 진단 및 해결

보호

- 사용자 위험 정책
- 로그인 위험 정책
- 다단계 인증 등록 정책

보고서

- 위험한 사용자
- 위험한 워크로드 ID
- 위험한 로그인
- 위험 검색

설정

- 위험에 처한 사용자가 알림을 감지했습니다.
- 주 단위 요약
- 설정

문제 해결 및 지원

- 문제 해결
- 새 지원 요청

다운로드 | 자세한 정보 | 데이터 내보내기 설정 | 신뢰할 수 있는 IP 구성 | 문제 해결 | 모두 선택 | 로그인을 손상됨으로 확인 | 로그인 보안 확인 | 새로 고침

자동 위험 수정을 허용하시겠습니까? 조건부 액세스에서 위험 정책을 설정하세요. 자세히 알아보기 →

자동 새로 고침 : **끄기** | 날짜 : **지난 7일** | 날짜 표시 형식 : **로컬** | 위험 상태 : **2이(가) 선택됨** | 위험 수준(실시간) : **선택된 항목 없음** | 위험 수준(집계) : **선택된 항목 없음** | 검색 유형 : **선택된 항목 없음** | 로그인 유형 : **2이(가) 선택됨** | 필터 추가

날짜 ↑↓	사용자 ↑↓	IP 주소	위치	위험 상태 ↑↓

결과가 없습니다.

사용자에게는 로그인 활동과 연결되지 않은 탐지가 있을 수도 있습니다. 모든 탐지를 보려면 위험 탐지로 이동하세요.

Check: 위험한 활동

엠클라우드브리지
Multi CLOUD BRIDGE

Microsoft 365 Business Premium 기능으로 계정 보안을 구성하여 로그인할 때 암호 외에 추가적인 인증 요소를 통하거나 신뢰할 수 있는 국가, 위치 및 디바이스를 등록하여 비밀번호가 유출되더라도 계정이나 기업 데이터를 보호할 수 있는 계정 보안 환경을 구축을 제공 합니다.

계정 보안 환경 확보

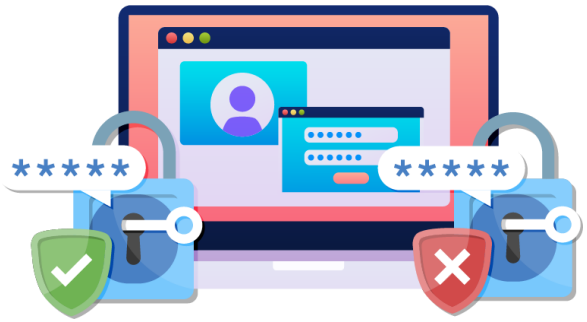
1차 인증(비밀번호)

- 사용자만 아는 지식 기반 인증
- 패스워드 길이, 복잡도 설정
- 세션 유휴시간 설정

다단계 인증(MFA)

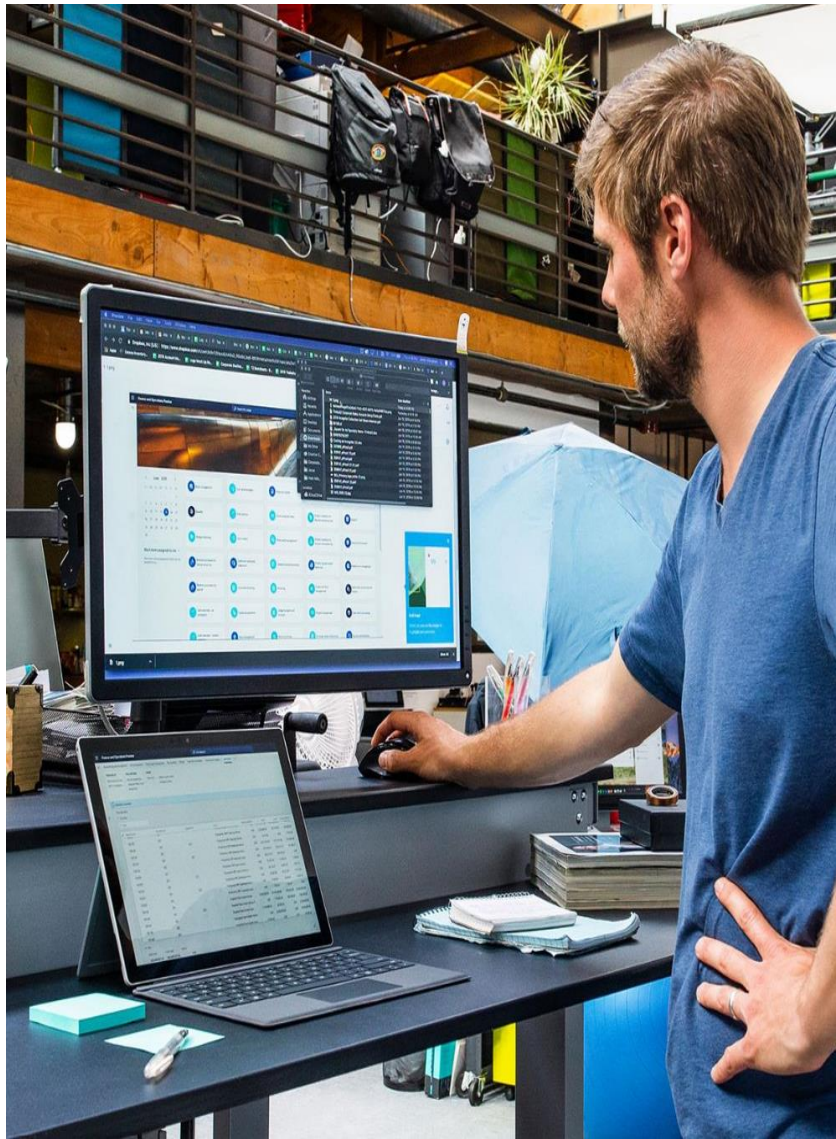
- 사용자가 소유한 소유기반 인증
- 문자 메시지, 앱 푸시, 토큰
- 필요에 따라 사용자 선별 적용

조건부 액세스

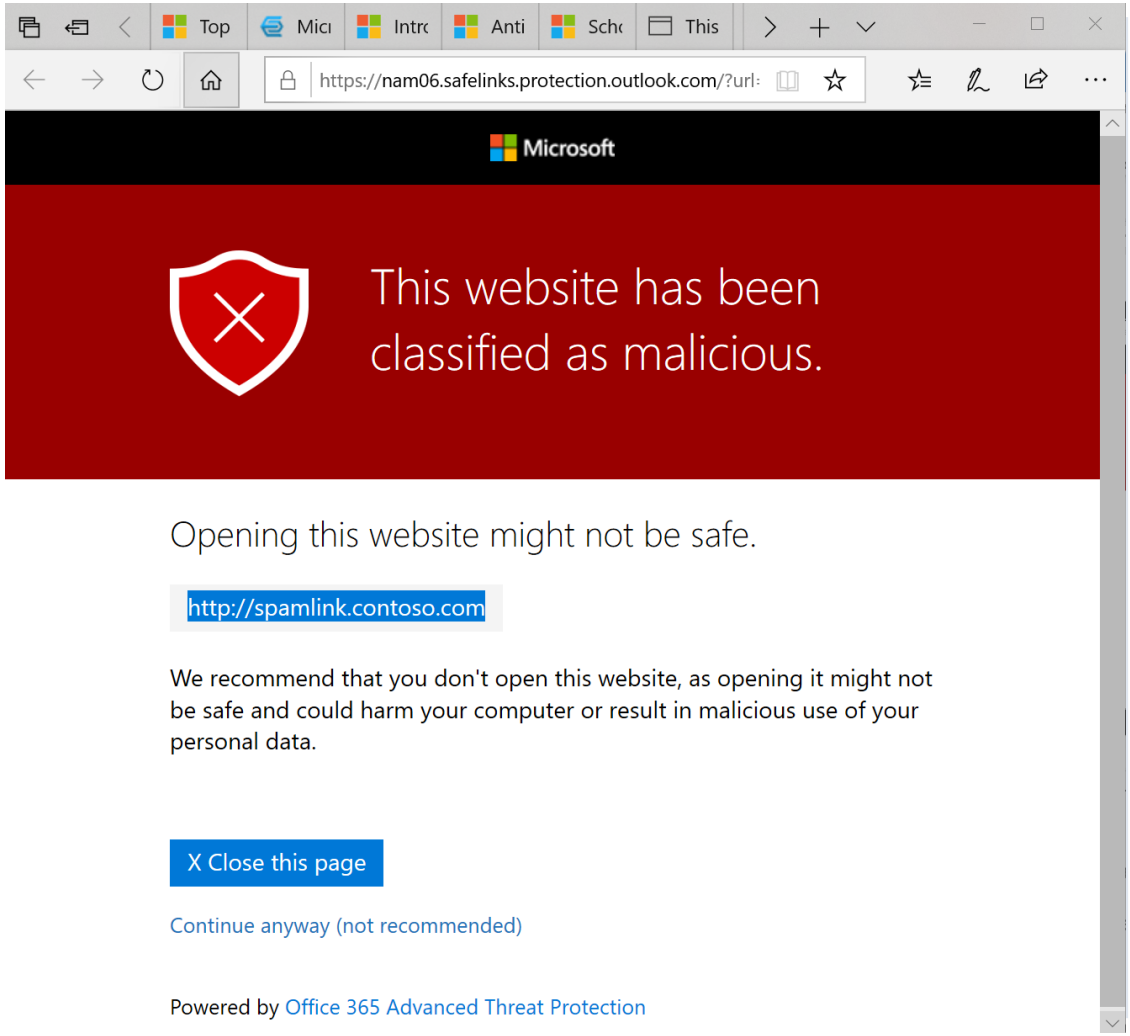


- 위치 기반 액세스로 사용자 보안 향상
- 장치 규정 준수 기반 액세스 제어
- 앱 기반 액세스 제어

클라우드 컨텐츠 보안 How To(1)



안전한 링크, 안전한 첨부파일

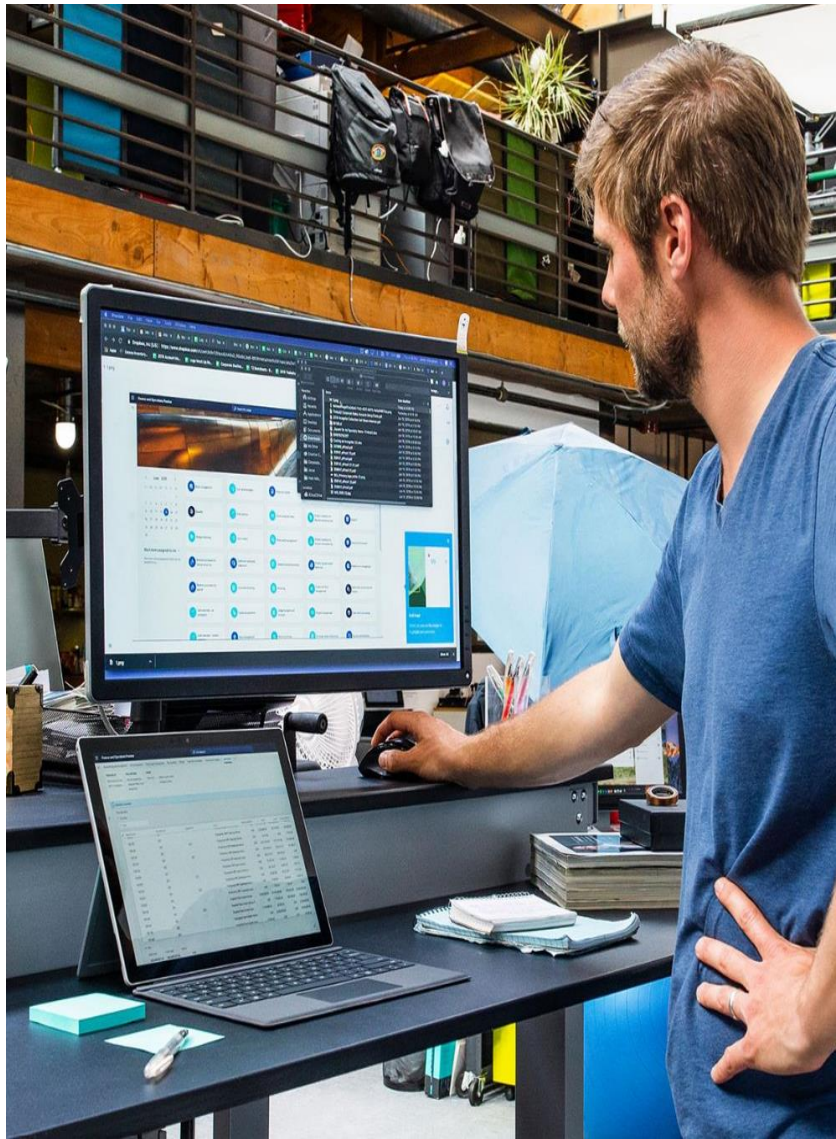


Office 365용 Microsoft Defender로 사이버 위협 보호

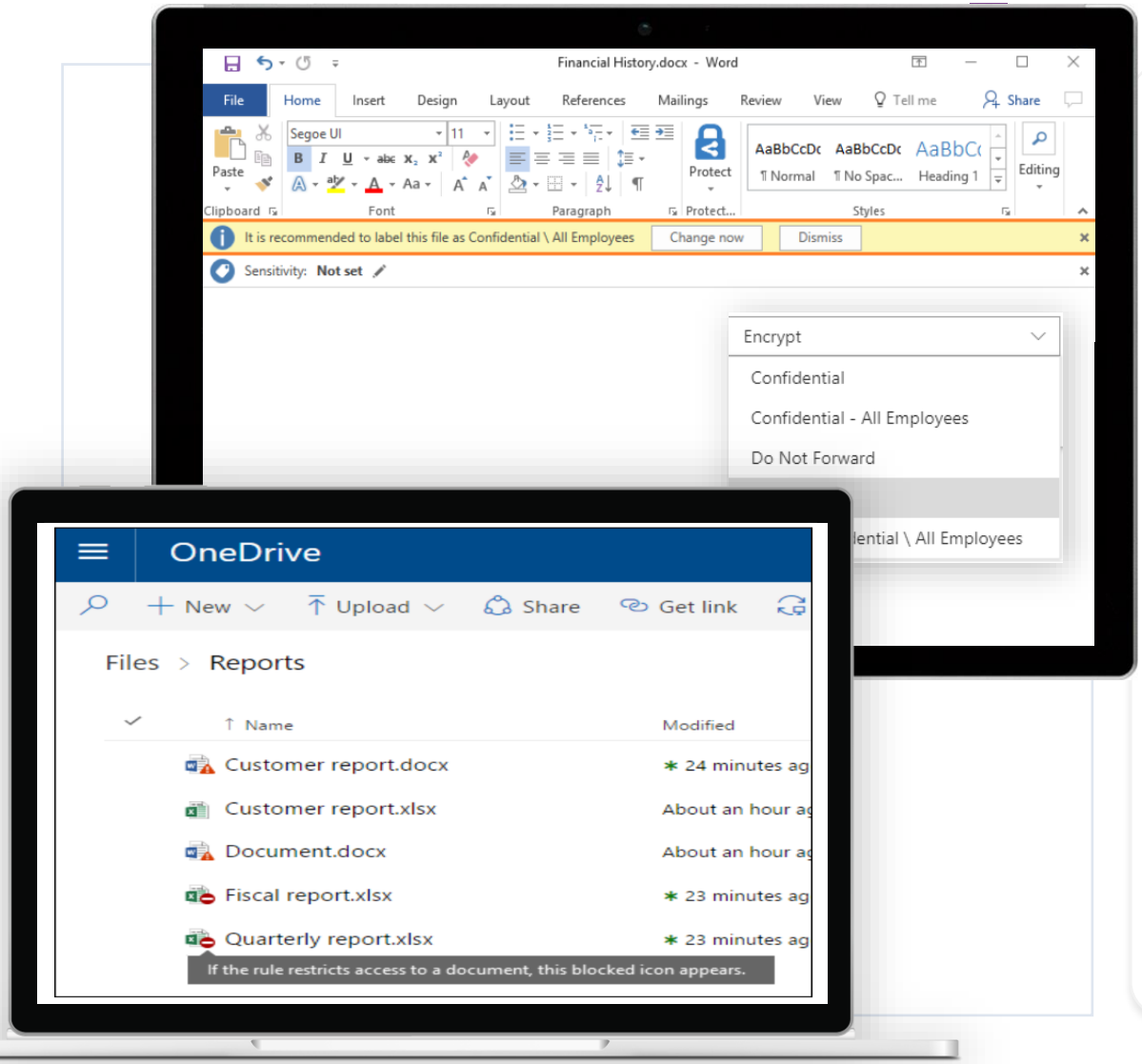
- Office 365용 Microsoft Defender 안전한 링크를 사용하여 실시간 검사를 통해 이메일 또는 Teams의 악성 링크로부터 보호
- 안전한 첨부 파일을 사용하여 Teams 및 OneDrive의 이메일 및 공유 문서 링크에 있는 첨부 파일에 대한 AI 기반 맬웨어 검사 가능
- 피싱 방지 기능으로 명의도용 및 스푸핑을 방지
- Microsoft Defender AV를 사용하여 랜섬웨어와 같은 의심스러운 프로세스로부터 Windows 장치를 더 효과적으로 보호

How To : 안전한링크

클라우드 컨텐츠 보안 How To(2)



DLP 및 AIP으로 데이터 보호



DLP 및 Azure Information Protection으로 데이터 보호

- HIPAA, PCI_DSS, SSN 등에 대해 사전 구성된 DLP 정책 템플릿을 사용하여 신용 카드 번호와 같은 민감한 정보의 공유를 방지
- 직원이 아닌 사람이 이메일을 전달, 인쇄 또는 볼 수 있는지 여부를 제어
- 직원이 아닌 사람이 문서를 편집, 인쇄 또는 볼 수 있는지 여부를 제어, 액세스를 취소할 수도 있습니다.

DLP 및 AIP으로 데이터 보호

데이터는 다양한 위치에서 생성되고, 가져오기 되고, 수정 됩니다.

데이터가 탐지 됨
디바이스, 클라우드 서비스, 온-프레미스

민감한 데이터는 분류 & 레이블링
민감도에 기반: 보호 정책 또는 보존 정책에 사용

데이터는 정책에 따라 보호 됨
보호는 암호화, 사용 권한, 시각적 표시, 보존, 삭제 또는 공유 차단과 같은 DLP 작업의 형태로 이루어질 수 있음

데이터는 다양한 위치에서 공유 됨
보호는 지속적이며, 데이터와 함께 이동

모니터링 되는 데이터
데이터 공유, 사용, 잠재적 남용에 대한 보고 및 조치 취하기 및 수정

데이터 보존, 만료, 삭제
데이터 거버넌스 정책 활용

DLP

Microsoft Teams	Exchange Online	SharePoint Online	OneDrive for Business	Office desktop apps
채팅 메시지 채널 대화	전송중인 이메일 이메일 본문 첨부파일 그룹 포함 또는 제외	크롤링할 수 있는 모든파일 Teams 에서 사용되는 파일 사이트 포함 또는 제외	SharePoint와 동일한 파일 형식 계정 포함 또는 제외	In-App 정책 팁 Word PowerPoint Excel Outlook

정책 팁
공유 방지
사용자 재정의
알림 메일

Teams DLP

- 사용자가 의도하지 않은 실수로 Teams의 대화나 채팅에서 고객이나 프로젝트의 기밀이 될 수 있는 중요한 정보를 대내/외적으로 공유하는 것을 방지

메시지 발신자

메시지 수신자

✓ Teams에서는 커뮤니케이션 DLP로 동작

✓ 파일이나 문서는 SharePoint/OneDrive의 DLP로 동작

How To : DLP(데이터손실방지)

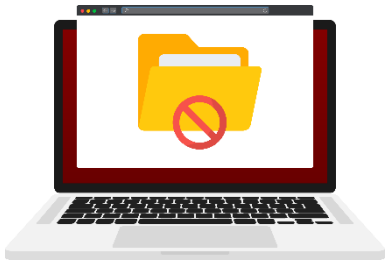
Microsoft 365 Business Premium 기능으로 데이터 보안을 구성하여 Microsoft 365 애플리케이션의 Office 파일, 메일 및 메시지를 자동으로 모니터링하고 데이터의 외부 유출을 차단할 수 있으며, 기업 맞춤형 환경 검증을 통해 강력한 보안 거버넌스 환경을 구축을 제공 합니다.

데이터 보안 환경 확보

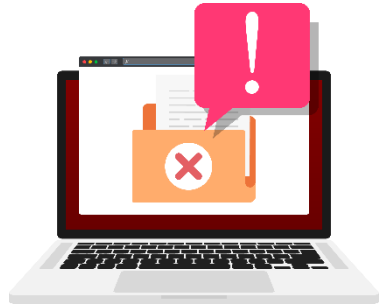
키워드 규칙 생성

의심스러운 행위 감지

전송 차단



관리자 알림



규칙 생성 및 검사

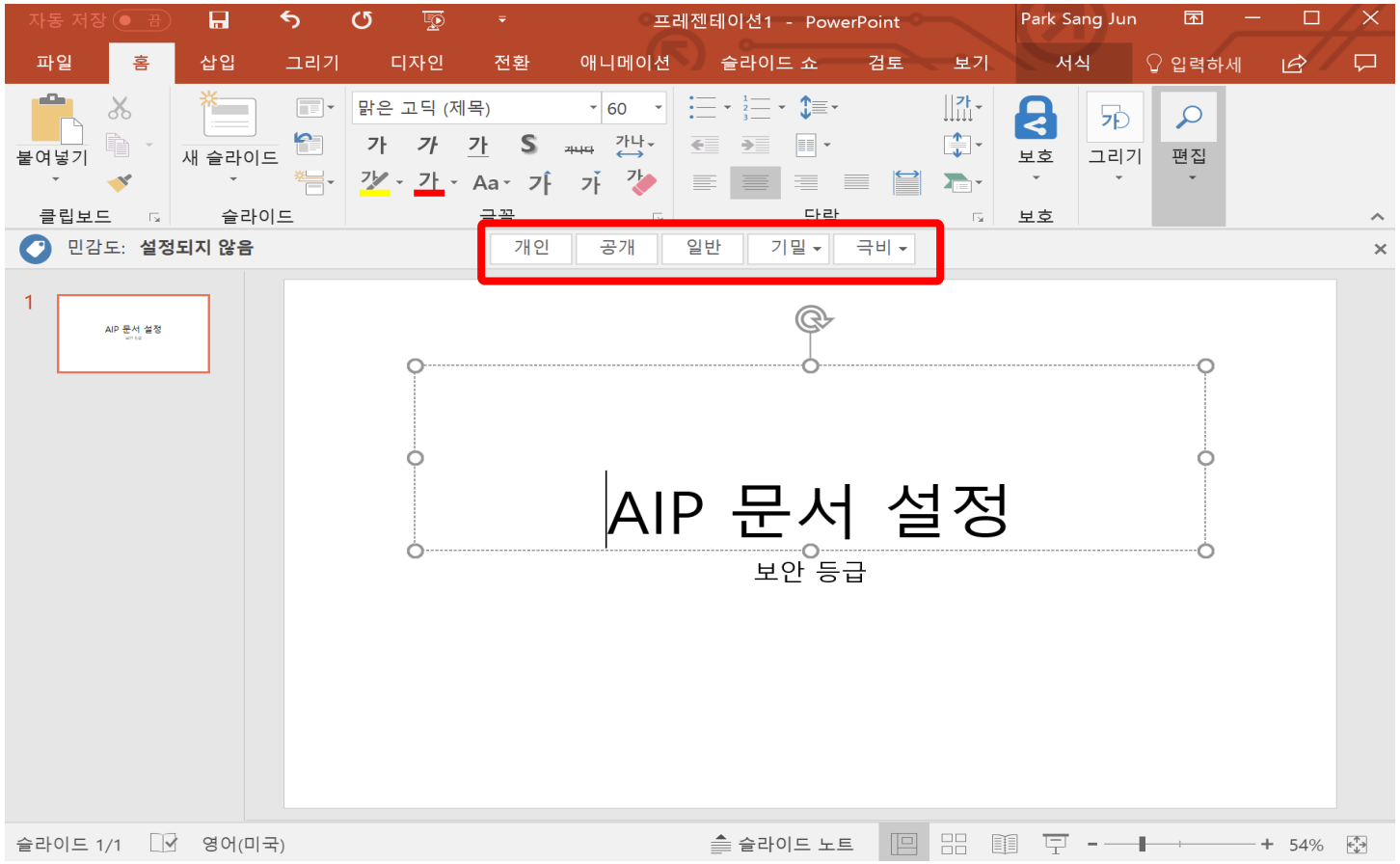
- 특정 부서, 역할, 사용자에 대해 규칙을 관리할 수 있습니다.
- 관리자는 데이터 손실 방지(DLP)를 사용하여 사용자가 사내 민감한 자료를 외부 사용자에게 보낼 수 없도록 설정합니다.
- 클라우드 드라이브에 저장된 민감한 데이터가 채팅, 메일, 문서 공유로 유출되는 경우를 항시 검사합니다.

작업 및 보고

- DLP 검사 단계에서 설정하였던 규칙의 행위가 감지되었을 경우 외부 발송을 차단합니다.
- 위반사항에 대한 내용을 관리자에게 알립니다.
- 사고 관리 대시보드를 통하여 보고서 형태로 위반된 행위를 검토할 수 있습니다.

수 많은 중요 문서 및 계약서 유출 걱정 No

- AIP 기능을 활용하여 문서에 대한 유출 걱정 No



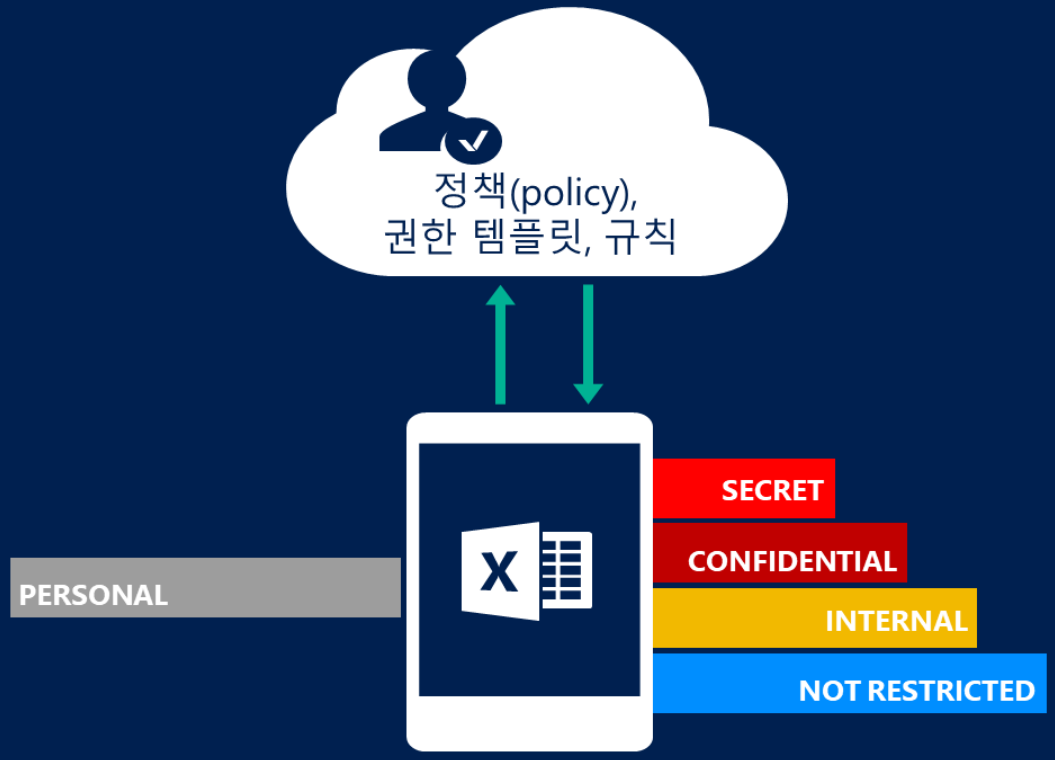
AIP를 통한 외부 사용자와 안전한 문서 공유와 협업

- AIP(Azure Information Protection)는 문서분류 및 워터마크, 문서 암호화 및 권한설정 등을 통해 기업의 기밀 정보와 중요한 데이터의 무단 사용으로부터 정보 보호가 가능하며 외부 유통된 문서/정보에 대한 추적과 권한 회수가 가능합니다.

AIP문서 분류 정책

- 문서분류 정책(Policy), 권한 템플릿 및 규칙 등을 설정하여 중요 문서에 대한 유출 위협으로부터 능동적으로 대처할 수 있습니다.

문서의 중요도 및 보안 등급에 따른 분류



- 정책(Policy)에 따른 자동 문서 분류 및 강제 암호화 (Automatic)
- 문서 분류를 위한 시스템에 의한 사용자에게 권장 (Recommended)
- 사용자 지정 (User set)

AIP문서 분류 정책

- 암호화된 데이터는 누가(인증), 무엇을(권한), 언제까지(제어) 사용할 수 있도록 안전하게 공유할 수 있습니다.

AIP 암호화된 데이터의 권한 설정

누가

무엇을

언제까지

보유권한	사용자 A	사용자 B	사용자 C
열람	O	O	O
편집	O	X	X
보존	O	X	X
복사/붙여넣기	O	X	X
인쇄	X	X	X
기한	-	12/31	10/25

AIP 추적 및 권한 회수

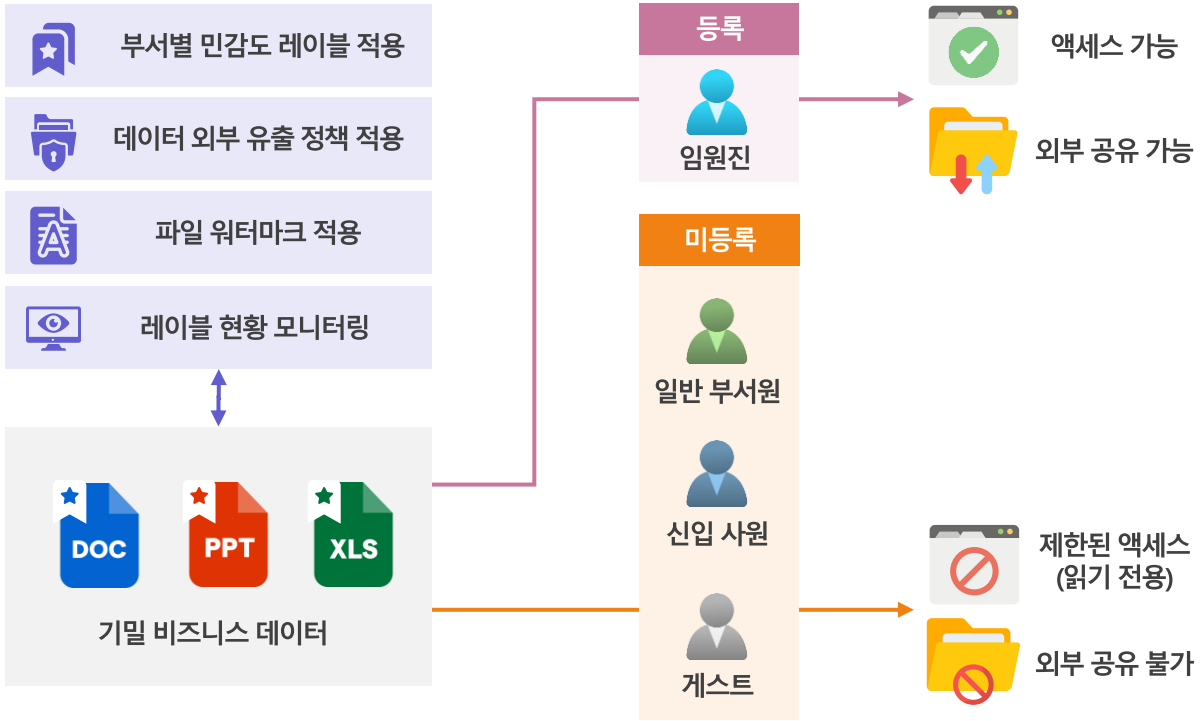
- 시작은 넓고 단순하게, 소규모 그룹 단위로 단계별 적용, 빠르게 다음으로

1. 분류	간단한 단계를 수행, 큰 영향을 줄 수 있음 (ie.인사부와 법무부에 '전달 금지' 옵션 사용)
2. 자동화	테스트, 단계별 배포, 그리고 피드백 – IT 는 모두 알지 못함
3. 보호	모든 PC/디바이스에 걸쳐 민감한 내부 이메일 흐름 통제 (Exchange Online, Office 365 Message Encryption)
4. 외부 공유	파트너(B2B)와 '보호된 문서 파일' 공유
5. 모니터	권한 회수에 대한 사용자 교육과 사용 활성화함

How To : 워터마크

데이터 보안 기능으로 민감도 레이블을 활용하여 부서, 사용자 별로 중요 레이블을 적용하고 미등록 된 사용자에게는 중요 레이블이 적용된 파일의 액세스가 제한할 수 있으며 메일, 메시지 등의 외부 공유가 일제히 차단되어 중요한 파일 데이터의 외부 유출을 보호합니다.

민감도 레이블



데이터 보안의 시나리오

임원진만 기밀 데이터에 액세스할 수 있도록 민감도 레이블을 적용하여 타 부서, 신입 사원 및 게스트로부터 비즈니스 데이터를 보호합니다.

등록 된 부서

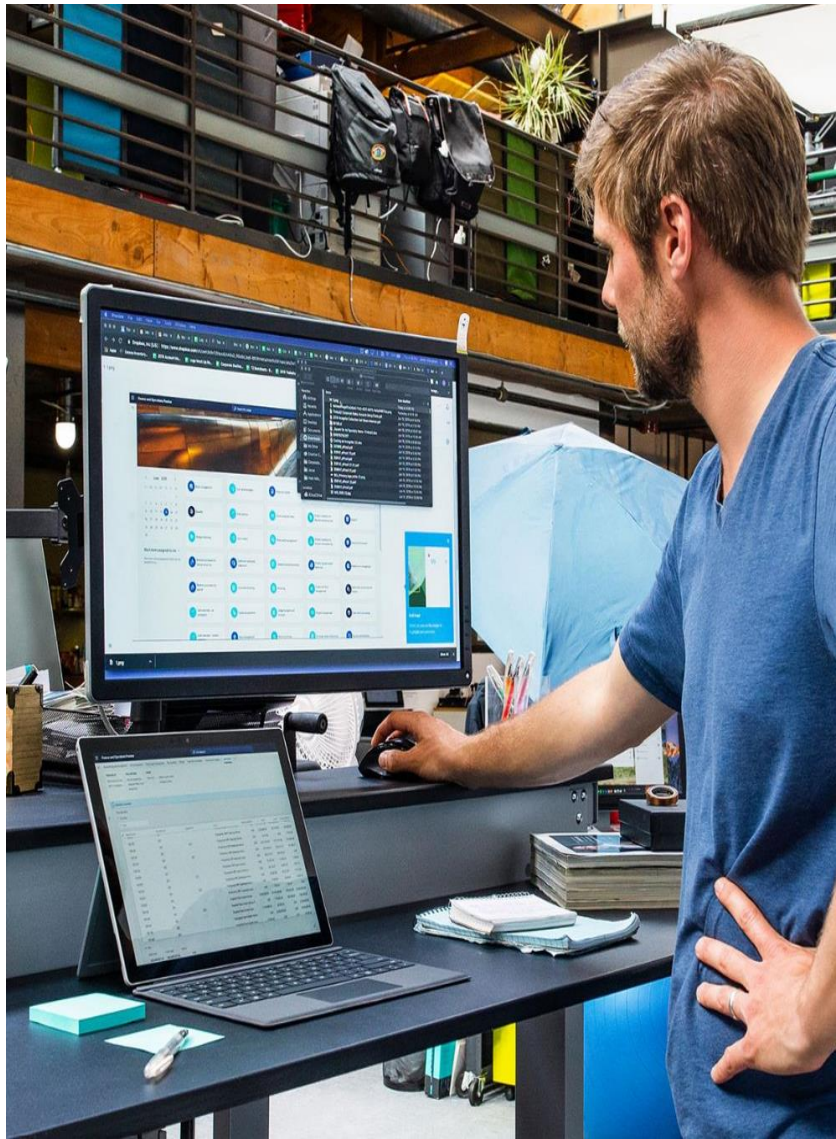
① 파일을 읽거나 쓰기 할 수 있습니다.
② 파일 외부 공유가 가능합니다.

미등록 된 부서

① 제한된 액세스(읽기만 가능)만 가능합니다.
② 파일 외부 공유가 제한됩니다.

Endpoint 보안 How To

보안 정책을 통한 회사 관리 앱과 개인 관리 앱을 분리



Intune을 사용하여 모바일 장치에서 데이터 관리

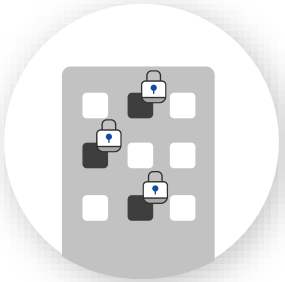
모바일 장치 관리(MDM)

조건부 액세스:
회사 소유 기기에 대한 액세스를 관리합니다.

- 관리용 기기 등록
- 설정, 인증서, 프로필 프로비저닝
- 장치 규정 준수 보고 및 측정
- 원격으로 장치에서 회사 데이터 제거

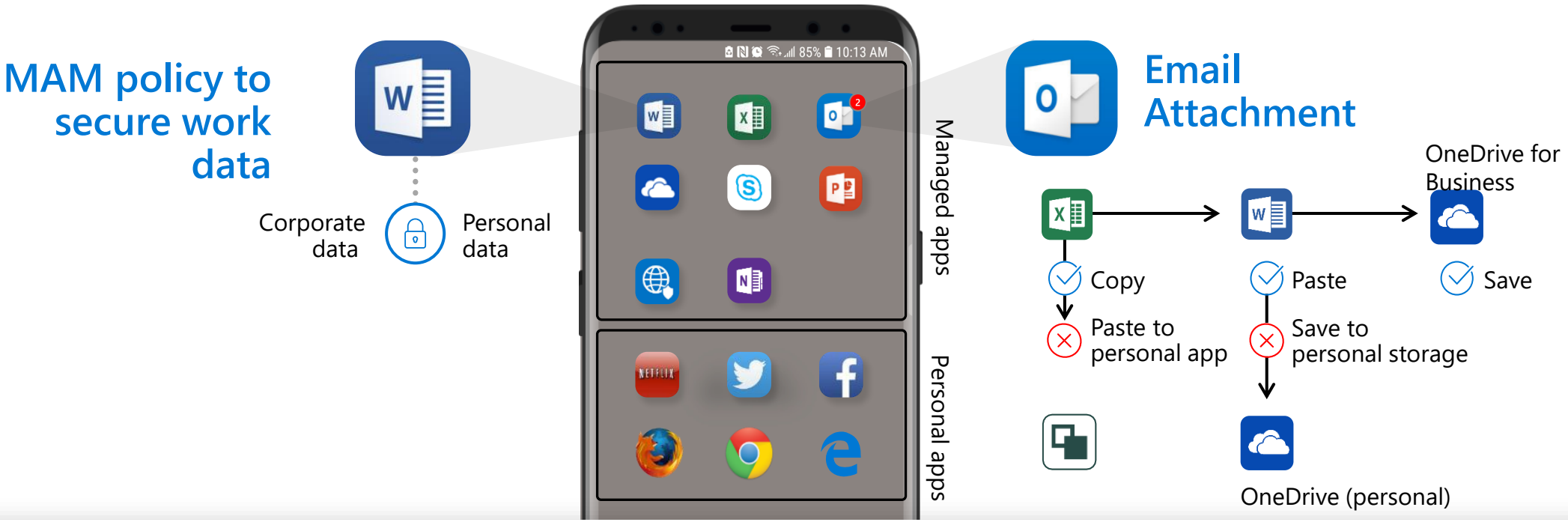
모바일 애플리케이션 관리(MAM)

조건부 액세스:
개인 장치의 업무 이메일이나 파일에 액세스하는 데 사용할 수 있는 앱 관리



- 사용자에게 모바일 앱 게시
- 구성 및 앱 업데이트
- 업무 데이터를 개인 앱에 저장할 수 없도록 시행
- 모바일 앱 내 기업 데이터 보호 및 제거

개인 기이에서 업무 데이터 관리하기



AIP(Azure Information Protection)를 사용하면 업무 데이터에 대한 액세스 제어를 지정할 수 있습니다.

회사 관리 앱을 개인 앱과 분리하고 관리 앱에서 업무 데이터에 액세스하는 방법에 대한 정책을 설정하세요.

Intune 앱은 회사 데이터를 장치 내의 개인 앱에 복사하여 붙여넣을 수 없도록 보장합니다.

How To : 앱 보호 정책

Microsoft 365 Business Premium 기능으로 디바이스 보안을 구성하여 디바이스 사용을 제한하고 보안 정책을 중앙 관리센터에서 관리, 배포 및 감시할 수 있으며 사용자의 디바이스가 정책을 준수하는지 식별하여 엄격하게 보안 관리할 수 있는 환경 구축을 제공 합니다.

디바이스 보안 환경 확보

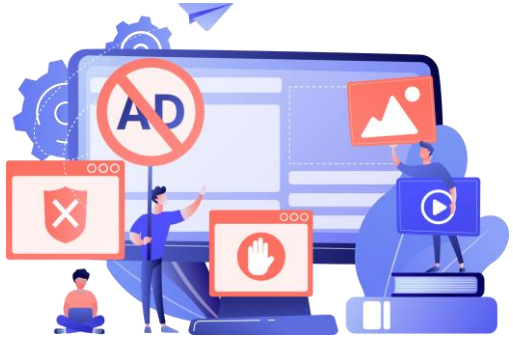
디바이스 보안 관리

- 기기 데이터 삭제, 사용자 계정 로그아웃
- Windows 10 자동 업데이트 지원
- 랜섬웨어, 맬웨어 보안 강화 설정

중앙 관리센터 감시

- 회사 디바이스 규정 준수 식별
- 디바이스 이벤트 로그 분석
- 보안 위협에 해당되는 의심스러운 행위 감시

디바이스 설정 제한



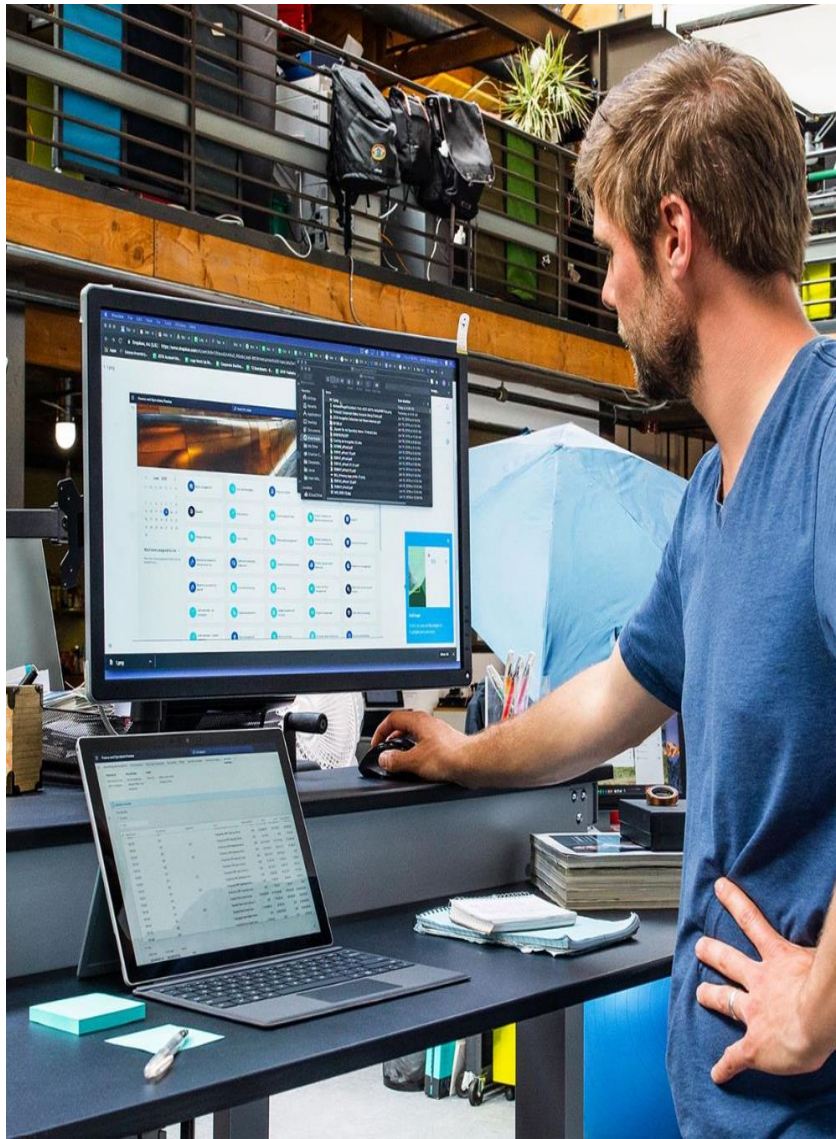
- 사용자 디바이스 애플리케이션 배포
- 카메라, USB 및 제어판 접근 차단
- 네트워크 환경 제한

사용자 장치의 관리를 최소화하고 중앙 관리센터에서 의심스러운 행위를 보안, 감시

보안 시나리오로 알아보는 업무 혁신

Endpoint 보안 How To

비즈니스용 Microsoft Defender



비즈니스용 Microsoft Defender

보안 강화

최대 **300**명의 직원을 보유한 기업을 위해 특별히 설계된 기기 보호입니다.

엔터프라이즈급 보호

엔드포인트 탐지 및 대응, 위협 및 취약성 관리와 같은 업계 최고의 Defender 기술을 사용하여 랜섬웨어 및 기타 사이버 위협으로부터 장치를 보호하세요.

사용하기 쉬운

간편한 마법사 기반 온보딩을 통해 빠르게 시작하고 실행하세요. 즉시 사용 가능한 정책과 자동화된 조사 및 해결 기능을 통해 최신 위협으로부터 자동으로 보호할 수 있으므로 비즈니스 운영에 집중할 수 있습니다.

비용 효율적

Microsoft 365 Business Premium의 일부로 또는 독립 실행형 솔루션으로 두 가지 유연한 계획으로 제공됩니다. 사용자당 월 3달러로 사용자당 최대 5개의 장치를 보호하세요..

Microsoft Defender for Business now generally available: https://aka.ms/DefenderforBusiness
Microsoft Defender for Business servers add-on now generally available: https://aka.ms/MDB-TechblogNov22

.

비즈니스용 Microsoft Defender

이제 비즈니스용 **Microsoft Defender**가 **Business Premium**에 포함됩니다.

Microsoft Defender Business ($3pupm)[1]

Enterprise-grade endpoint security

Per user license

- ✓ 차세대 보호
- ✓ Cross-Platform support iOS, Android, Windows, MacOS)2
- ✓ 엔드포인트 탐지 및 대응
- ✓ 위협 및 취약점 관리
- ✓ ...그리고 더

Microsoft 365 Business Premium ($22pupm)[1]

포괄적인 생산성 및 보안 솔루션

Per user license

Microsoft 365 Business Standard ($12.50)[1]
Office apps and services, Teams

+

Microsoft Defender for Business

Microsoft Defender for Office 365 Plan 1

Intune

Azure AD Premium Plan 1

Azure Information Protection Premium P1

Exchange Online Archiving

Autopilot

Azure Virtual Desktop license

Windows 10/11 Business

Shared Computer Activation

Licensing Options

1. 독립형 **SKU**로 최대 **300**명의 사용자
   - 최대 **5**개의 장치에서 사용할 수 있는 권한

1. **Microsoft 365 Business Premium**의 일부로 포함되며 최대 **300**명의 사용자가 사용할 수 있습니다.

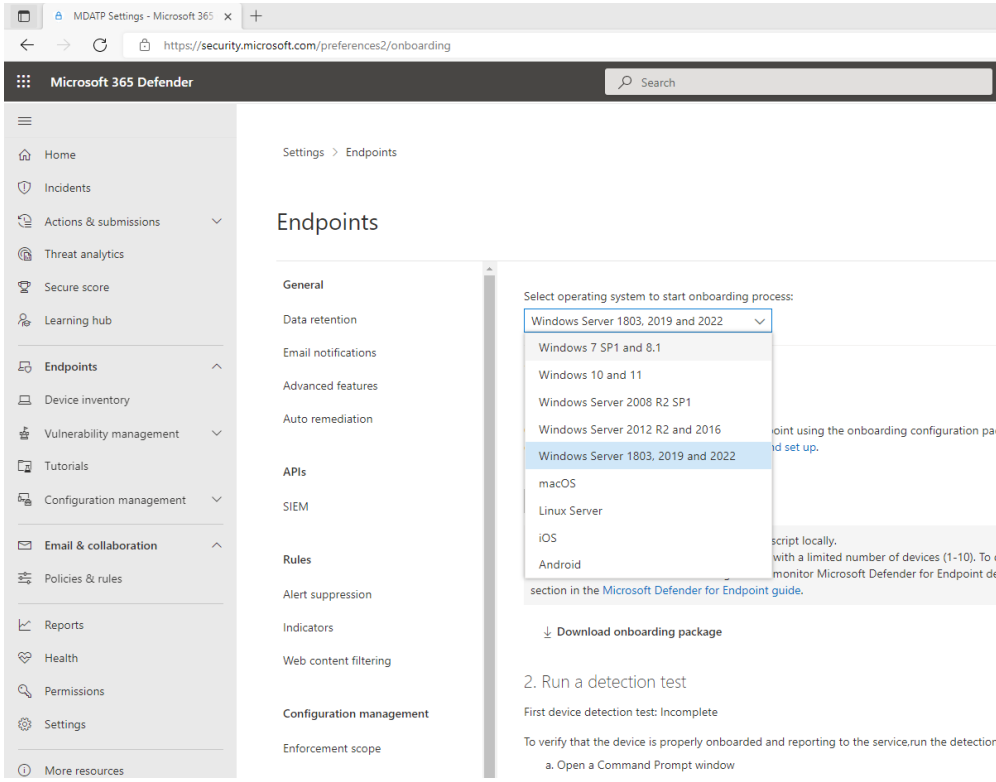
2. 이제 **Add-on** 제품을 사용할 수 있습니다.

비즈니스용 Microsoft Defender

비즈니스용 **Defender** 서버 추가 기능을 새로 사용할 수 있음

Defender for Business 또는 **Microsoft 365 Business Premium***에 대한 추가 기능 **Windows** 및 **Linux** 서버 보호

- 단일 관리 환경으로 클라이언트와 서버 모두에 대해 동일한 보호를 제공합니다.
- Microsoft 365 Lighthouse 통합을 통한 다중 고객 관리
- $3 서버 인스턴스당



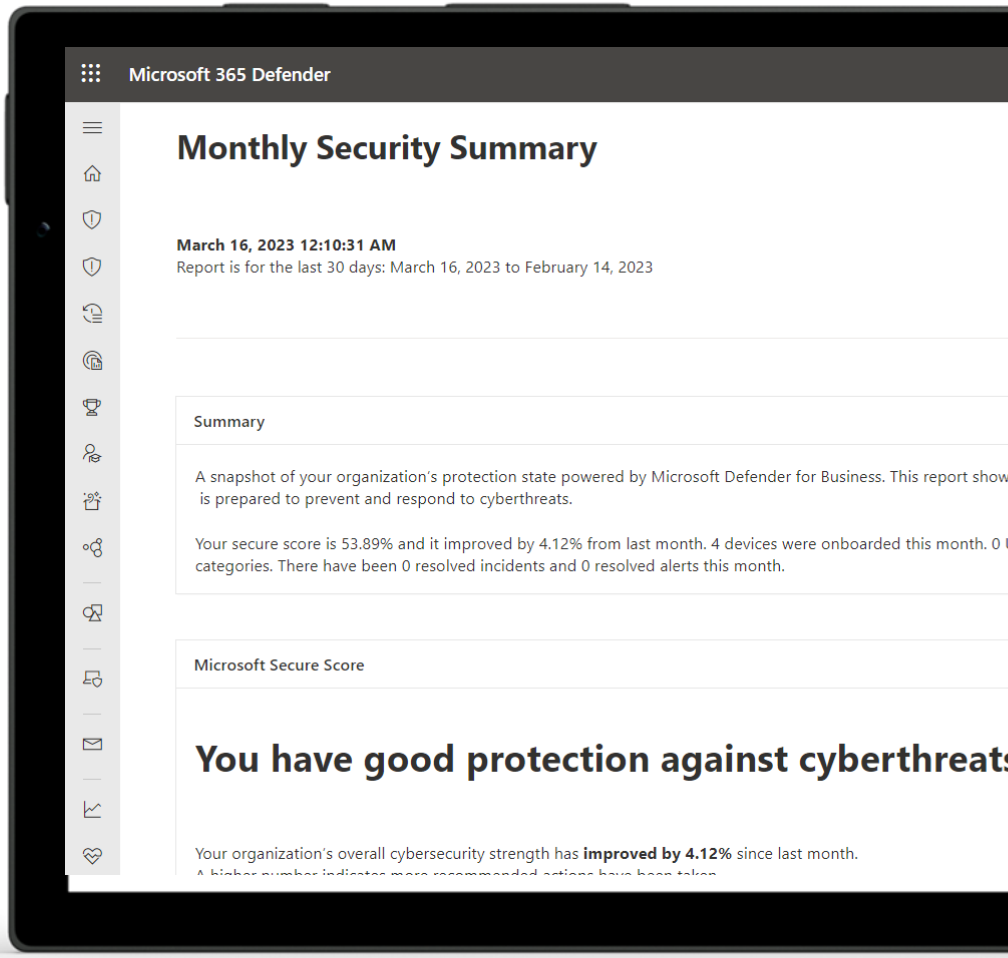
*추가 기능을 사용하려면 최소 하나의 Microsoft 365 Business Premium 또는 Defender for Business 구독이 필요합니다.

비즈니스용 Microsoft Defender

월별 보안 요약

보안 상태를 더 잘 이해하고 장치 전반에 걸쳐 개선이 필요한 영역을 식별합니다.

- 단일 관리 환경으로 클라이언트와 서버 모두에 대해 동일한 보호를 제공합니다.
- 보안을 강화할 영역을 식별합니다.
- Defender for Business로 방지된 위협을 확인하세요



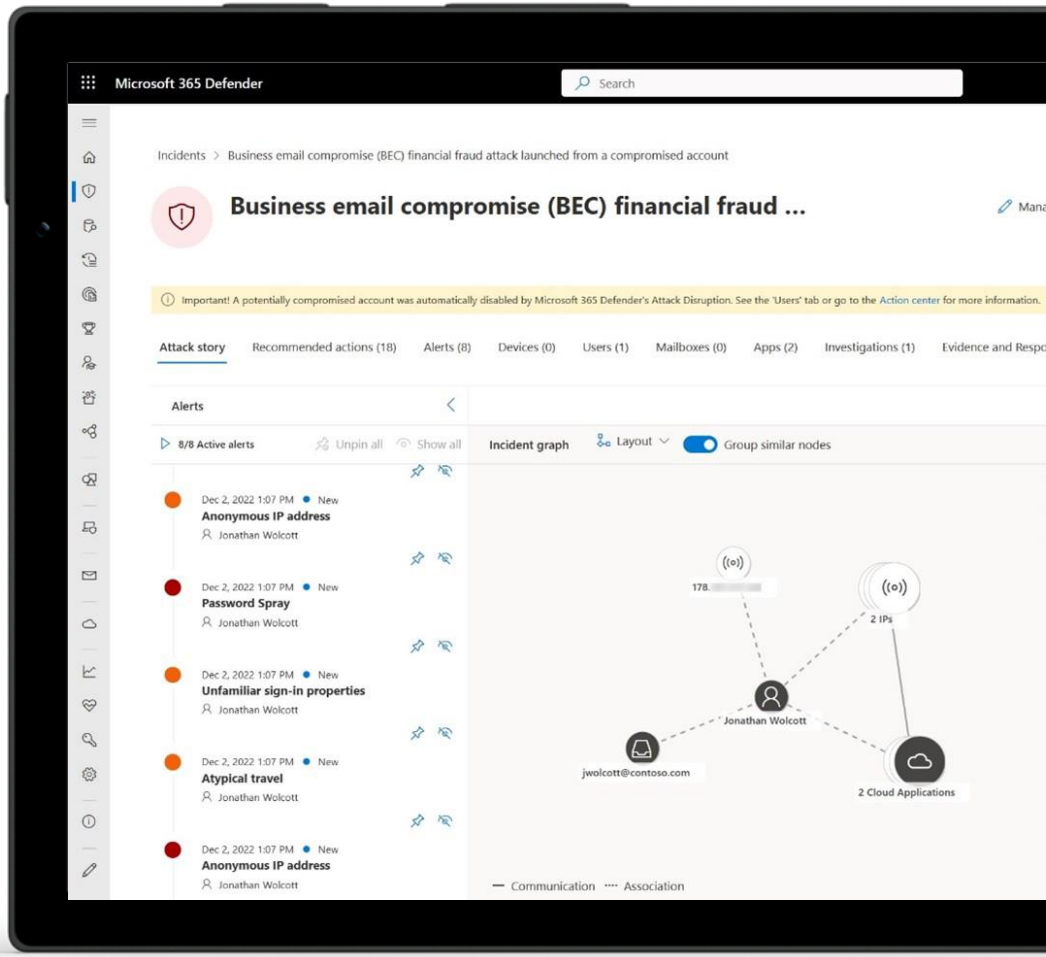
*추가 기능을 사용하려면 최소 하나의 Microsoft 365 Business Premium 또는 Defender for Business 구독이 필요합니다.

비즈니스용 Microsoft Defender

자동 공격 중단

랜섬웨어 및 맬 웨어가 비즈니에서
확산되는 것을 방지하세요.

- 진행 중인 공격과 관련된 장치를 자동으로 비활성 하거나 제한합니다.
- 정상적인 장치가 손상된 시스템과 통신하는 것을 방지.
- 사이버 위협으로 인한 피해를 최소화합니다.



Cross-Platform 엔드포인트 보안을 제공합니다.

Windows macOS

Endpoints*

iOS

Mobile device OS*

Windows 365

Azure Virtual Desktop

Virtual desktops

1이제 서버 지원을 위한 추가 기능을 사용할 수 있습니다. 2MDB 독립 실행형용 Intune이 없는 iOS 및 Android 보안이 이제 GA됩니다. Intune 플랜 1은 Microsoft 365 Business Premium에 포함되어 있습니다. 자세한 내용은 설명서를 참조하세요.

비즈니스용 Microsoft Defender

Microsoft Defender
for Business

보안 강화

위협 및 취약점 관리

공격 표면 감소

차세대 보호

엔드포인트 탐지 및 대응

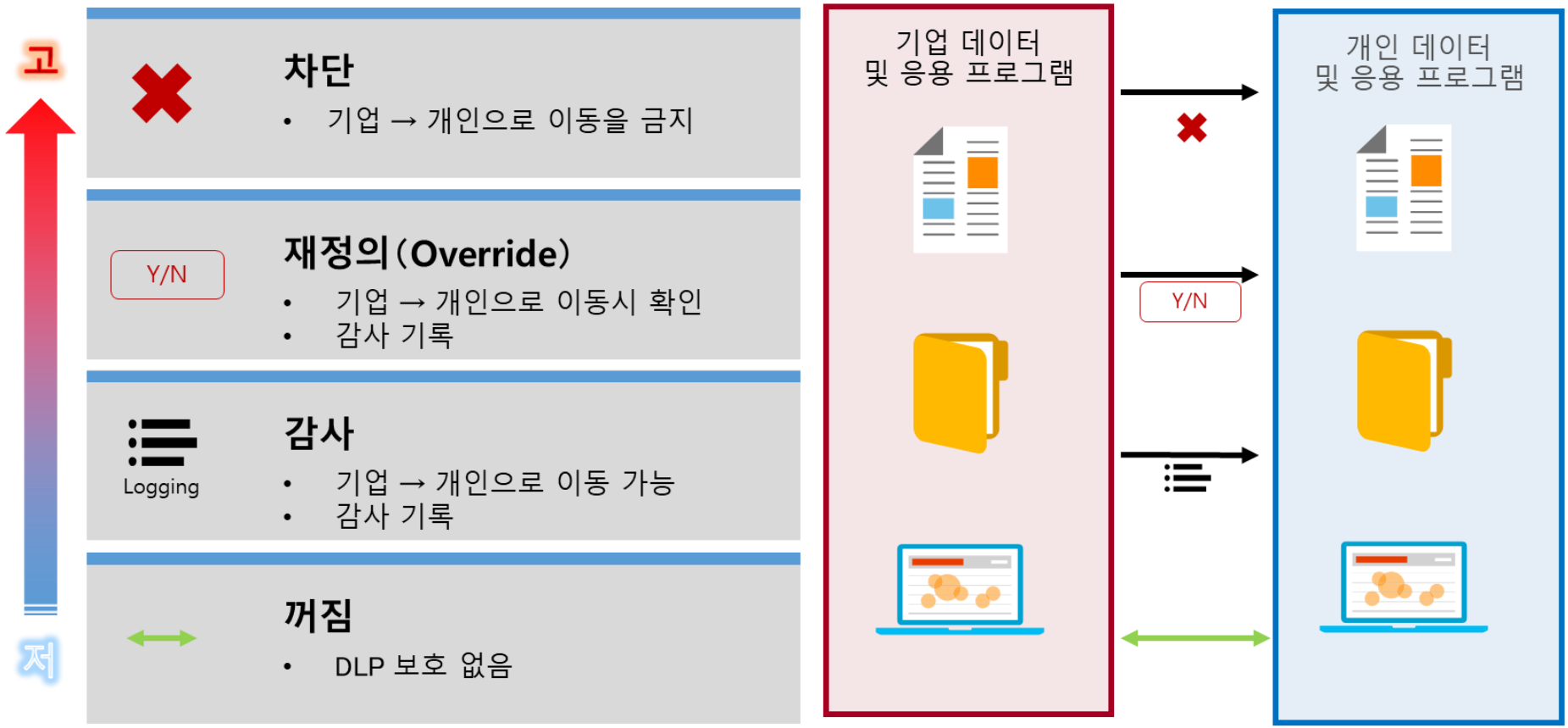
자동 조사 및 교정

단순화된 온보딩 및 관리

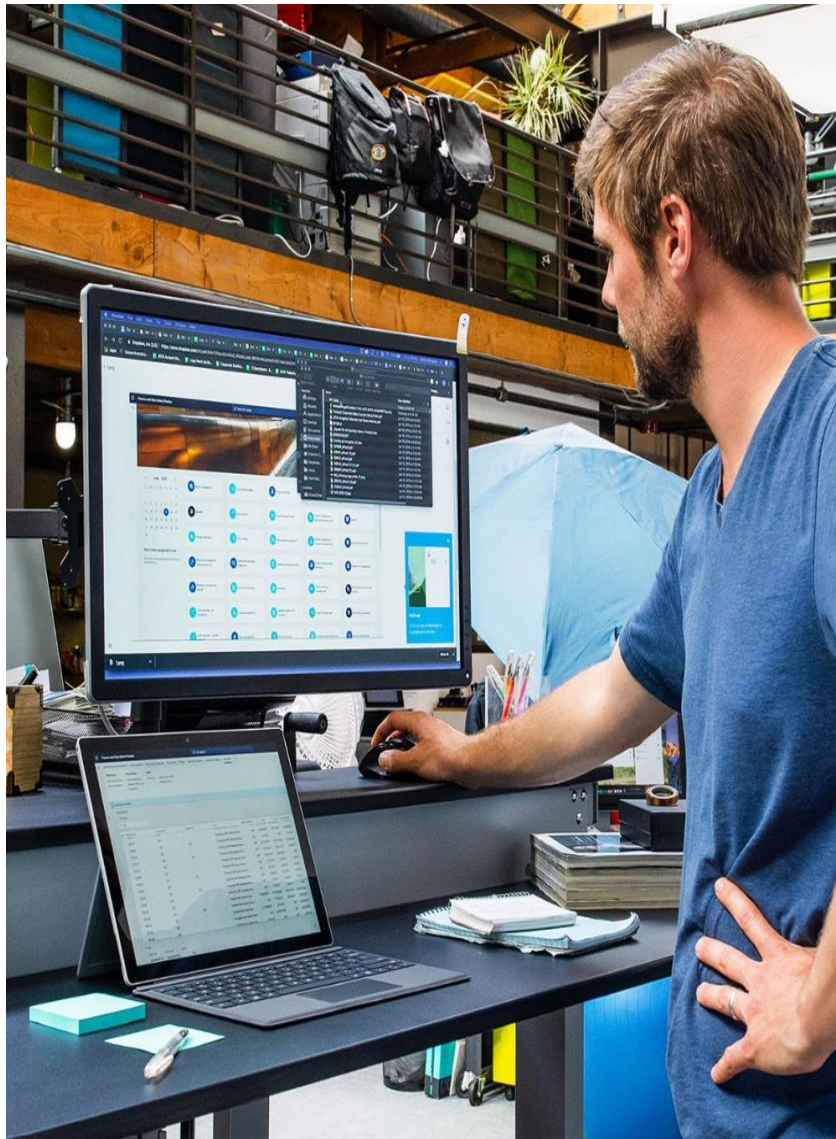
API 및 통합

How To

- 4단계 제한 모드에 따라 앱과 영역 기준으로 정책 적용이 가능하고, 관리되는 앱과 영역에서의 정보 유출을 방지



Microsoft 365 Premium Value

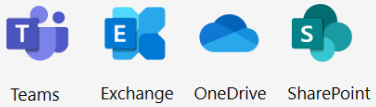


우리는 아래와 같은 해답을 제시합니다.

300인 이하 기업을 위한 솔루션

Microsoft 365 Business Basic

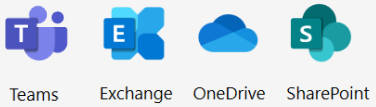
Cloud Services



$6 per user/month[1]

Microsoft 365 Business Standard

Cloud Services

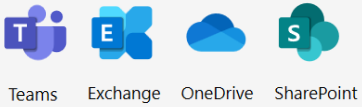


Desktop Apps

$12.50 per user/month[1]

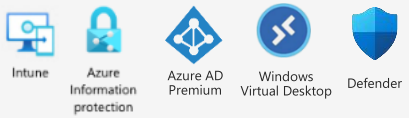
Microsoft 365 Business Premium

Cloud Services



Desktop Apps

Comprehensive Security



$22 per user/month[1]

Microsoft 365 Business Premium Benefits

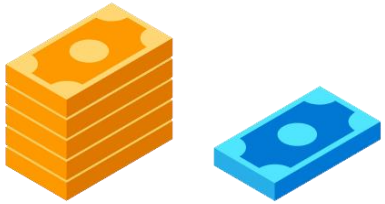
어디서나 안심하고 비즈니스를 운영할 수 있는 단일 솔루션

포괄적이고 사용하기 쉬운

생산성과 보안을 위한 단일 솔루션

클라우드 플랫폼으로 배포가 단순화됨

신속하게 시작하고 실행할 수 있습니다.



비용 절감

다중 포인트 솔루션 비용 제거

헬프 데스크 비용 절감

라이선스 복잡성 완화

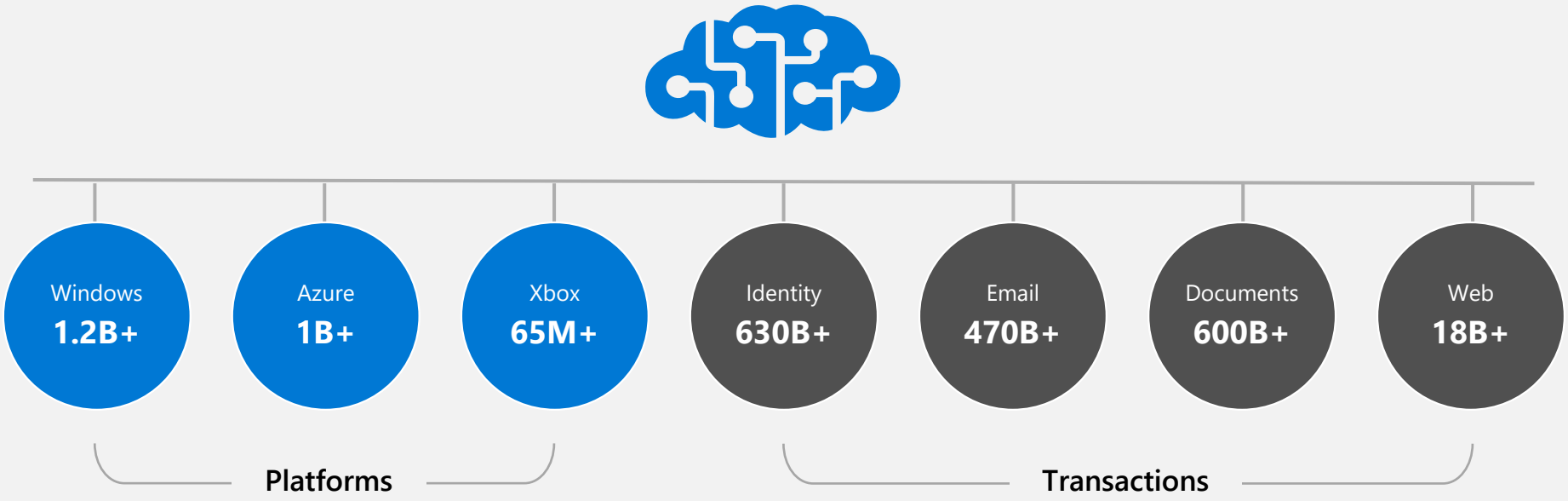
엔터프라이즈 급 기술

고급 보안; 기업의 신뢰를 받는

AI 기반 위협 인텔리전스

최고 등급의 보안 공급업체

보안에 대한 Microsoft의 고유한 유리한 지점



300B

2019년 사용자 활동 프로파일링 및 분석

2.3B

매일 발견되는 엔드포인트 취약점

11B

2019년에 차단된 악성 및 의심스러운 메시지

12B

2019년에 검사, 모니터링, 통제된 클라우드 활동

보안에 대한 Microsoft의 고유한 유리한 지점

Microsoft Defender for Business는 Business Premium을 더욱 완벽하고 비용 효율적으로 만듭니다.

Security, Identity and Device Mgmt

Remote access solutions	$5
Advanced Email protection	$5
Single Sign-On	$2
Conditional Access+ MFA	$6
Endpoint anti-virus protection	~$3
Endpoint Detection and Response	~$5
Device management	$4

Collaboration and Productivity

Productivity apps and file storage	$12
Chat based collaboration	$6.67

>$45
monthly cost of 3rd party solutions[1]

$22
monthly[2]

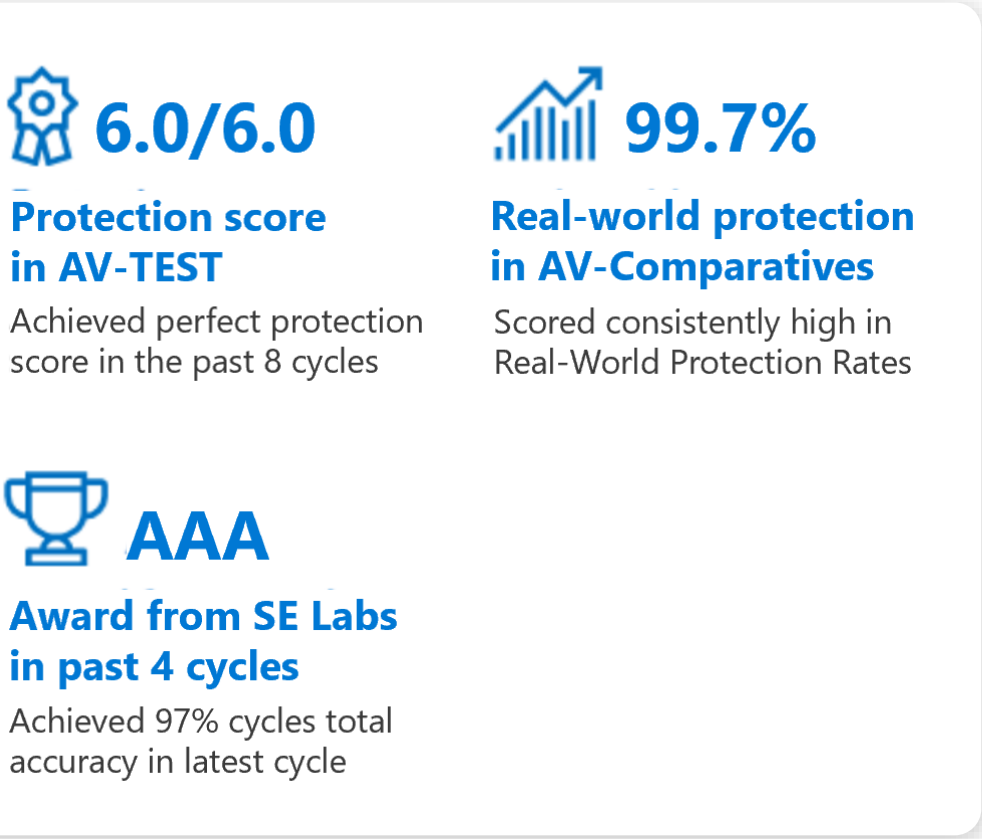
Microsoft 365 Business Premium

어디서나 안전하게 비즈니스를 운영할 수 있는 하나의 솔루션

New! Microsoft Defender for Business Premium customers now Generally Available in Microsoft 365 Business Premium

Microsoft Defender는 지속적으로 최고 AV 등급

1. **AV-TEST**: 최신 테스트에서 보호 점수 **6.0/6.0**
2. **AV-비교**: 최신 테스트에서 보호 등급 **99.7%**
3. **SE Labs**: 최신 테스트에서 **AAA** 수상
4. **SE Labs**: 최신 테스트에서 **AAA** 수상



https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/top-scoring-industry-antivirus-tests

어디서나 비즈니스를 안전하게 운영

Microsoft 365 Premium

How To

How To Work?

- 여러 위치에서 일하는 직원

보안을 어떻게 유지할 수 있나요?

- 다양한 개인 및 모바일 장치

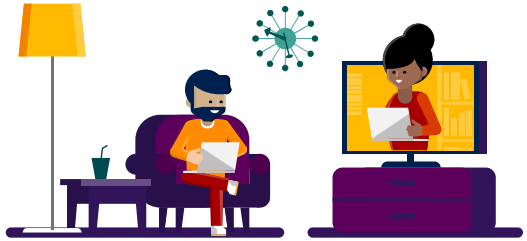
비용을 어떻게 줄일 수 있나요?

- 피싱 및 랜섬웨어 증가

동료, 고객, 파트너와 협업

실시간 팀워크

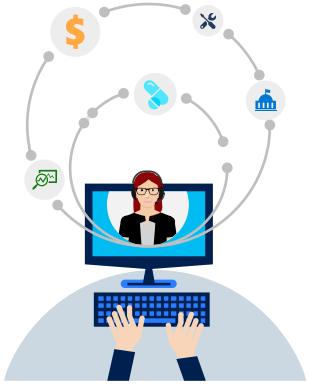
어디에서나 미팅,업무 참여



원활한 외부 협업

회사 데이터에 액세스하는 장치를 보호하고 관리

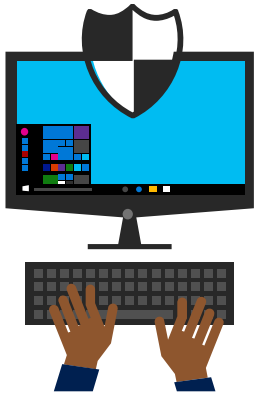
모바일 장치에서 업무 데이터 관리



Autopilot을 사용하여 배포 자동화

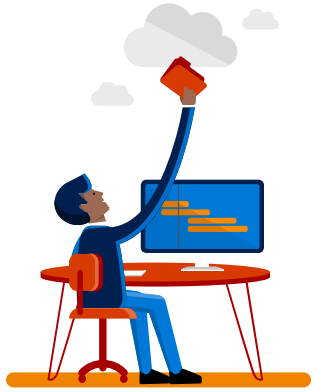
비즈니스용 Defender로 장치를 보호

하이브리드 작업은 ID 및 액세스 보안에서 시작



분실 및 도난당한
비밀번호로부터 보호

업무용 앱에 대한
보안 액세스



원격 데스크톱
액세스 활성화

어디서나 안전한 액세스를 활성화하고 신원을 보호하세요.

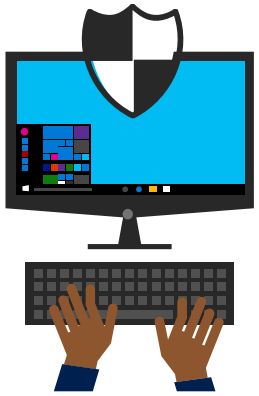
Windows Virtual Desktop 액세스 활성화

Windows Virtual Desktop으로 원격 데스크톱 액세스 활성화

- 확장성이 뛰어나고 최신 상태로 유지되는 유일한 다중 세션 Windows 10 환경 제공
- Office 최적화 활성화
- RDS 데스크톱 및 앱을 마이그레이션하고 라이선스를 단순화하고 비용을 절감
- 몇 분 안에 배포하고 확장하세요. Azure Portal의 통합 관리 인터페이스로 관리
- Windows, Android, Mac, iOS, HTML 5를 포함한 모든 최종 사용자 기기 플랫폼 지원

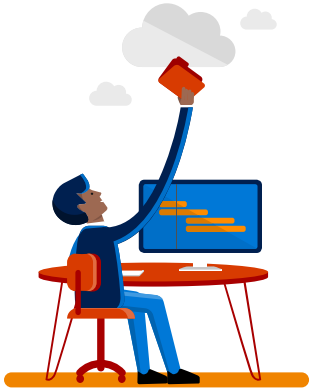
사이버 위협으로부터 방어하고 비즈니스데이터를 보호

Office 365용 Microsoft Defender, DLP 및 Azure Information Protection



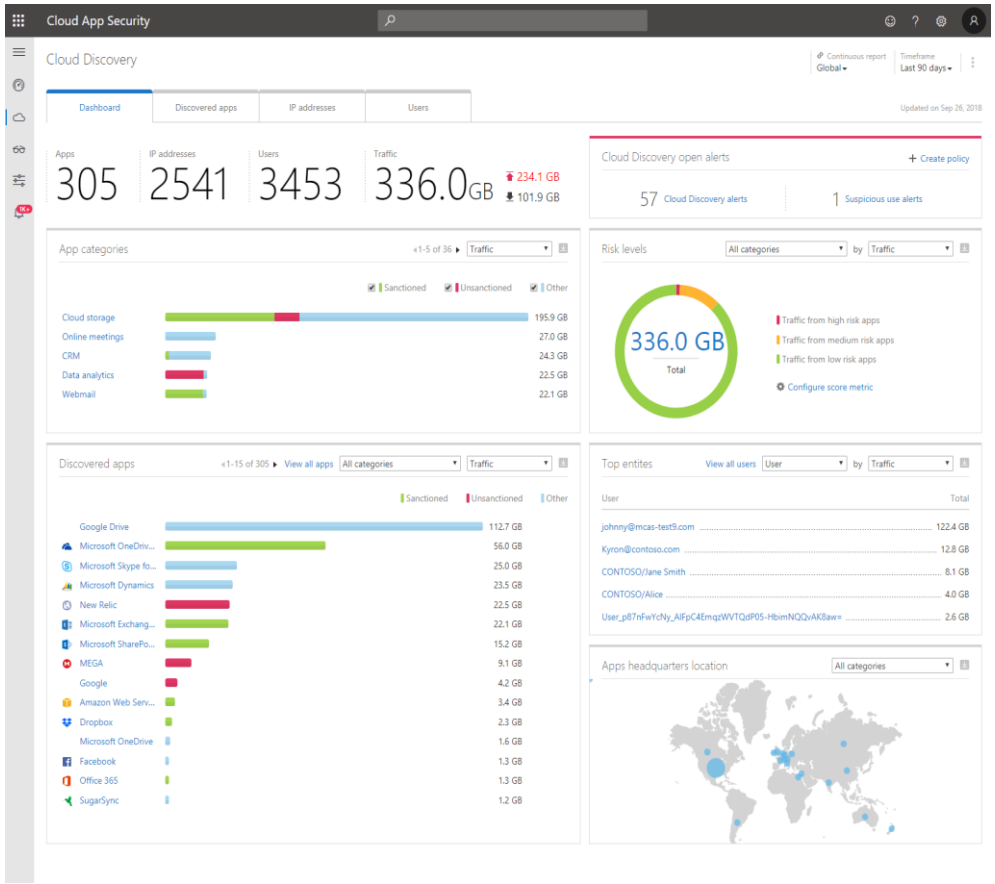
피싱, 사이버 위협으로 사용자를 보호

기밀 비즈니스 데이터를 보호



클라우드 앱 사용에 대한 가시성 확보

Cloud App Discovery를 통해 클라우드 앱 사용에 대한 가시성을 확보



Cloud App Discovery를 통해 클라우드 앱 사용에 대한 가시성을 확보

- 16,000개 이상의 클라우드 앱에 대한 위험 평가를 통해 클라우드 앱의 보안을 이해
- 사용 패턴을 이해하고 위험도가 높은 사용자를 식별합니다. 추가 분석을 위해 데이터 내보내기
- IT가 제어할 수 있도록 애플리케이션의 우선 순위를 지정하고 애플리케이션을 통합하여 SSO(Single Sign-On) 및 사용자 관리를 지원

M365 Business Premium을 통한 포괄적인 보안

Microsoft 365 Business Premium

Identity Security

User

MFA와 같은 Azure AD 기능

셀프 서비스 비밀번호 재설정

조건부 액세스

동적 그룹

Device Security

Device

EDR을 통한 랜섬웨어 및 맬웨어 방지를 위한 비즈니스용 Microsoft Defender

Intune을 통한 모바일 및 노트북의 완전 중앙 집중식 관리

분실 및 도난당한 장치의 데이터 원격 삭제

BitLocker 암호화

Wi-Fi, VPN 프로필과 함께 강력한 핀 요구 사항 적용

Application Security

Application

Intune 앱 보호 정책을 사용하여 개인 앱에 회사 데이터 복사/붙여넣기/저장을 제한합니다.

맬웨어 및 제로 데이 공격으로부터 보호하기 위한 Defender for Office 365

민감한 데이터가 전송되는 것을 모니터링하는 데이터 손실 방지

"전달 금지" 또는 "이메일 암호화"와 같은 이메일 제한 사항

Document Security

Document

Azure Information Protection은 Teams를 포함한 보안 공유를 위해 문서를 보호하고 분류합니다.

문서에 대한 액세스 권한 취소

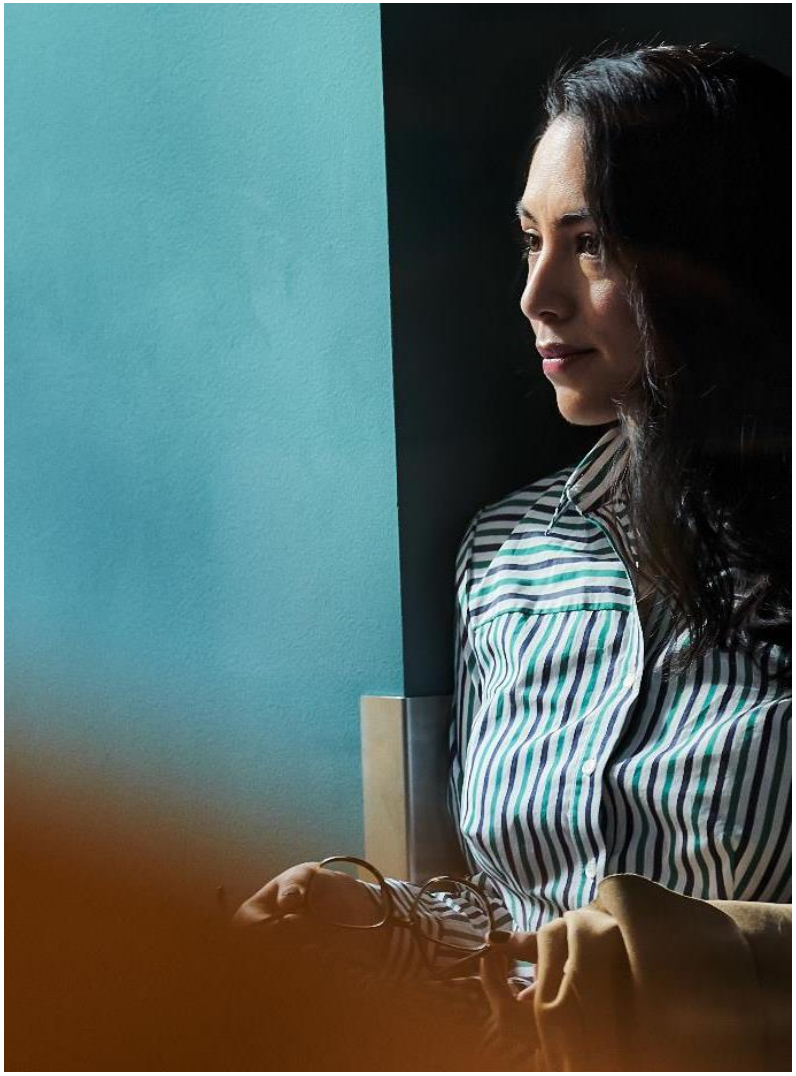
민감한 문서 추적

Microsoft 365 Business Premium 요약 혜택

Microsoft 365 Business Premium은 사용하기 쉬운 공동 작업, 커뮤니케이션, 보안을 위한 올인원 솔루션입니다.

Microsoft 365는 피싱, 바이러스, 랜섬웨어 공격과 같은 사이버 위협으로 인해 비용이 많이 드는 피해 위험을 줄이는 데 도움이 됩니다.

Microsoft 365는 유사한 타사 제품 컬렉션에 비해 비용이 저렴하고 관리하기 쉽습니다.



Microsoft

Next steps

eunjung@poohmvp.onmicrosoft.com
박은정(EunJung Park)

••••••••••

Login

https://forms.office.com/r/Nf3QNq8jE3

안녕하세요? 박은정 MVP입니다.

M. Cloud Bridge

Specialized Consulting Firm in Data & AI

Specialized Consulting Firm in Data & AI Cloud System

Data & BI

Big Data & AI

Data Flow & Automation

Data Infra & Security

Thank You

T. 02.552.9700

E. info@mcloudbridge.com

H. www.mcloudbridge.com

데이터에 가치를 더하여 고객의 성장에 공헌합니다.

Specialized Consulting Firm in **Data & AI** Cloud System

Copyrightⓒ 2022-2023 by M(Multi) Cloud Bridge Co., Ltd All rights reserved.