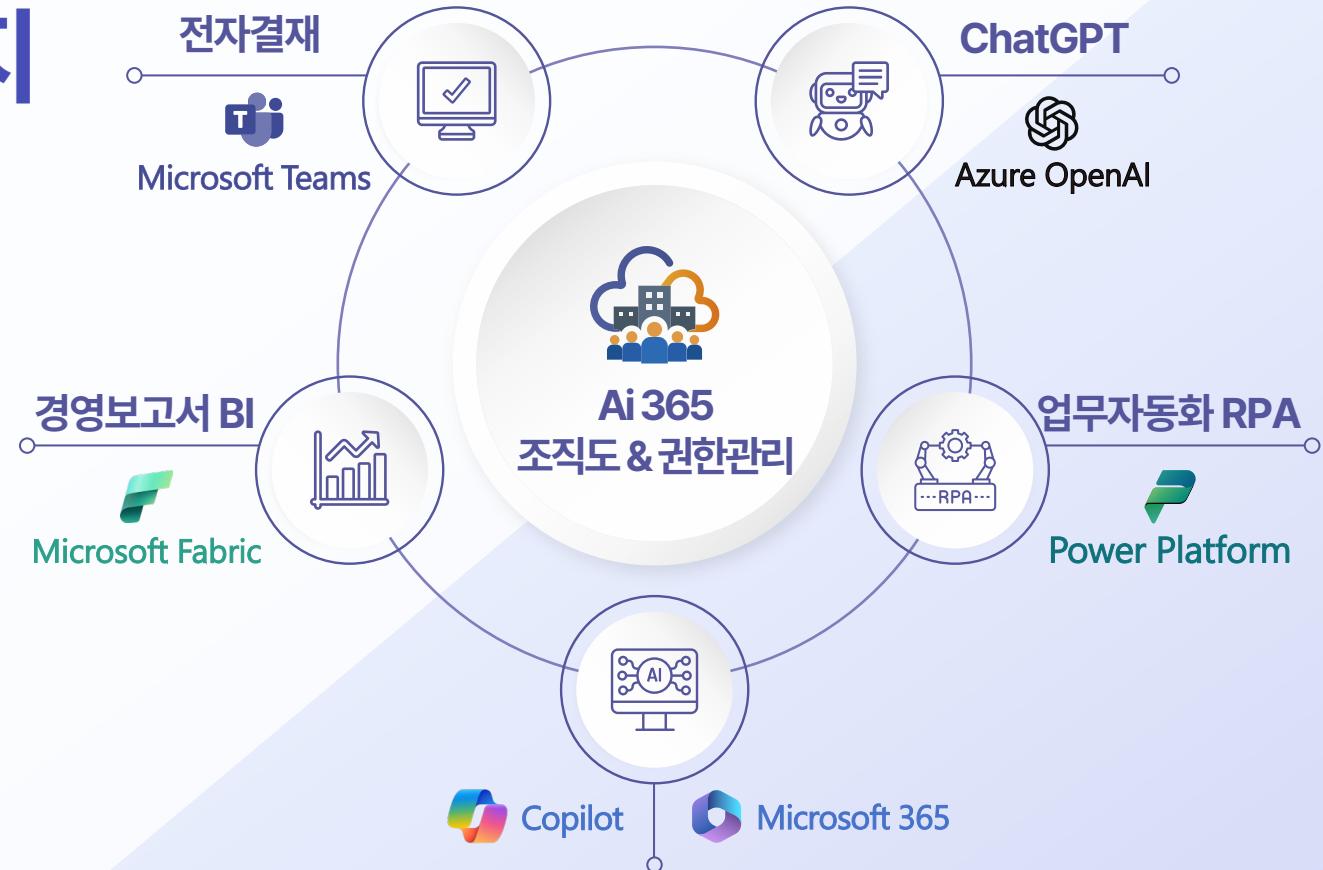


Ai 365 모니터링 보고서

Microsoft 365 부터 Azure까지 생산성 및 비용 모니터링

엠클라우드브리지
이경준 부문장



Agenda

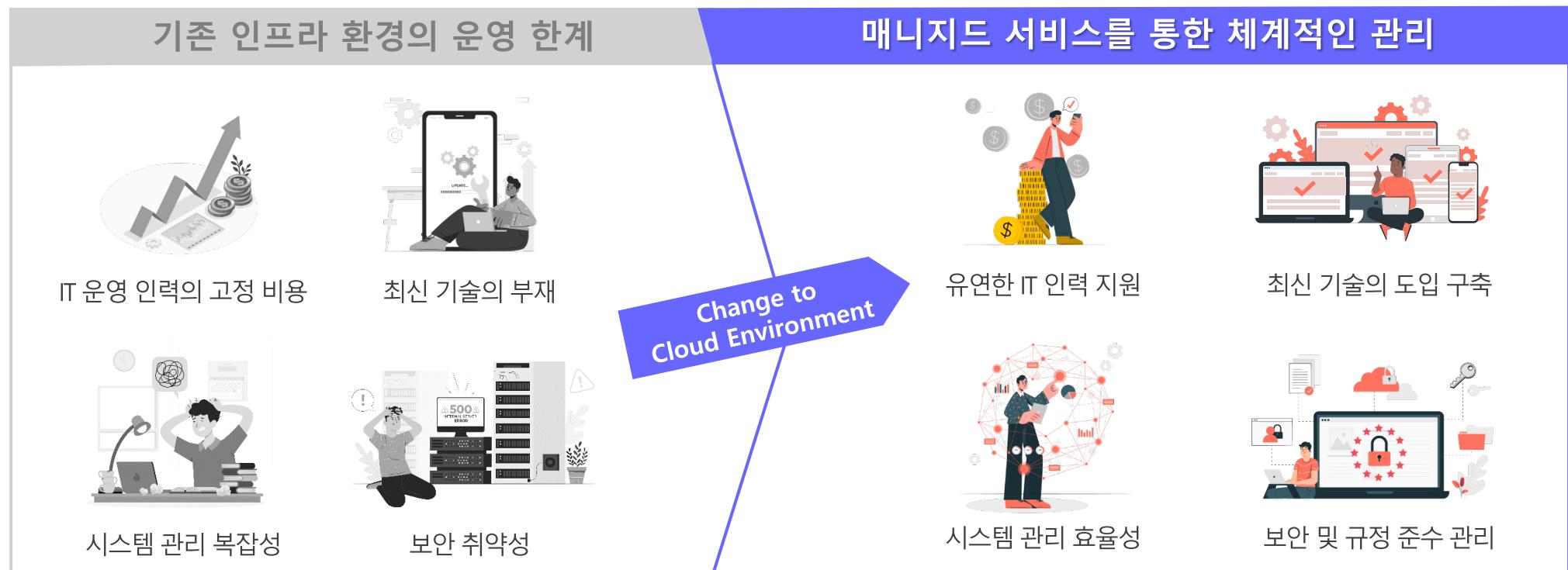
1. 매니지드 서비스(MCOM) 필요성
2. Ai 365 모니터링 보고서 개요
3. Microsoft 365 생산성 및 비용 보고서
4. EMS 보안 현황 보고서
5. Azure 리소스 현황 및 비용 보고서

1

매니지드 서비스(MCOM) 필요성

클라우드 도입에 따른 인프라 운영 관리 변화로 기존 인프라 환경에서의 한계점으로 지적되었던 IT 운영 인력의 고정 비용, 최신 기술의 부재, 복잡한 시스템 관리 그리고 보안 취약점까지 매니지드 서비스를 통한 체계적인 관리로 효율적이고 원활하게 운영 될 수 있도록 지원합니다.

클라우드 도입에 따른 인프라 운영 관리 변화

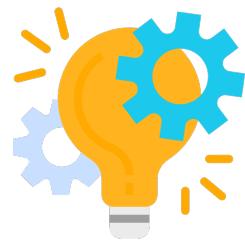


전문 엔지니어의 숙련된 인프라 기술 지원과 시각화 된 월별 보고서로 안정적인 인프라 모니터링을 제공

매니지드 서비스 지원 내용으로 지속적으로 발전하는 최신 기술의 도입 및 관리와 보안 위협 및 취약성으로부터 인프라를 보호하고 신속하게 문제를 해결 할 수 있도록 지원하며, 비용 효율적인 유연한 IT 인력 투입으로 체계적인 클라우드 인프라 운영 관리가 될 수 있도록 지원 합니다.

매니지드 서비스(MCOM) 지원 내용

최신 기술 도입 및 관리



새로운 기술에 대하여 절대적인
습득 시간이 필요하므로 빠르게
숙지하고 도입할 수 있도록 지원 할
수 있는 숙련된 엔지니어의 필요

클라우드 보안 운영



랜섬웨어와 해킹, DDoS 공격
등의 피해로 업무가 마비 되는
현상을 보호하기 위해 전문화
된 인프라 보안 엔지니어 필요

문제 해결 지원



클라우드 인프라에서
지속적으로 발생되는 문제점을
신속하고 효율적으로 지원할 수
있는 엔지니어 필요

유연한 IT 인력



클라우드 인프라 운영 관리를
위한 고정 인건 비용에 대해서
유연하고 최적화 된 전문
엔지니어 필요

매니지드 서비스(MCOM) 지원 영역으로 클라우드 서비스의 월 운영 보고서와 리소스 비용 관리, 서비스 운영 및 패치 등의 유지보수, 긴급 장애 대응, 안정적인 인프라 정책 관리와 보안 취약점 검사로 고객사의 보안 태세를 향상시키고 인프라 운영 시간과 비용을 줄일 수 있습니다.

매니지드 서비스(MCOM) 지원 영역

월간 보고서

사용량에 대한 비용 및 운영에 대한 월별 보고서 제공

유지 보수

클라우드 서비스 운영에 따른 보안 및 패치 등의 유지 보수

인프라 운영 관리

적절한 클라우드 리소스 관리로 인프라의 안정성 증대

비용 관리

용도와 필요에 맞는 서비스 운영으로 비용 효율적 운영

긴급 점검

클라우드 서비스 운영 중 긴급 문제에 대한 대응

클라우드 보안

보안 취약점에 대한 대응으로 고객사의 보안 태세 향상



월간 보고서



비용관리



유지보수



긴급 점검



안정적인 인프라

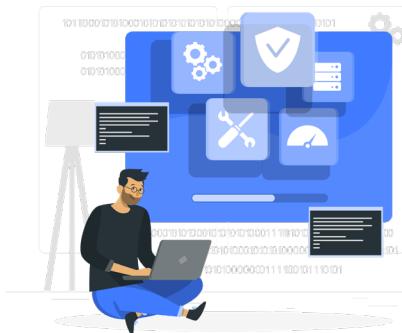


클라우드 보안

모니터링의 필요성은 기업 내 다양한 인프라 환경에서의 애플리케이션, 시스템의 성능과 장애 대응 및 보안 감사 그리고 비용 현황 데이터를 통합 된 하나의 대시보드를 통하여 성능 최적화, 장애 대응 및 예측, 보안 강화, 비용 관리 등의 다양한 측면에서 비즈니스 가치를 제공합니다.

모니터링의 필요성

성능 최적화



- 효율적인 운영 워크플로 구축
- 불필요한 리소스 정리
- 시스템 안정성 유지

장애 대응 및 예측



- 시스템 장애 예방적 유지보수
- 시스템 다운 타임 감소
- 신속한 장애 해결

보안 강화



- 데이터 보호 강화
- 비즈니스 데이터 규정 준수
- 보안 위협 및 취약점 대응

비용 관리



- 최적화된 지출 및 비용 절감
- 체계적인 리소스 및 비용 관리
- 현재 비용 추세와 예상 비용 파악

성능 최적화, 장애 대응 및 예측, 보안 강화, 비용 관리 등 다양한 측면에서 비즈니스 가치를 제공

2

Ai 365 모니터링 보고서 개요

Ai 365 모니터링 보고서는 원활한 클라우드 운영을 위해 Microsoft 365 및 Azure 서비스 상태와 조직 내 사용자 활동 현황, 라이선스 및 리소스 상태, 서비스 보안 현황과 M365 저장소 용량 및 Azure 클라우드 리소스 사용량 정보를 제공하여 최적화 된 운영 관리를 지원합니다.

Ai 365 모니터링 보고서 개요



라이선스 현황

- Microsoft 구독 제품 현황
- 사용자 할당 라이선스 현황
- 라이선스 금액 현황



사용자 현황

- 조직내 사용자 현황
- 사용자 활동량 및 사용량 현황
- 위험한 사용자 현황



서비스 상태

- Microsoft 365 서비스 상태
- Azure 네트워크 상태
- Resource 상태



리소스 상태

- Azure Backup 상태
- Microsoft Defender 상태
- VM Metric 상태

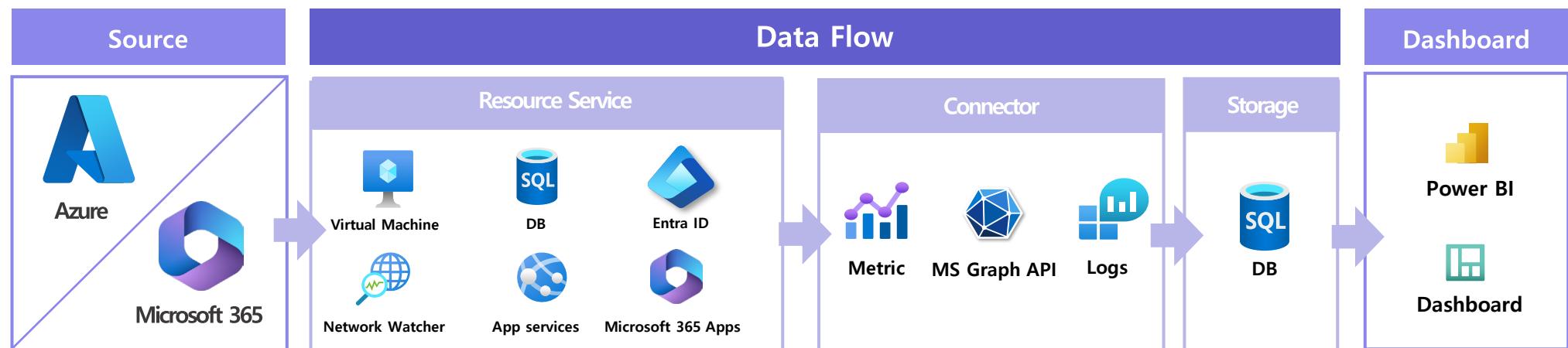


보안 현황

- 계정 보안 현황
- 장치 보안 현황
- 데이터 보안 현황

Ai 365 모니터링 아키텍처는 Azure 및 Microsoft 365의 수많은 Log 데이터와의 연결을 통하여 안정적인 운영을 위하여 필요한 정보들을 하나의 대시보드에서 확인 할 수 있도록 데이터를 중앙화하고 Power BI 기반으로 사용 현황 및 리소스 상태, 비용에 대한 정보를 제공 합니다.

Ai 365 모니터링 아키텍처



모니터링 서비스 도입 효과

- Azure 리소스 및 M365 사용 현황을 시각화 하여 상태 모니터링 및 분석 용이
- Azure 리소스 및 M365 상태 경고 및 알림을 설정하여 빠르게 대응 가능
- Azure 리소스 및 M365 상태를 자동 업데이트 하여 번거로움 감소
- 대시보드 활용을 통해 리소스 상태를 모니터링 하고 분석하는데 드는 시간과 비용을 절감

Ai 365 모니터링의 특징

- **전문 인력 보유:** Power BI 기술력을 활용하여 대시보드 구축이 가능한 BI 엔지니어와 Azure 및 Microsoft 365 기술지원이 가능한 MS 자격을 갖춘 엔지니어로 구성 되어, 모니터링 및 장애 발생시 빠른 대응 가능
- **다양한 레퍼런스 경험:** MCB는 다수의 Power BI 프로젝트 경험과 능력을 보유, 고객사 맞춤 대시보드 및 보고서 제작 가능

Microsoft 365 및 EMS 모니터링은 Microsoft 365 플랫폼의 안정적인 운영을 위해 제공되는 모니터링으로, 클라우드 저장소를 포함한 Outlook, Teams 및 SharePoint 등의 플랫폼에 대한 상태 모니터링과 보안 침해 및 거버넌스 규정 준수에 관한 내용을 제공하고 있습니다.

Microsoft 365 및 EMS 모니터링

상태 모니터링

Microsoft 서비스의 현재 상태와 문제를 해결할 때 업데이트를 표시합니다.

상태

- ▲ 인시던트 1개, 권고 6개
- ▲ 인시던트 1개
- ▲ 인시던트 1개
- ▲ 인시던트 1개
- 권고 6개

Exchange Online
Microsoft 365 suite
Microsoft Teams
SharePoint Online
OneDrive for Business
Azure Information Protection
Dynamics 365 Apps
Identity Service
Microsoft 365 apps

라이선스 모니터링

이름	사용 가능한 라이선스	활성화된 라이선스	계정
Azure Active Directory Basic	10	0/10	조직
Dynamics 365 Customer Engagement Plan	작용되지 않음	작용되지 않음	조직
Dynamics 365 Customer Insights vTrial	9998	2/10000	조직
Dynamics 365 Customer Service Enterprise 바이럴 평가판	9976	24/10000	조직
Dynamics 365 Field Service 바이럴 평가판	9976	24/10000	조직
Dynamics 365 Marketing Business Edition	9998	2/10000	조직
Dynamics 365 Operations Application Partner Sandbox	6	44/50	조직
Dynamics 365 Premium 바이럴 평가판	9998	2/10000	조직
Field Service 및 Customer Service ...	6	44/50	조직
117	83/200	조직	
0	1/1	조직	
999945	55	조직	
9971	29/10000	조직	
9949	51/10000	조직	

사용량 모니터링

활성 사용자

활성 사용자 - Microsoft 365 서비스

14 사용자

활성 사용자 - Microsoft 365

2 활성 사용자

전자 메일 활동

451 활동

신체적 거리 준수 보고서가 등록되었습니다.

Microsoft Teams

20 활동

신체적 거리 준수 보고서가 등록되었습니다.

활성 사용자

활성 사용자

로 이용되었습니다. 고객은 새 Exchange 관리 센터에서만 메일 폴더를 만들거나 보거나 편집할 수 있습니다. 지금 사용하세요!

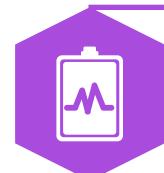
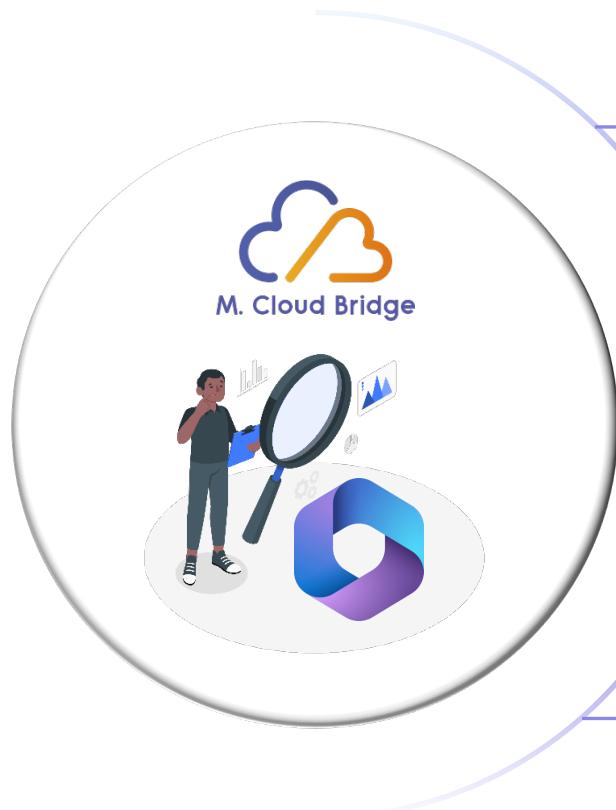
파일 위치: 2023.03.27.-2023.04.27. | 정책: 모두 | 기여 사용자: 모두 | +4개 항목 더 보기

상태	활동 수	마지막 발생 날짜
Office Manager Default Alert P...	활성	2023년 4월 26일 오후 6:00
Office Manager Default Alert P...	활성	2023년 4월 21일 오후 1:00
DLP-24	활성	2023년 4월 21일 오후 12:46
DLP-24	활성	2023년 4월 21일 오후 11:16
MIP AutoLabel simulation completed	활성	2023년 4월 21일 오후 10:49
eDiscovery search started or exported	활성	2023년 4월 21일 오후 10:26
eDiscovery search started or exported	활성	2023년 4월 21일 오후 10:26
MIP AutoLabel simulation completed	활성	2023년 4월 21일 오후 10:18
DLP-24	활성	2023년 4월 21일 오후 10:06
MIP AutoLabel simulation completed	활성	2023년 4월 21일 오후 9:54
DLP-24	활성	2023년 4월 20일 오후 12:52

보안 모니터링

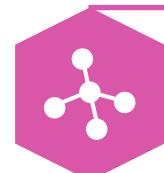
Microsoft 365 및 EMS 모니터링은 Microsoft 365 협업 플랫폼을 사용함에 있어 발생되는 서비스의 장애와 이슈를 신속하게 파악하고, 보안 위협과 데이터 유출을 최소화할 수 있으며 부서 및 사용자별 사용량의 가시성을 제공하여 조직 내 활용도를 파악할 수 있도록 지원합니다.

Microsoft 365 및 EMS 모니터링 상세 내용



상태 모니터링

- Microsoft 365 Service Health: 서비스의 상태 및 가용성 정보를 제공하며, 서비스 문제 및 예정된 유지 보수 작업을 모니터링
- Microsoft 365 로그: 로그 데이터를 검색하고 분석하여 서비스 상태, 사용자 활동, 보안 이슈 등을 모니터링



라이선스 모니터링

- Microsoft 365 관리자 포털: 현재 조직에서 구독 중인 라이선스를 확인 할 수 있으며, 각 라이선스의 총 수량 및 할당 된 개수 등을 모니터링
- Microsoft 365 청구 페이지: 구매한 라이선스의 금액을 확인하는 모니터링



보안 모니터링

- Microsoft Secure Score: Microsoft 365의 보안 상태를 측정하여 보안 위험을 최소화하도록 도와주는 도구
- Microsoft Cloud App Security: 클라우드 애플리케이션 사용에 대한 실시간 가시성을 제공하며, 클라우드 애플리케이션의 사용, 데이터 이동 및 보안 위협을 모니터링

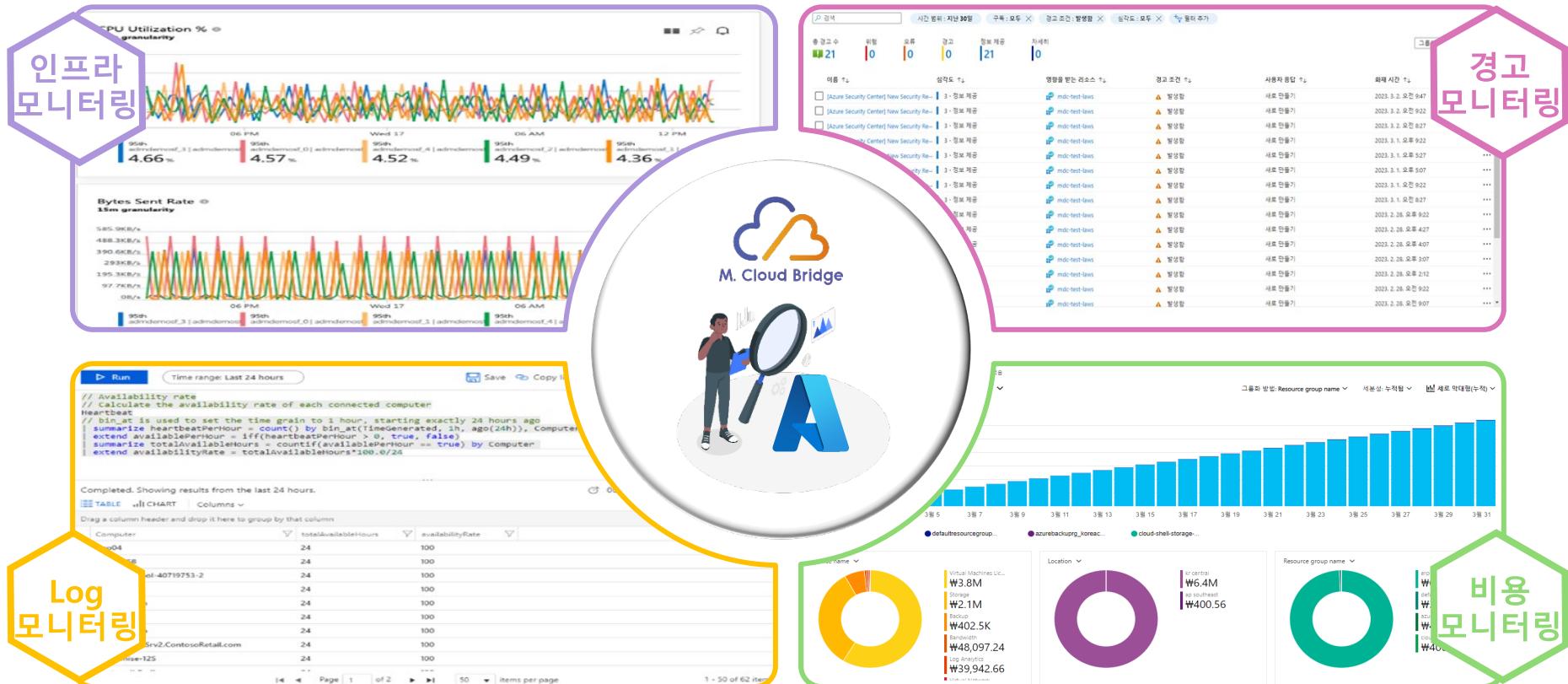


사용량 모니터링

- Microsoft 365 사용량 분석: 사용자, 팀 및 애플리케이션을 분석하는 기능을 제공하고 사용량 데이터를 사용하여 사용자 및 팀의 생산성을 최적화
- Microsoft 365 Admin Center: 사용자, 그룹 및 애플리케이션의 사용량을 모니터링하고 관리하는 대시보드

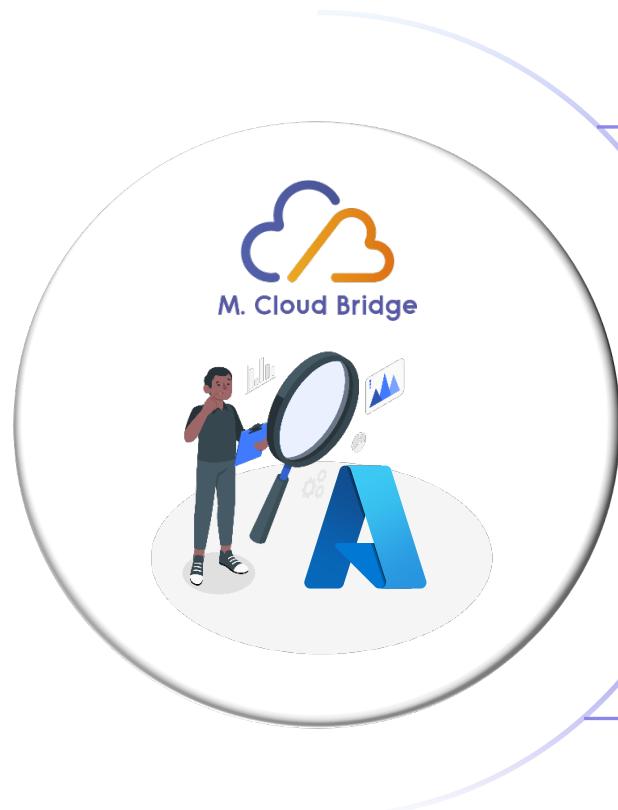
Azure 서비스 및 비용 모니터링은 가상머신의 CPU, Memory, Disk, Network 등의 정보를 제공하여 안정적인 서버 운영을 할 수 있도록 지원하며, 리소스 및 서비스 사용량에 따른 알림 및 취약점 경고, 비용을 안내하여 최적화된 서비스를 이용할 수 있도록 정보를 제공 합니다.

Azure 서비스 및 비용 모니터링



Azure 서비스 및 비용 모니터링은 클라우드 서비스의 가용성과 효율성을 향상시키기 위해 Azure 리소스에 해당되는 다양한 정보들을 분석하는 포괄적인 모니터링을 지원하며 이벤트 로그를 수집하여 성능 이슈를 진단하고 사용량을 기반으로한 비용 모니터링을 제공합니다.

Azure 서비스 및 비용 모니터링 상세 내용



인프라 모니터링

- 가상 머신의 CPU, 메모리, 디스크 사용률, 네트워크 성능 등을 모니터링
- Network Watcher를 이용한 네트워크 모니터링: 네트워크 서비스에 대한 모니터링 제공



경고 모니터링

- Azure Monitor를 이용한 경고 규칙: 사용자가 정의한 경고 규칙에 따라 경고를 생성 하며, 경고 규칙은 이벤트, 메트릭, 로그 데이터 등에 따라 생성
- 알림: 경고 발생 시 이메일, SMS, 푸시 알림 등의 방식으로 알림을 제공



Log 모니터링

- Log Analytics을 이용한 로그 검색: 로그 쿼리 언어를 사용하여 로그 데이터를 검색하고 분석
- 로그 데이터 분석: 수집한 로그 데이터를 분석하여 성능 이슈나 장애 발생 원인을 파악



비용 모니터링

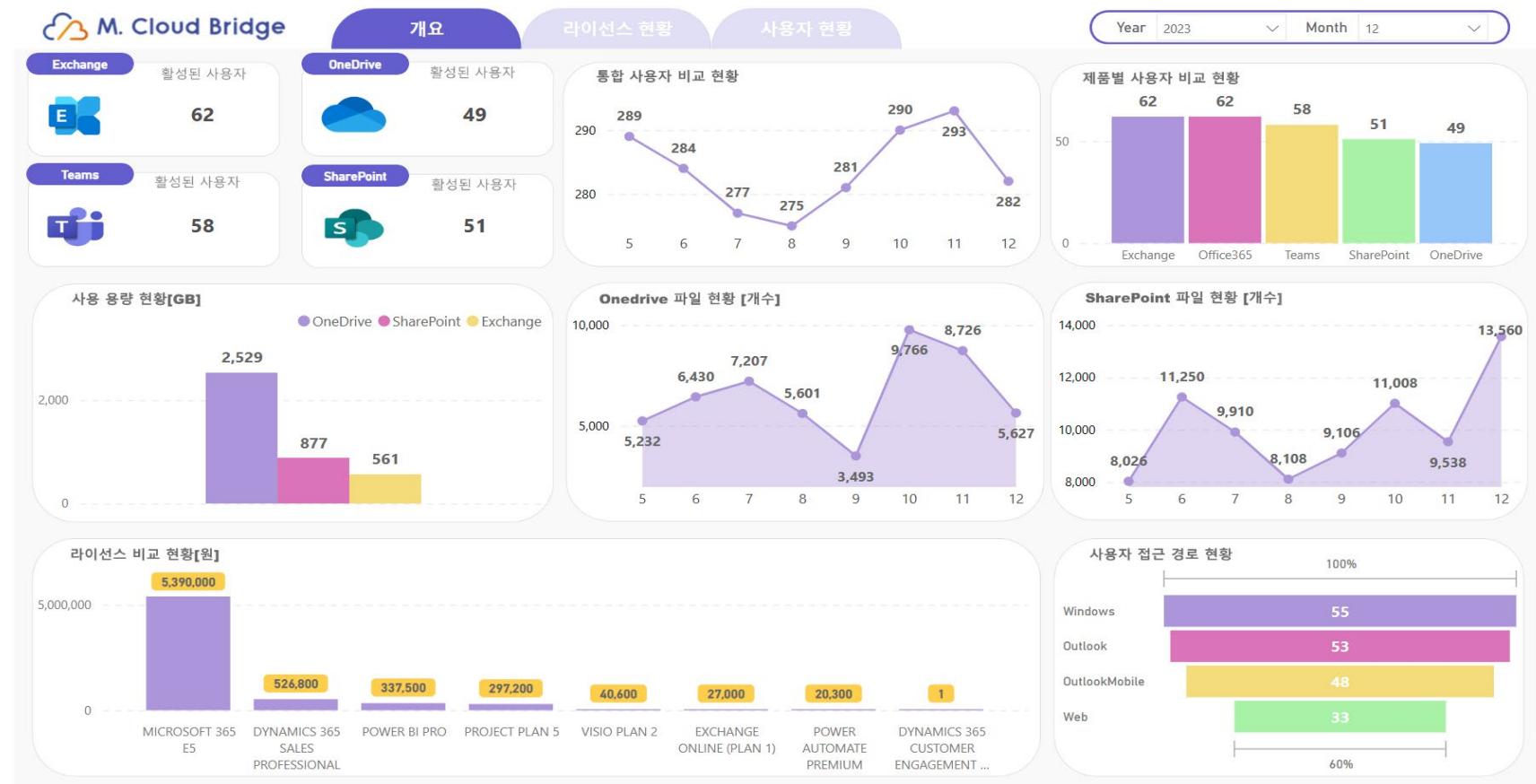
- Cost Management를 이용한 비용 모니터링: Azure 서비스와 리소스의 사용량을 기반으로한 비용 모니터링
- 비용 최적화: 비용 추이를 확인하여 비용 최적화 진행

3

Microsoft 365 생산성 및 비용 보고서

Microsoft 365 생산성 및 비용 보고서는 Microsoft 365의 기본 사용 현황을 파악 할 수 있는 개요 탭을 중심으로, 조직에서 사용하고 있는 라이선스 현황과 비용, 플랫폼별 사용량을 확인 할 수 있는 보고서를 제공하여 플랫폼별 사용량과 비용을 한눈에 확인할 수 있습니다.

Microsoft 365 생산성 및 비용 보고서



Microsoft 365 라이선스 현황

M. Cloud Bridge

개요 라이선스 현황 사용자 현황

Year: 2023 Month: 12

제품별 사용자 통합 현황

제품	활성된 사용자	신규 사용자
Exchange	62	0
Office365	62	0
OneDrive	49	0
SharePoint	51	1
Teams	58	0
Total	282	1

제품별 사용자 현황

제품	활성 사용자 수
Exchange	62
Office365	62
Teams	58
SharePoint	51
OneDrive	49

활성된 서비스 개수 현황

서비스	활성 개수
Total	21

라이선스 사용자 현황

라이선스	활동량	라이선스 비용
MICROSOFT 365 E5	70	5,390,000
DYNAMICS 365 SALES PROFESSIONAL	6	526,800
POWER BI PRO	25	337,500
PROJECT PLAN 5	4	297,200
VISIO PLAN 2	2	40,600
EXCHANGE ONLINE (PLAN 1)	5	27,000
POWER AUTOMATE PREMIUM	1	20,300
DYNAMICS 365 CUSTOMER ENGAGEMENT PLAN	1	1
DYNAMICS 365 CUSTOMER INSIGHTS VTRIAL	1	0
DYNAMICS 365 CUSTOMER SERVICE ENTERPRISE VTR...	24	0
DYNAMICS 365 FIELD SERVICE VTRIAL	24	0
DYNAMICS 365 SALES PREMIUM VIRAL TRIAL	2	0
MICROSOFT COPILOT FOR SERVICE (PREVIEW)	4	0
MICROSOFT COPILOT STUDIO VIRAL TRIAL	4	0
MICROSOFT FABRIC (FREE)	66	0
MICROSOFT POWER APPS FOR DEVELOPER	25	0
MICROSOFT POWER APPS PLAN 2 TRIAL	64	0
MICROSOFT POWER AUTOMATE FREE	69	0
MICROSOFT TEAMS EXPLORATORY	2	0
POWER PAGES VTRIAL FOR MAKERS	3	0
RIGHTS MANAGEMENT ADHOC	1	0
Total(합계)	403	6,639,401

월별 라이선스 사용자 현황

월	활성 사용자 수
5	372
6	351
7	360
8	371
9	383
10	385
11	403
12	403

라이선스 분포 현황 Top 5

라이선스	비중
MICROSOFT POWER APPS FOR DEVELOPER	21.63%
MICROSOFT FABRIC (FREE)	20.69%
POWER BI PRO	7.84%
MICROSOFT POWER AUTOMATE FREE	7.84%
MICROSOFT 365 E5	21.94%

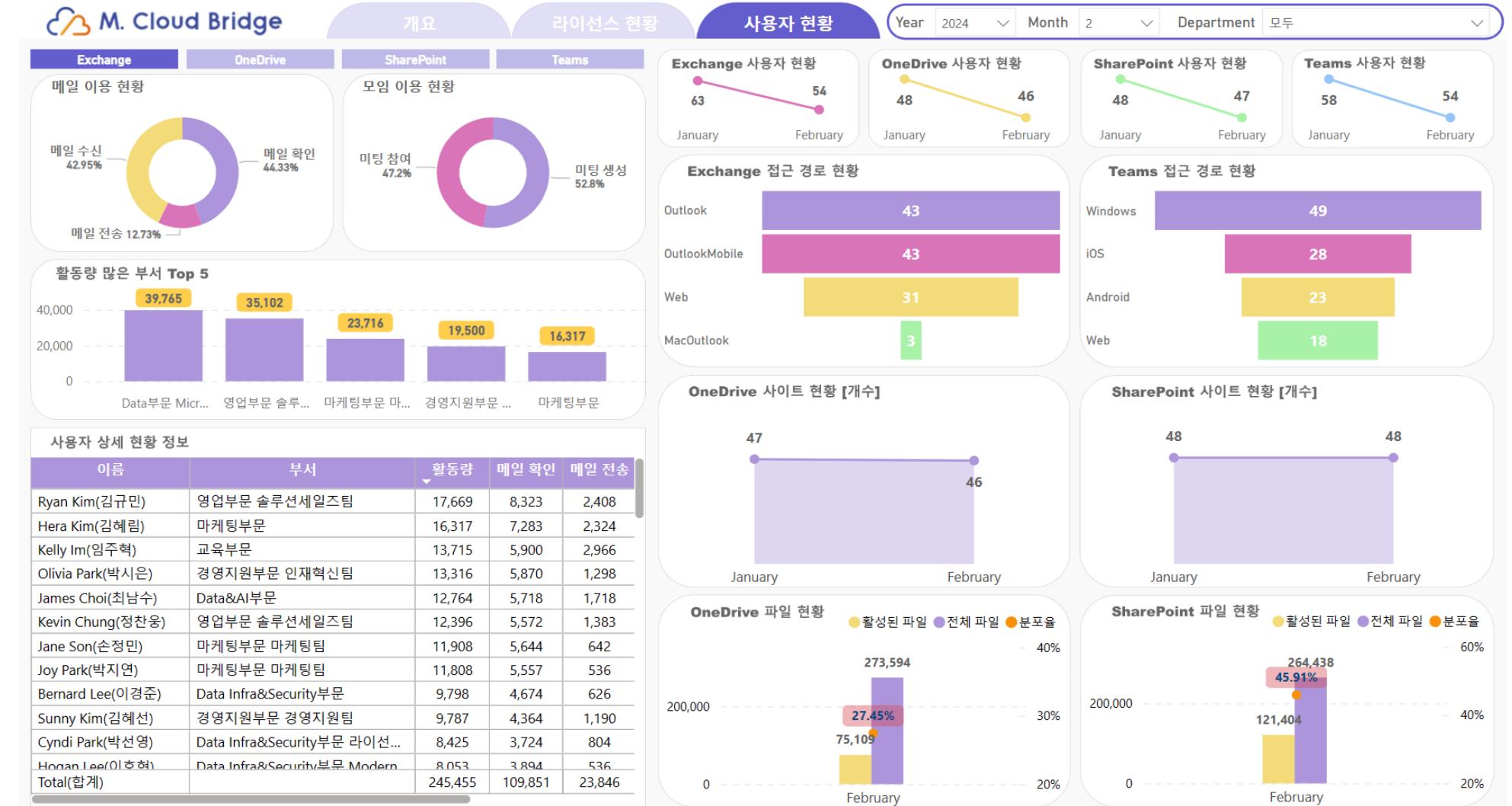
라이선스 활성화 현황 Top 5

라이선스	활성화 수
MICROSOFT 365 E5	70
MICROSOFT POWER AUTOMATE FREE	69
MICROSOFT FABRIC (FREE)	66
MICROSOFT POWER APPS PLAN 2 TRIAL	64
MICROSOFT POWER APPS FOR DEVELOPER	25
POWER BI PRO	25

라이선스 비용 현황 Top 5 [원]

라이선스	비용
MICROSOFT 365 E5	5,390,000
DYNAMICS 365 SALES PROFESSIONAL	526,800
POWER BI PRO	337,500
PROJECT PLAN 5	297,200
VISIO PLAN 2	40,600

Microsoft 365 사용 현황



4

EMS 보안 현황 보고서

EMS 보안 현황 보고서는 Microsoft 365 플랫폼의 보안 현황으로 사용자, 장치 및 보안에 대한 개요 탭을 중심으로 조직의 보안 점수와 취약점 점수 그리고 사용자 계정 활동, 디바이스 관리 현황과 보안 위협 노출 등의 보안 현황을 제공하여 보다 안전한 보안 태세를 지원합니다.

EMS 보안 현황 보고서

M. Cloud Bridge

보안

개요 보안 사용자 디바이스

Year: 2024 Month: 3

오늘의 노출 점수: **34.6**

오늘의 보안 점수: **439.0**

심각성: 6.45% (High), 16.13% (Medium), 77.42% (Critical)

취약성 점수: 1074 (보안 권장 사항), 32 (소프트웨어 인벤토리), 49 (취약점)

위험 검색 발생 위치: 쇼어라인, 브레머턴, 시애틀, 벨뷰, 머서아일랜드, 레이크

경고

심각성	상태	사용자	카테고리	소스
Informational	New	brax-kim	CommandAndControl	CustomerTl
Informational	New	intune-machine	CommandAndControl	CustomerTl
Medium	New	hah05106	DefenseEvasion	WindowsDefenderAtp
Medium	New	hbd09193	DefenseEvasion	WindowsDefenderAtp
Informational	New	jackson-kim	DefenseEvasion	WindowsDefenderAv
Low	New	jeannie-park	Discovery	WindowsDefenderAtp
Medium	New	james-choi	Execution	WindowsDefenderAtp
Medium	New	jeannie-park	Execution	WindowsDefenderAtp
Medium	New	james-choi	Malware	WindowsDefenderAtp
Medium	New	jeannie-park	Persistence	WindowsDefenderAtp

최근 위험 검색 상태

위험 상태	날짜	위험 수준	사용자	동작
수정됨	2024년 3월 1일 금요일	높음	Hogan Lee(이호현)	로그인
수정됨	2024년 3월 1일 금요일	높음	Lumi Han(한소예)	로그인

최근 위험 사용자 상태

위험 상태	날짜	위험 수준	사용자	상태
수정됨	2024년 3월 1일 금요일	보통	Hera Kim(김혜림)	활성
해제됨	2024년 3월 1일 금요일	보통	Chovy Choi(최영철)	활성

사용자

총 사용자: **31**, 실사용자: **28**, 멤버: **19**

로그인 실패: **19**, 인증 실패: **8**, 위험 사용자: **2**

디바이스

총 디바이스: **179**, 사용 디바이스: **177**

부실 디바이스: **13**, 비관리형 디바이스: **10**, 비규격 디바이스: **15**

시스템

Android, iOS, Windows, Windows Server

위험 노출 수준: **8**

EMS 보안 정보



개요

보안

사용자

디바이스

Year 2024

Month 2

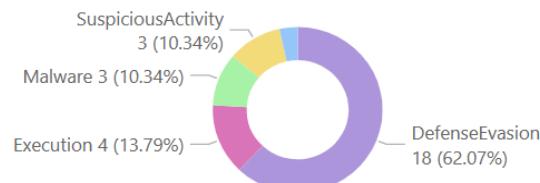
보안 개요

오늘의 노출 점수 오늘의 보안 점수
34.6 **439.0**

보안 권장 사항

소프트웨어	권장 사항
OS	Configuration change
Security controls (Antivirus)	Configuration change
Security controls (Attack Surface Reduction)	Configuration change

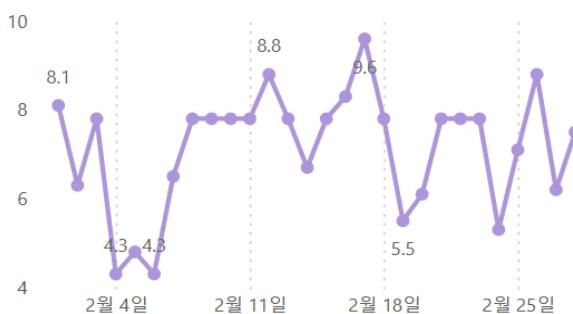
보안 경고 카테고리



보안 위반 사용자

사용자	위험 수준	동작	위험 세부 정보	위치	IP 주소	UPN
Aron Kim(김영민)	높음	내부 규정 위반	사용자가 내부 규정을 위반함	Vancouver - Washington - US	23.155.24.6	aron.kim@mcloudbridge.com
Aron Kim(김영민)	높음	인증 실패	사용자가 다단계 인증을 통과함	Seattle - Washington - US	23.155.24.6	aron.kim@mcloudbridge.com

취약성 점수



취약성 점수 상세

명칭	CVSS v3	심각성
CVE-2023-36541	8.00	High
CVE-2023-3655	7.50	High
CVE-2023-36558	6.20	Medium
CVE-2023-36560	8.80	High
CVE-2023-36562	7.10	High
CVE-2023-36632	5.30	Medium
CVE-2023-36696	7.80	High
CVE-2023-36705	7.80	High
CVE-2023-36719	7.80	High
CVE-2023-36727	6.10	Medium
CVE-2023-36728	5.50	Medium
CVE-2023-36730	7.80	High

보안 위협 경고 상세

상태	DNS	심각성	조사 상태
New	brax-kim	Informational	UnsupportedAlertType
New	brax-kim	Medium	UnsupportedAlertType
Resolved	donny-lee	Informational	SuccessfullyRemediated
New	hah05106	Low	PartiallyInvestigated
New	hah05106	Medium	PartiallyInvestigated
New	hah05106	Medium	TerminatedBySystem
New	hah05106	Medium	UnsupportedAlertType
Resolved	hah05106	Medium	TerminatedBySystem
New	hbd09193	Medium	TerminatedBySystem

EMS 사용자 정보

M. Cloud Bridge

개요 보안 사용자 디바이스

Year: 2023 Month: 3

사용자 개요

총 사용자	실사용자	멤버
31	29	25
로그인 실패	인증 실패	위험 사용자
26	11	2

사용자 로그인 실패 현황

Core Directory	26
Self-service Password Management	2

사용자 로그인 실패 상세

사용자	활동 내역	서비스
lumi.han@mcloudbridge.com	Restore user	Core Directory
lumi.han@mcloudbridge.com	Self-service password reset flow activity progress	Self-service Password Management
lumi.han@mcloudbridge.com	Set user manager	Core Directory
allie.shin@mcloudbridge.com	Update user	Core Directory
allison.lee@mcloudbridge.com	Update user	Core Directory
bernard.lee@mcloudbridge.com	Update user	Core Directory
dani.kim@mcloudbridge.com	Update user	Core Directory
hogan.lee@mcloudbridge.com	Update user	Core Directory
ian.jeong@mcloudbridge.com	Update user	Core Directory

위험 사용자 수준 및 상태

2

사용자 인증 실패

Previously satisfied	27
Password	3
Mobile app notification	1

위험 사용자 상세

사용자	위험 수준	위험 상태	위험 세부 정보	상태	위험 처리 상태
Jackson Kim(김동영)	낮음	수정됨	사용자가 보안 설정된 암호 변경을 수행했습니다.	활성	-
Kathy Jang(장민지)	낮음	해제됨	-	활성	-

사용자 인증 실패 상세

인증 방법	인증 방법 세부 정보	결과 세부 정보
Previously satisfied		First factor requirement satisfied by claim in the token
Previously satisfied		MFA requirement satisfied by claim in the token

EMS 디바이스 정보

M. Cloud Bridge

개요 보안 사용자 디바이스

Year: 2023 Month: 5

디바이스 개요

총 디바이스	사용 디바이스	
179	177	
부실 디바이스	비관리형 디바이스	비규격 디바이스
10	16	16

Defender 온보딩

상태	수
Onboarded	14
Can be onboarded	12
Insufficient info	5

디바이스 위험 노출

노출 레벨	수
High	12
Low	5
Medium	8
No data available	6

부실 디바이스

사용자	디스플레이	조인
Allie Shin(신유지)	WIN-ALLIE22	Azure AD joined
Bernard Lee(이경준)	WIN-APC7ANRMCSA	Azure AD joined
Bernard Lee(이경준)	WIN-DPSTN7THT6U	Azure AD registered
Olivia Park(박시은)	WIN-LSP8G6LLVL0	Azure AD joined
Jake Jeong(정진우)	WIN-TQF8PHI62RJ	Azure AD joined

비관리형 디바이스

사용자	디스플레이	조인
Allison Lee(이윤지)	WIN-3P3UD4OBVO8	Azure AD joined
Bernard Lee(이경준)	samsungSM-S928N	Azure AD registered
Henk Lee	TABLET-5SDDBNA5K	Azure AD registered
Henk Lee	TABLET-QJ8D748L	Azure AD joined
Jake Jeong(정진우)	WIN-TQF8PHI62RJ	Azure AD joined

비규격 디바이스

사용자	디스플레이	조인
Jake Jeong(정진우)	WIN-TQF8PHI62RJ	Azure AD joined
Kaylee Oh(오아영)	Kaylee-Oh	Azure AD joined
Kelly Im(임주혁)	KELLY-IM	Azure AD joined
Lara Lee(이민선)	LARA-LEE	Azure AD joined
Olivia Park(박시은)	WIN-LSP8G6LLVL0	Azure AD joined

Defender 설치 현황

상태	수	퍼센트
Unknown	14	(45.16%)
Not Supported	17	(54.84%)

Defender OS 종류

OS 종류	수
Windows	26
Android	3
iOS	2

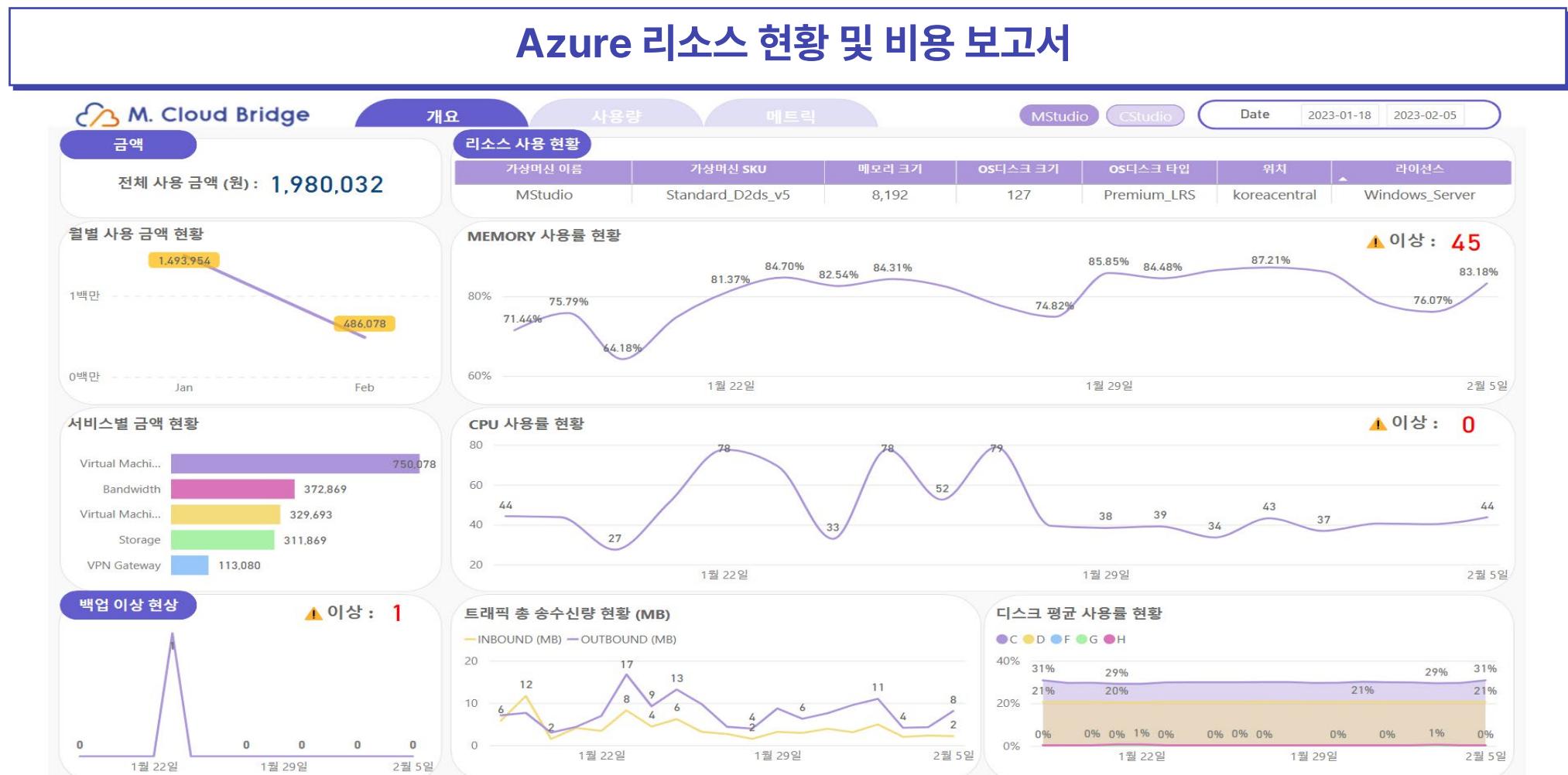
디바이스 위험 노출 상세

노출 레벨	디바이스	백신
High	alan-kim	Not Supported
High	book-49ctfcjsg9	Not Supported
High	dani-kim	Not Supported
High	desktop-fvg2lv8	Not Supported
High	desktop-rb7bpfp	Not Supported
High	intune-test	Not Supported
High	jackson-kim	Not Supported

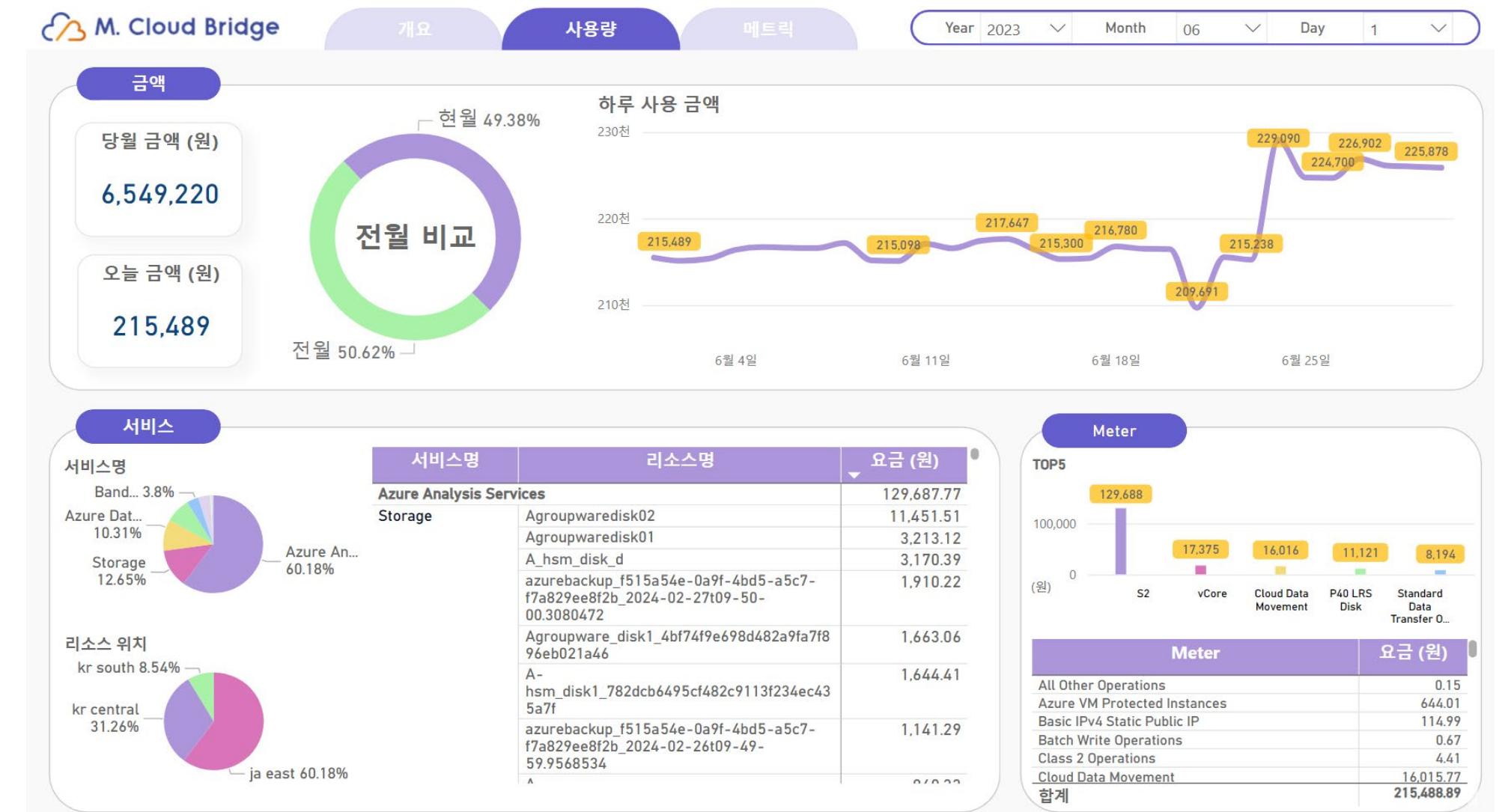
5

Azure 리소스 현황 및 비용 보고서

Azure 리소스 현황 및 비용 보고서는 사용중인 Azure 리소스의 사용량과 요금을 확인 할 수 있는 개요 탭을 중심으로, 리소스 사용 요금 지표와 CPU, RAM, Disk 등의 리소스 메트릭 정보를 제공함으로써 서비스의 운영 현황과 리소스별 비용 현황을 확인하도록 지원합니다.



Azure 사용량 정보



Azure 메트릭 정보

M. Cloud Bridge

개요 사용량 메트릭

Year: 2023 Month: 12 Day: 8

가상머신 이름	가상머신 SKU	메모리 크기	OS 디스크 크기	OS 디스크 탑업	위치	라이선스
CStudio	Standard_D2ds_v5	8,192	127	Premium_LRS	koreacentral	Windows_Server

가상머신

MStudio CStudio

DISK

DISK	C	D	F	G	H
디스크 용량	126.45 GB				
정상	C				
주의					
위험					
40	0	0	0	0	0

최신 디스크 사용률

DISK	사용률
C	29.09%
D	20.49%
F	0.22%
G	0.22%
H	0.70%

MEMORY

▲ 위험 0 주의 496

시간 사용률(MB)

시간	사용률(MB)	사용률
2023-12-08 오후 3:16:00	7,307	89.20%
2023-12-08 오후 3:17:00	7,222	88.16%
2023-12-08 오후 2:42:00	7,196	87.84%
2023-12-08 오후 3:49:00	7,189	87.76%
2023-12-08 오후 3:15:00	7,170	87.52%
2023-12-08 오후 2:18:00	7,168	87.49%
2023-12-08 오후 4:03:00	7,165	87.46%
2023-12-08 오후 3:50:00	7,148	87.26%

CPU

▲ 위험 0 주의 0

시간 사용률

시간	사용률
2023-12-08 오전 12:00:00	5.39
2023-12-08 오전 12:01:00	5.34
2023-12-08 오전 12:02:00	7.44
2023-12-08 오전 12:03:00	5.47
2023-12-08 오전 12:04:00	5.10
2023-12-08 오전 12:05:00	4.81
2023-12-08 오전 12:06:00	5.41
2023-12-08 오전 12:07:00	5.11

NETWORK

총 수신량 2.8MB 총 송신량 10.8MB

시간 트래픽 수신량(B) 트래픽 송신량(B)

시간	트래픽 수신량(B)	트래픽 송신량(B)
2023-12-08 오전 12:00:00	856.55	2,488.84
2023-12-08 오전 12:01:00	945.48	3,614.87
2023-12-08 오전 12:02:00	1,147.24	2,853.67
2023-12-08 오전 12:03:00	980.12	2,917.68
2023-12-08 오전 12:04:00	667.30	2,493.56
2023-12-08 오전 12:05:00	814.49	2,803.61
2023-12-08 오전 12:06:00	668.49	2,465.70

BACKUP

▲ 이상 1

백업 시작 시간 백업 완료 시간 백업 소요 시간 상태

백업 시작 시간	백업 완료 시간	백업 소요 시간	상태
2023-12-02 오후 10:57:00	2023-12-03 오전 2:07:00	190분	Completed
2023-12-03 오후 9:00:00	2023-12-04 오전 2:08:00	308분	Completed
2023-12-04 오후 9:01:00	2023-12-05 오전 2:09:00	308분	Completed
2023-12-05 오후 9:02:00	2023-12-06 오전 2:10:00	308분	Completed
2023-12-07 오후 9:04:00	2023-12-08 오전 2:12:00	308분	Completed
2023-12-08 오후 9:05:00	2023-12-09 오전 2:13:00	308분	Completed
2023-12-09 오후 9:06:00	2023-12-10 오전 2:14:00	308분	Completed

27

Copilot 기능과 적용을 위한
필수 보안 기능
Microsoft Security(EMS)

엠클라우드브리지
이경준 부문장



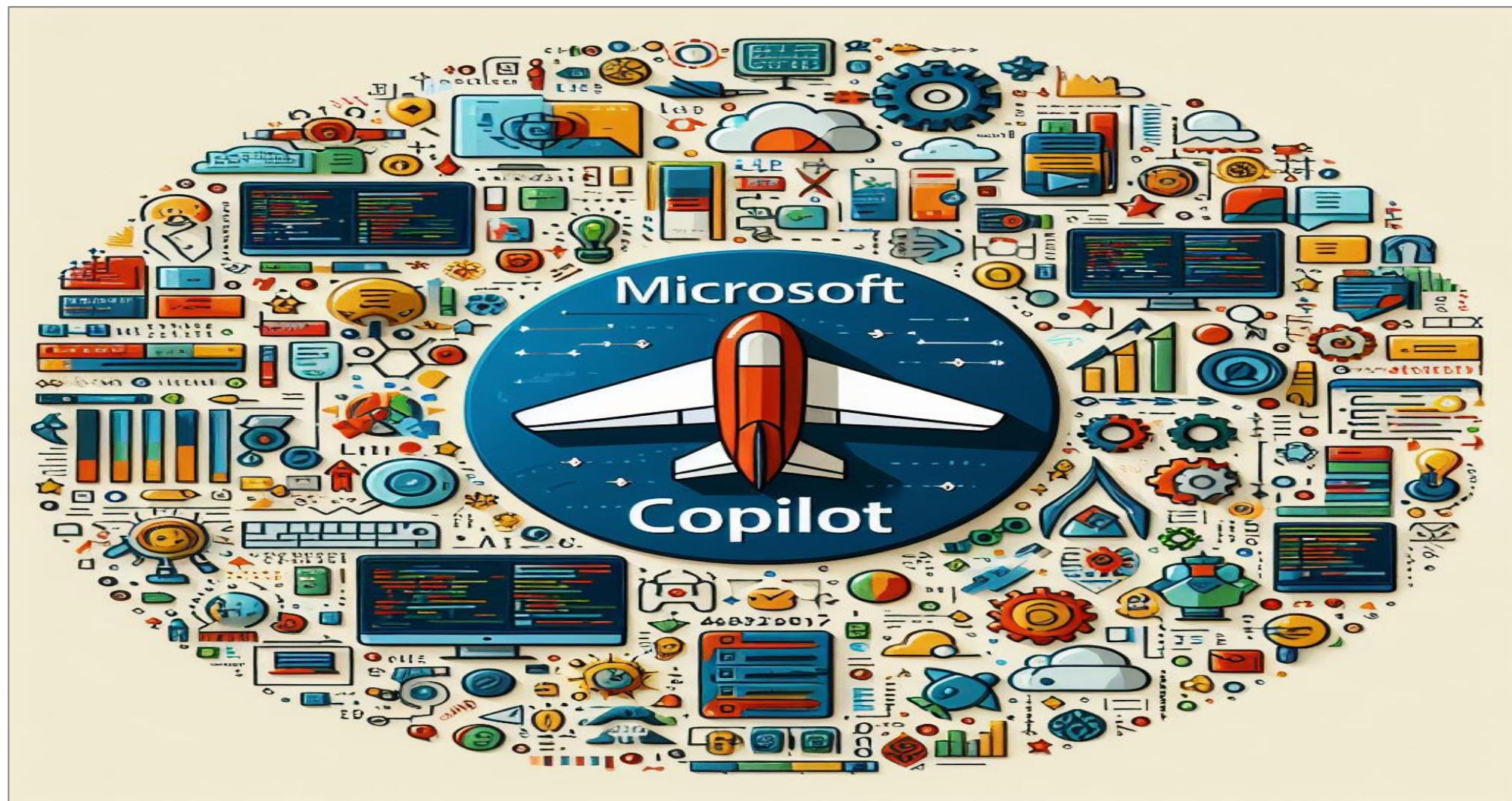
Agenda

1. Copilot 소개
2. Microsoft Copilot
3. Windows Copilot
4. Microsoft 365 Copilot
5. Microsoft Security(EMS)
6. Security Copilot
7. 결론

1

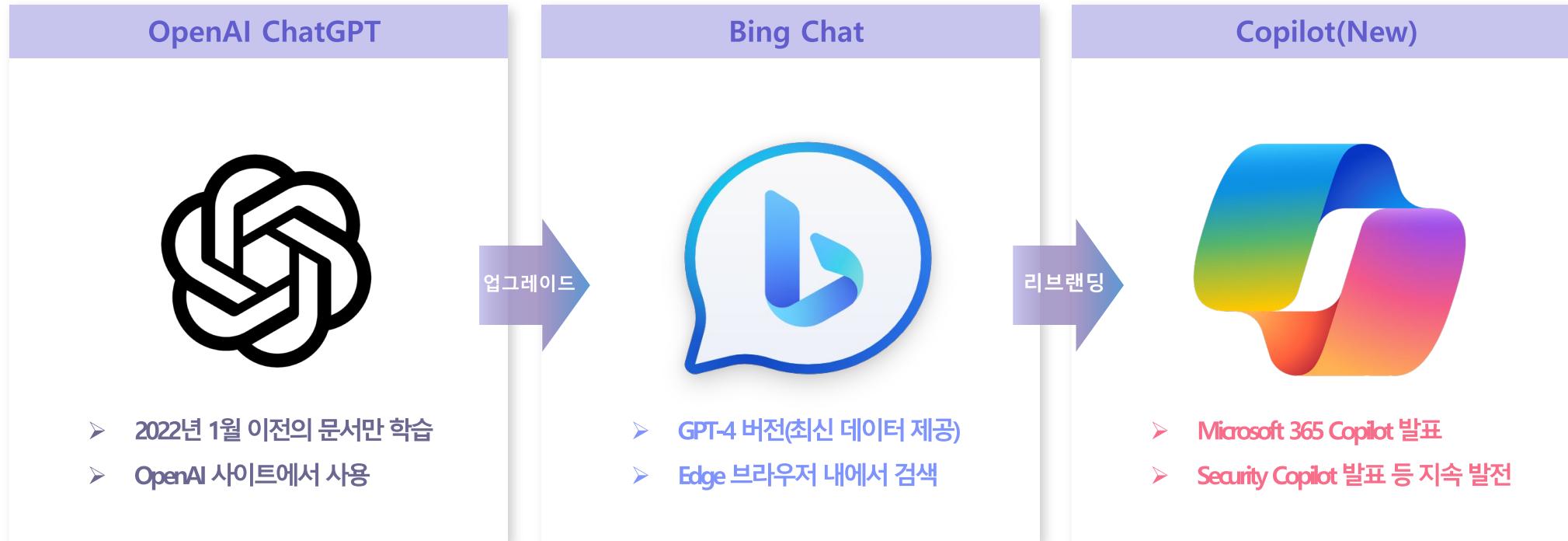
Copilot 소개

Copilot 소개



Copilot의 탄생은 2022년 1월 까지의 데이터로 훈련 되어 있는 ChatGPT(GPT3.5)와 더 발전된 기술인 GPT4 기반의 최신 데이터 정보를 실시간으로 제공할 수 있는 Bing Chat으로 업그레이드 되고, 이후 MS의 정책에 따라 Copilot으로 리브랜딩 되며 발전을 지속 하고 있습니다.

Copilot의 탄생



업그레이드 되는 엔진의 성능과 Sales / Microsoft 365 / Security 등 지속적인 기능 및 플랫폼 확장

Copilot의 기능은 인터넷 상의 다양한 데이터를 기반으로 창의적인 아이디어를 활용한 문서, 이메일, 프레젠테이션의 초안 작성과 다양한 데이터 내용을 요약 정리해주며, 사용자 대신 시스템을 제어하거나 비즈니스 데이터의 보안에 대한 지침과 분석을 사용자에게 제공합니다.

Copilot의 기능



신속한 의사결정을
돕는 인공지능 도우미

- ✓ 편리한 웹 검색 및 창의적인 이미지 제공

간단명료한 자료조사와 AI기반의 창의적인 이미지 제공



손쉬운 컴퓨터 제어

주 업무에만 집중할 수 있도록 컴퓨터 시스템 제어



업무 환경의 협업 및 커뮤니케이션 조력

효율적인 협업 및 커뮤니케이션 기능 제공



보안 정밀 분석

조직 내 복잡하고 다양한 보안 로그를 대신 분석

Copilot Platform 종류는 인터넷 기반의 검색 기능인 Microsoft Copilot, 윈도우 사용과 시스템 제어에 도움을 주는 Windows Copilot, 비즈니스 업무 생산성을 높여주는 Microsoft 365 Copilot과 사내 보안 이벤트의 관리 및 분석을 지원하는 Security Copilot 이 있습니다.

Copilot Platform 종류

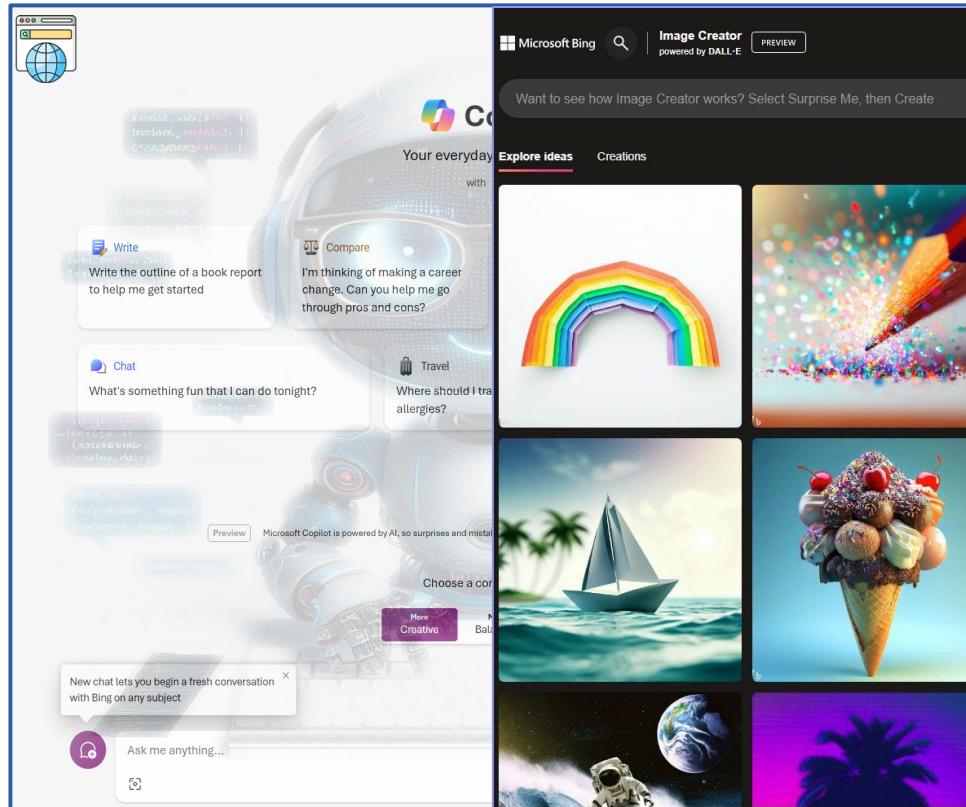
Microsoft Copilot	Windows Copilot	Microsoft 365 Copilot	Security Copilot
 Bing Chat	 Windows 11	 Microsoft 365 Copilot	 Security Copilot
Edge 브라우저 사이드바에서 인공지능 기능 액세스 	윈도우 운영체제 내 서비스 AI 도우미 역할 (Preview) 	Microsoft 365 App 업무 효율을 위한 인공지능 보조 역할 	대규모 데이터와 위협 인텔리전스를 활용해 보안 관리 
<ul style="list-style-type: none">* 인터넷에서의 복잡하고 포괄적인 답변을 찾고 요약된 정보를 제공* 텍스트, 전자 메일, 소셜 미디어 게시물 또는 아이디어를 생성	<ul style="list-style-type: none">* 사용자 대상 윈도우 사용과 제공 프로그램 액세스 접근 도움* PDF 문서 파일의 내용 요약과 문서 작성 기능 제공	<ul style="list-style-type: none">* 사용자를 위해 워드 문서의 글을 요약하거나 창작* 간단한 명령만으로 아이디어를 디자인된 프레젠테이션으로 전환* 인사이트 확보, 동향 파악, 전문적인 데이터 시각화	<ul style="list-style-type: none">* 특정 사용자 또는 이벤트와 관련된 감사 로그를 자연어로 요약해보안 분석에 대한 인사이트를 제공* 조직의 외부 공격 대상에 연결해 위험에 대한 최신 정보를 식별하고 분석

2

Microsoft Copilot

Microsoft Copilot은 기존의 OpenAI의 GPT-4 Turbo 기반 채팅 플랫폼에서 검색 플랫폼인 Bing과 만나 사용자 프롬프트를 더욱 폭넓게 이해하고 웹 검색을 통해 더욱 많은 정보를 수집 및 가공하여 사용자에게 알맞은 답변을 생성하거나 창의적인 AI 이미지를 무료 제공합니다.

What is Microsoft Copilot

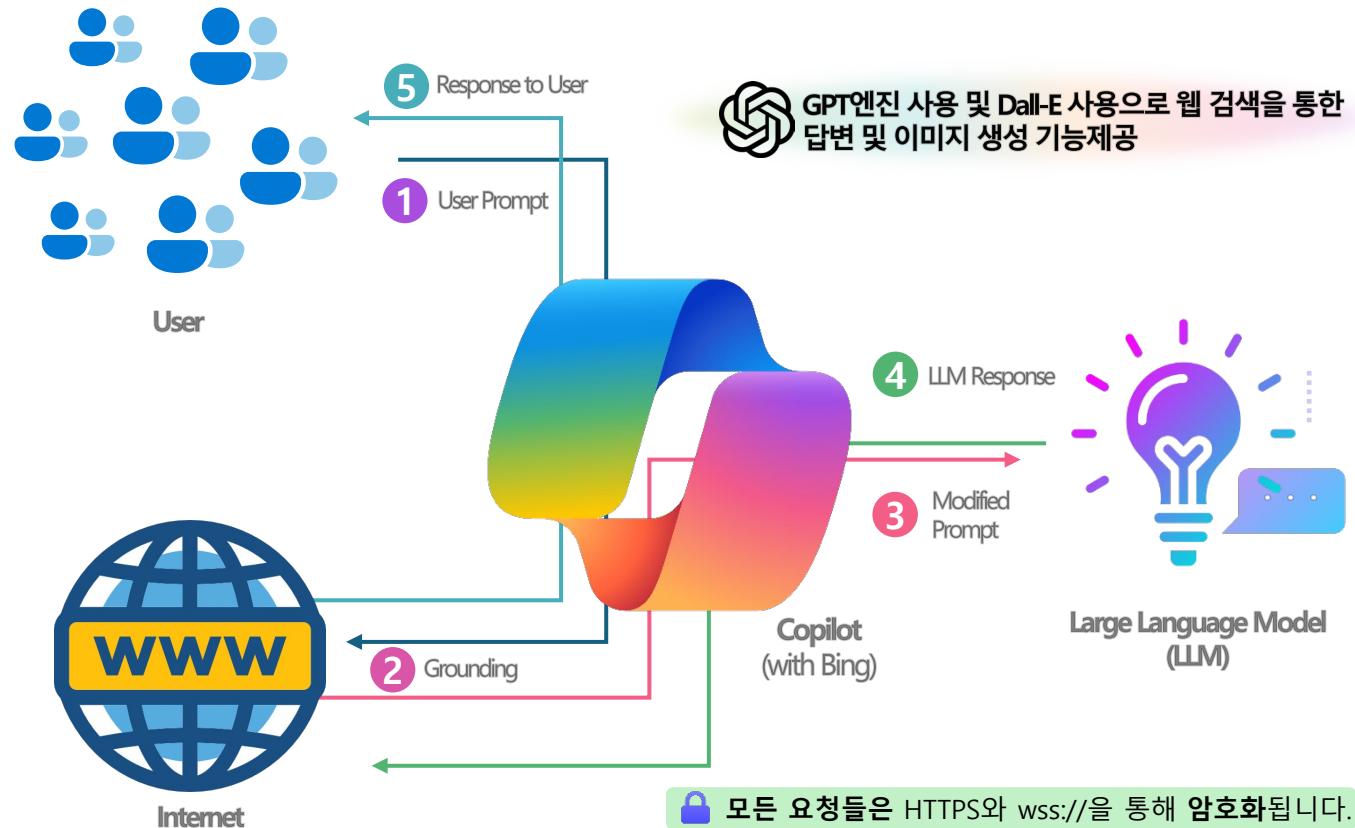


웹을 검색할 때마다 업무 보조원, 플래너처럼 사용자가 해야 할 일에 대한 창의적인 아이디어와 유용한 답변을 신속하게 제공

- ① 웹 또는 모바일 및 Windows, Edge 및 Bing에서 Copilot에 액세스할 수 있습니다.
- ② 텍스트, 음성, 이미지를 사용하여 인공지능 Copilot에게 필요한 정보를 질의하고 답변 받을 수 있습니다.
- ③ Designer(이전의 Bing Image Creator)에서 매일 15개의 부스트로 이미지를 더 빠르게 만들 수 있습니다.
- ④ 문서 및 웹 페이지를 요약할 수 있습니다.
- ⑤ 확장 플러그 인 및 Copilot GPT를 결합하여 사용할 수 있습니다.

Microsoft Copilot의 동작 방식은 사용자가 명령 프롬프트에 질의에 대한 내용을 Copilot에게 질의하고, 데이터 조사를 위해 인터넷에 그라운딩하여 AI가 질의의 내용을 이해하고 답변을 생성할 수 있도록 LLM 자연어 처리한 뒤, 내용 취합하여 사용자에게 전달하게 됩니다.

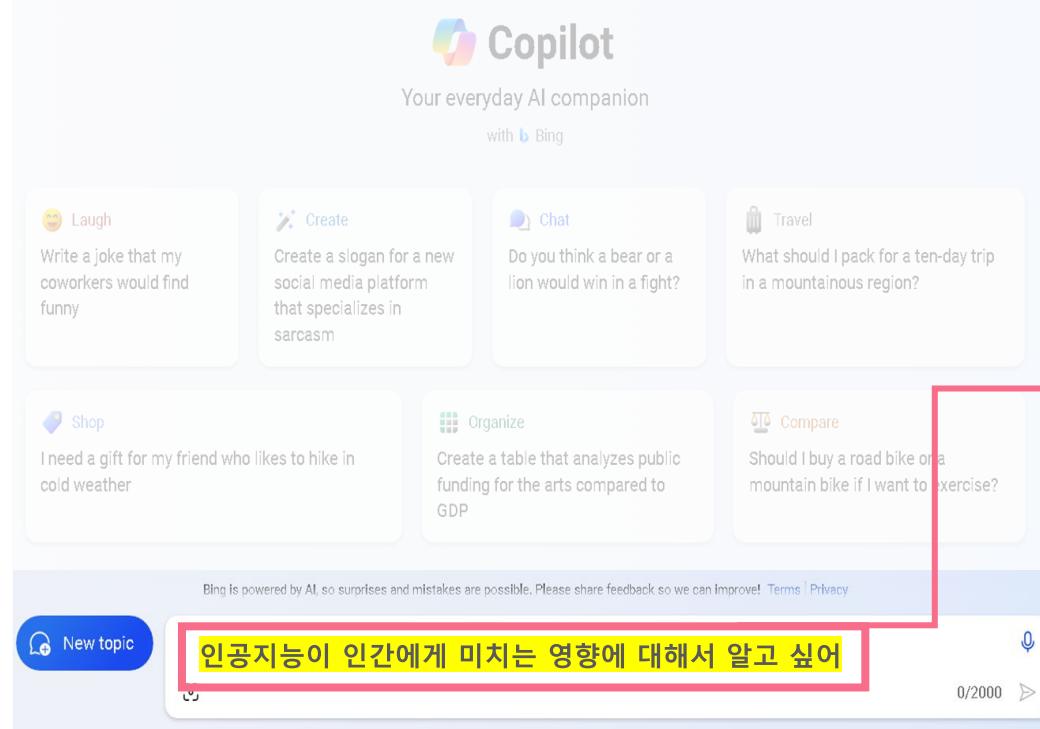
Microsoft Copilot 동작 방식



Microsoft Copilot의 예시는 사용자는 명령 프롬프트에 복잡하고 다양한 주제에 대해 Copilot에게 대신 내용을 조사, 정리할 수 있도록 지시하게 되면 사용자의 지시 내용을 기반으로 Microsoft Copilot은 수많은 데이터를 신속하게 취합하고 정리한 내용으로 최종 전달합니다.

Microsoft Copilot 예시

복잡하고 다양한 주제로 조사 지시



Microsoft Copilot 내용 전달

Copilot

인공지능 기술은 빠르게 발전하고 있으며, 그 영향력은 우리의 삶과 사회 전반에 깊은 변화를 가져오고 있습니다. 이에 따라 우리는 인공지능의 미래에 대한 이해와 대비가 필요합니다. 다음은 인공지능이 사회에 미치는 영향을 살펴보겠습니다:

1. 인공지능의 미래 전망:

- 기술 발전과 산업 변화:** 인공지능 기술은 지속적으로 발전하고 있으며, 자율 주행 자동차, 의료 진단 및 치료, 공장 자동화 등 다양한 분야에서 혁신적인 변화가 예상됩니다.
- 사회적 경제적 파급효과:** 높은 생산성과 효율성으로 인해 일부 직종은 자동화되고, 이로 인해 일자리의 감소가 우려됩니다. 그러나 동시에 새로운 일자리가 창출될 것으로 예상되며, 이러한 변화는 교육, 노동시장, 사회보장 등 다양한 분야에 영향을 미칠 것으로 보입니다.

2. 일자리와 경제적 영향:

- 일자리 변화와 새로운 직업의 등장:** 인공지능 기술의 발전은 일자리 구조에 변화를 가져올 것으로 예상됩니다. 단순 노동력이 필요한 업무는 자동화될 가능성이 높으며, 이에 따라 일부 직종은 사라질 수 있습니다.

Microsoft Copilot Designer의 예시는 사용자는 명령 프롬프트를 통해 희망하는 다양한 이미지의 특성을 입력하여 창의적인 이미지를 생성하도록 지시하게 되면 배경, 문구, 얼굴 표정 혹은 예술 스타일과 같은 세부 특성을 인식하여 단 몇 초 만에 이미지를 생성할 수 있습니다.

Microsoft Copilot Designer 예시

복잡한 아이디어의 그림 제작 질의

Copilot | Designer

AI를 사용하여 단어에 서 이미지 만들기

인공지능 로봇이 인공지능 로봇을 만드는
그림을 인상주의적으로 그려줘

가입 및 만들기

Designer의 Image Creator는 AI를 사용하여 단어를 기반으로 이미지를 생성하는 데 도움이 됩니다. 자세히 알아보세요.

Microsoft 및 파트너 제품의 제작이 포함된 Microsoft Rewards 관련 전자 메일을 받게 됩니다. 또한 Designer로부터 Image Creator 관련 알림도 받게 됩니다. 계속 진행하면 아래의 Rewards 악관 및 Image Creator 악관에 동의하는 것으로 간주합니다.

[개인 정보](#) | [Rewards 악관](#) | [Image Creator 악관](#)

검색, 채팅 및 만들기를 모두 한 곳에서 사용할 수 있습니다.
새 Bing에서 Image Creator를 사용해 보세요.

AI로부터 창의적인 이미지 생성



3

Windows Copilot

Windows Copilot은 Windows 11 컴퓨터 환경에서 제공되는 생성형 AI 지능형 도우미로, 사용자는 인터넷 브라우저 실행 없이 콘텐츠 검색, 창의적인 이미지 생성 및 Windows 시스템 제어와 같은 업무를 손쉽게 지시하여 보다 향상된 업무의 생산성과 효율성을 제공합니다.

What is Windows Copilot



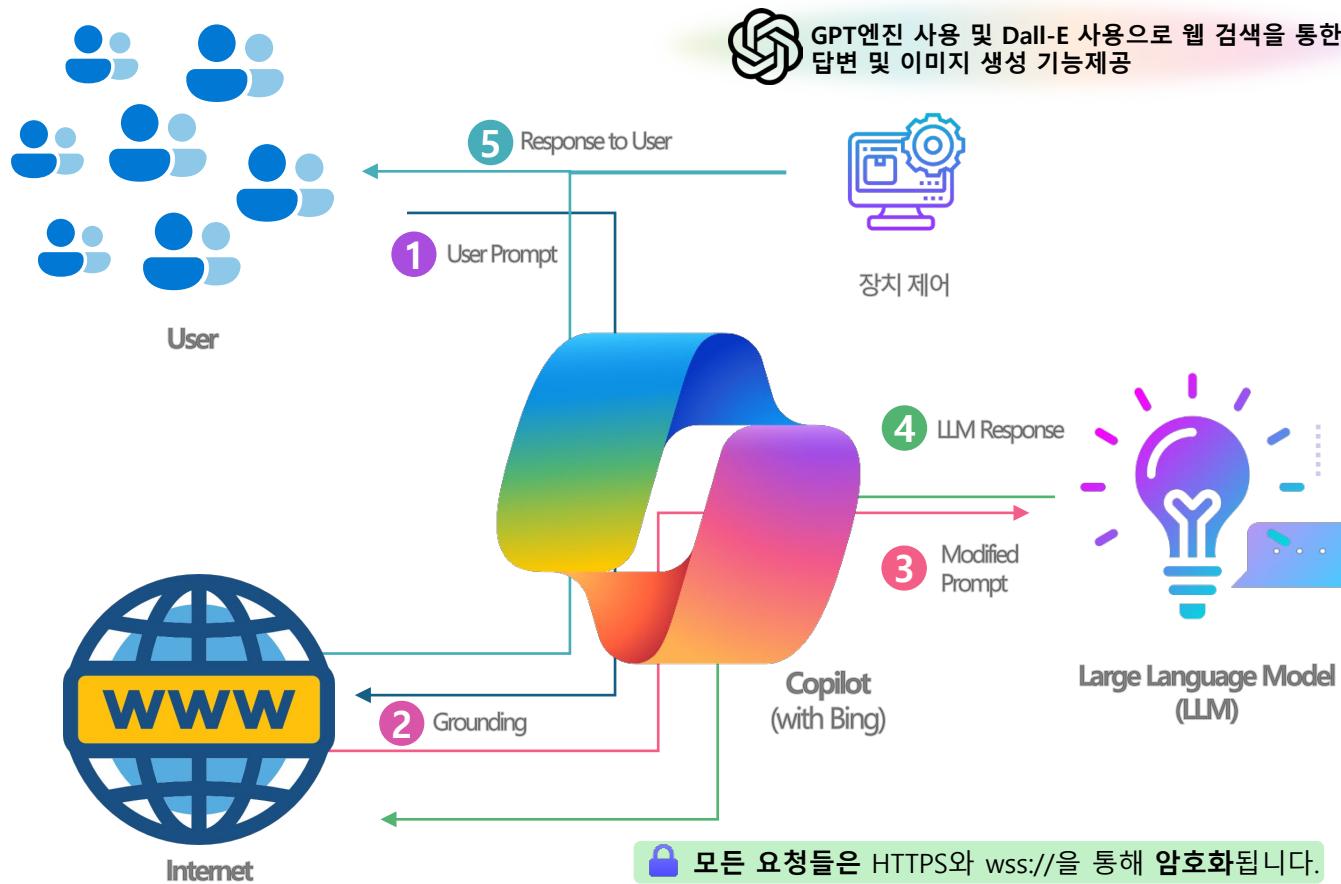
Windows Copilot은 Windows 11에서 제공되는 AI 기반 지능형 도우미로 시스템 제어와 콘텐츠 검색, 창작을 손쉽게 지시하고 현재 진행 중인 작업에 더 집중할 수 있게 해줍니다.

주요 특징

1. PC 설정 조정, 끌기 도우미로 창 정리 등의 번거로운 작업을 처리해 주므로 중요한 작업에만 집중할 수 있게 해줍니다.
2. Windows Copilot은 Bing Chat에 연결하여 참신한 아이디어와 질문에 관련된 유용한 정보를 수집하여 빠르게 확인하고 후속 질문을 할 수 있습니다.

Windows Copilot 동작 방식은 사용자 명령어 프롬프트가 Bing Chat을 통해 질의를 입력하면 Copilot은 인터넷 정보를 그라운딩하고, LLM 자연어 처리를 거쳐 이에 해당되는 응답을 인터넷 또는 윈도우 시스템 명령으로 접근하여 사용자에게 반환하는 방식으로 진행됩니다.

Windows Copilot 동작 방식



- 1 Copilot 프롬프트 입력**
사용자의 프롬프트가 Bing Chat를 통해 Copilot에 전달됩니다.
- 2 사용자 명령 검색**
사용자의 프롬프트를 그라운딩 합니다.
- 3 LLM 자연어 처리**
Copilot이 수정된 프롬프트를 LLM에 전달합니다.
- 4 Copilot 체크 및 리뷰**
Copilot이 LLM 응답의 체크 및 리뷰를 위해 Web 또는 시스템 명령으로 접근합니다.
- 5 사용자 응답 반환**
사용자에게 답변 및 시스템 명령 실행을 전달합니다.

Windows Copilot의 예시로 사용자는 명령 프롬프트를 통해서 Copilot에게 윈도우 시스템의 설정을 명령어로 제어 할 수 있으며, 추가로 Microsoft Copilot의 기능과 동일하게 웹 검색 또는 이미지 생성 등의 기능을 제공하여 Windows 사용자에게 더 넓은 경험을 제공합니다.

Windows Copilot 예시

1. Windows Copilot 명령

나
시스템 볼륨을 음소거 해줘

Copilot
사용:

볼륨 음소거/음소거 해제
기본 오디오 장치를 (음소거하거나 음소거 해제)하시겠어요?

Yes, proceed **No, thanks**

볼륨을 음소거하려면 대화 상자를 사용하여 선택을 확인할 수 있습니다.

참고 자료: bing.com

1 / 30 응답

① 대신 웹에서 응답
볼륨을 어떻게 음소거하나요?
다른 기능도 있나요?
감사합니다.

2. Windows Copilot 명령

나
고양이가 하늘에서 공놀이 하는 그림을 사실주의로 그려줘

Copilot
그림을 그려드리겠습니다.

이미지가 생성되고 있습니다.

80%

② 고양이가 별을 쫓는 그림으로 바꿔줘.
그림에 구름도 추가해주세요.
다른 동물들과 함께 공놀이하는 그림은 어떨까요?

DALL-E 3에서 구동

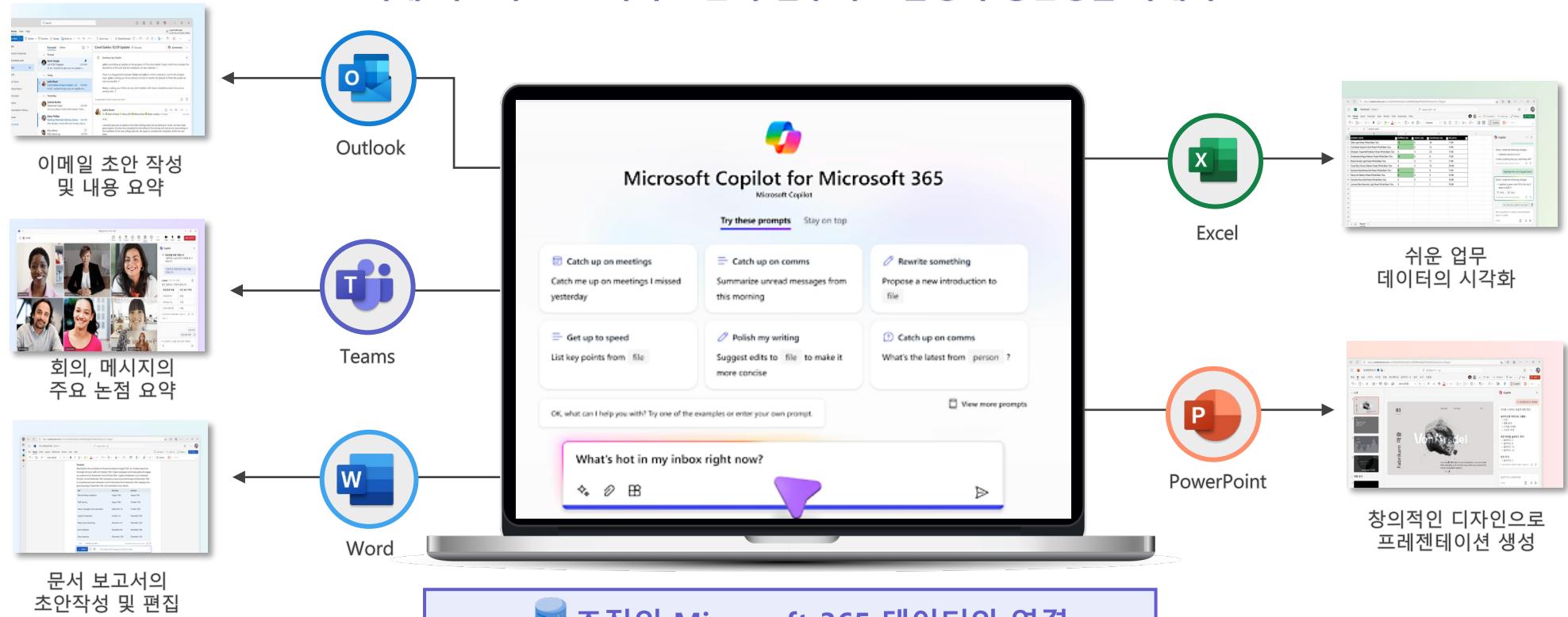
4

Microsoft 365 Copilot

Microsoft 365 Copilot는 사내 Microsoft 365 비즈니스 데이터와 연결되어 워드 보고서, 엑셀 데이터, 이메일 및 프레젠테이션 발표 자료를 창의적으로 작성하고 편집할 수 있으며, 회의에서 주고 받은 내용을 요약하여 조직 내 업무 생산성을 극대화할 수 있도록 지원합니다.

What is Microsoft 365 Copilot

사내 비즈니스 AI 비서로 문서 업무의 효율성과 생산성을 극대화



Microsoft 365 Copilot 기능은 데이터 입력, 문서 및 이메일 작성, 프레젠테이션 편집이나 다량의 데이터를 분석하고 요약해주거나 창의적인 아이디어를 도출하며 누락될 수 있는 일정 및 메일 관리를 지원하고 다양한 애플리케이션 별로 작업을 자동화할 수 있습니다.

Microsoft 365 Copilot 기능

문서 작성 및 분석의 효율성

- ▶ 문서 및 프레젠테이션 작업 시간 단축
- ▶ 신속한 다량의 데이터 분석, 요약

향상된 커뮤니케이션

- ▶ 수많은 메일, 일정의 손쉬운 관리
- ▶ 다양한 상황 별 발생되는 커뮤니케이션 방법 제공

최적화된 업무 및 자동화

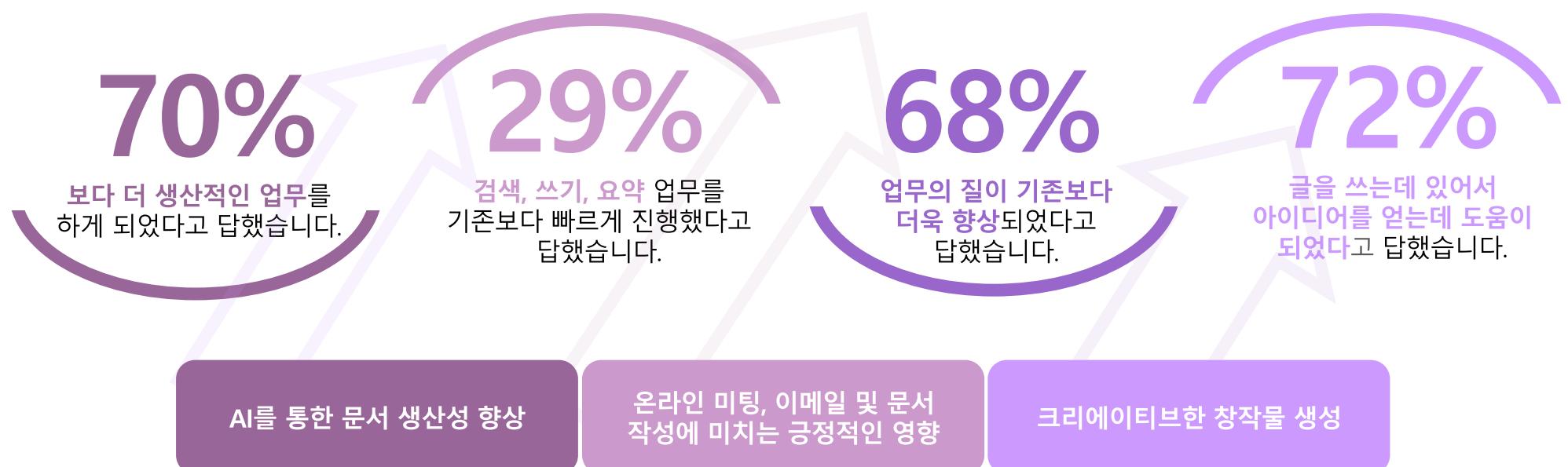
- ▶ 다양한 애플리케이션의 작업 자동화
- ▶ 역할 업무에 최적화된 워크플로 정의

창의성과 혁신 촉진

- ▶ 문서, 프레젠테이션 디자인, 혁신적인 아이디어
- ▶ 일상적인 작업 최소화

Microsoft 365 Copilot 사용으로 사용자는 수동적인 문서 작업 시간을 단축시킬 수 있었으며 다양한 데이터 조사와 분석에서 발생되는 단순 작업의 피로를 줄이고 AI 기반의 창의적인 아이디어를 쉽게 도출해낼 수 있었기 때문에 사용자의 업무 생산성이 크게 향상되었습니다.

Microsoft 365 Copilot 사용으로 인한 사용자 업무 생산성 향상



Copilot을 응용한 업무의 제안 및 자동화로 새로운 업무 방식을 도입 및 생산성 향상

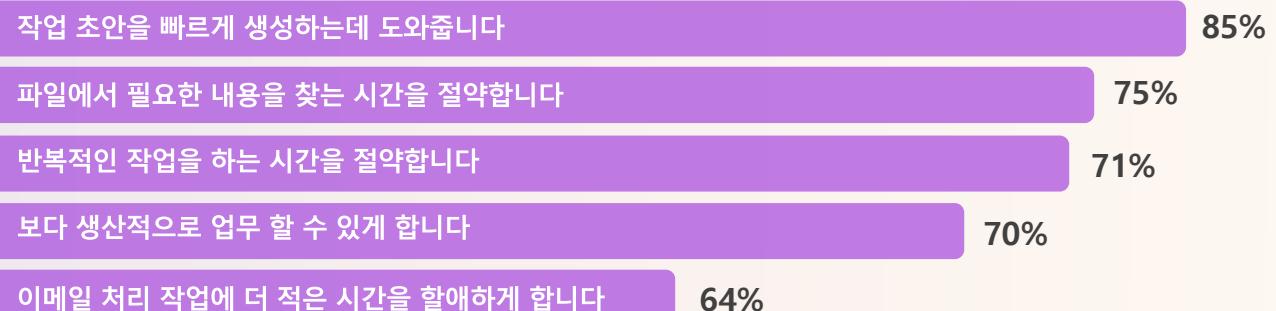
Microsoft 365 Copilot 도입에 따른 업무 개선은 기존의 수동적이고 비효율적인 업무 환경을 새롭게 변화시켰으며, 반복적인 단순 업무를 자동화하고 창의적인 아이디어를 쉽게 도출하거나 사용자가 주 업무에 더 많은 시간을 할애하여 보다 집중 할 수 있는 결과를 제공합니다.

Microsoft 365 Copilot 도입에 따른 업무 개선



사람들을 더 생산적이고
창조적이게 만들고
업무 시간을 절약합니다

▶ 작업의 생산성과 속도



▶ 업무의 질과 창의적인 아이디어

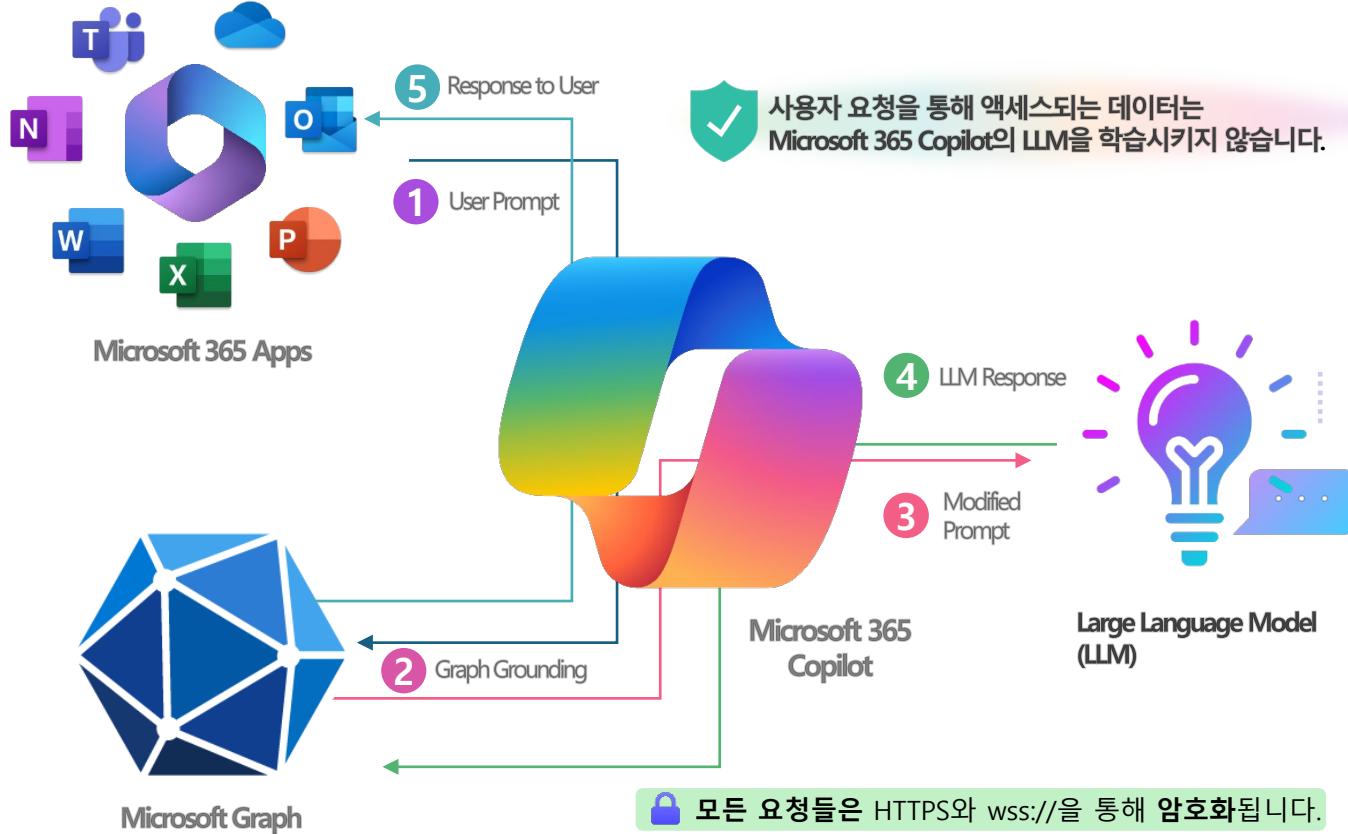


▶ 업무 집중 시간



Microsoft 365 Copilot의 동작 방식 프롬프트를 통해 질의를 하면, Copilot은 비즈니스 데이터에 접근하기 위해 Microsoft Graph에 그라운딩하고 LLM 자연어 처리를 진행한 후에 이에 해당되는 응답을 다시 전달하여 사용자에게 답변을 하는 동작 방식으로 되어 있습니다.

Microsoft 365 Copilot 동작 방식



1 Copilot 프롬프트 입력
사용자의 프롬프트가 Apps를 통해 Copilot에 전달됩니다.

2 Microsoft Graph 인덱싱
그라운딩을 위해 Copilot이 Microsoft Graph에 접근합니다.

3 LLM 자연어 처리
Copilot이 수정된 프롬프트를 LLM에 전달합니다.

4 Copilot 체크 및 리뷰
Copilot이 LLM 응답의 체크 및 리뷰를 위해 Microsoft Graph 데이터에 접근합니다.

5 사용자 응답 반환
사용자에게 답변을 전달합니다.

App별 Microsoft 365 Copilot은 Excel, Word, PowerPoint에서 사용자의 데이터를 기반으로 문서의 초안 작성, 편집, 내용 요약을 신속하게 진행시킬 수 있으며 Outlook에서 메일 초안을 작성해주거나 OneNote에서 사용자의 할 일과 메모 정리를 지시할 수 있습니다.

App별 Microsoft 365 Copilot



Copilot in Excel

간편한 데이터 분석, 이해, 시각화



Copilot in Outlook

받은 편지함 확인 및 후속 조치 관리



Copilot in OneNote

할 일과 메모를 손쉽게 정리



Copilot in Word

문서의 작성, 이해, 개선



Copilot in Teams

모든 채팅, 모임, 통화를 빠르게 파악



Copilot in PowerPoint

아이디어를 멋진 프레젠테이션으로 구현

사용자를 위한 Microsoft 365 Copilot 활용으로 사용자는 고객사에서 수신 되었던 메일과 채팅 메시지를 관리하거나 초안 작성하고, 회의 내용을 정리하여 참여자들의 기여도를 파악할 수 있으며 사용자의 Office 문서를 기반으로 창의적인 생산물을 쉽게 작성할 수 있습니다.

사용자를 위한 Microsoft 365 Copilot 활용



Microsoft 365 Chat

"Summarize all the emails and chats that mentioned project in the last 2 hours"

지난 2시간 동안 프로젝트를 언급한 모든 이메일과 채팅을 요약해줘



Copilot in Teams

"Did everyone who attended the call contribute to the discussion?"

통화에 참석한 모든 사람이 토론에 기여했습니까?



Copilot in Excel

"Add a column to calculate the average of the different columns for each month"

각 달마다 다른 열들의 평균을 계산하는 열을 추가해줘



Copilot in Outlook

"We apologize for the product issue and reply to the email in a professional tone that we will respond by 3 p.m. today"

제품 문제에 대해 사과 드리며 오늘 오후 3시 까지 답변을 드리겠다는 이메일을 전문적인 어조로 회신해줘



Copilot in Word

"Please add a new paragraph based on the 23-year Contoso bonus plan for the financial year"

재무연도 23년의 Contoso 보너스 플랜에 기반하여 새 단락을 추가해줘



Copilot in PowerPoint

"Please make a draft PPT using the Word document on Project Contoso product design guidelines"

Project Contoso 제품 디자인 지침에 대한 Word 문서를 활용하여 초안으로 PPT 만들어줘

올바른 Copilot 활용 방법으로 올바른 단어 선정과 적절한 문법, 어디에 있는 데이터를 참고 해야 하고 구체적으로 조사해야 할 주제가 무엇인지에 대해서 사용자가 명령 프롬프트에 작성하여 Copilot이 작업 내용을 보다 명확하게 파악할 수 있도록 지시하는 것이 필요합니다.

올바른 Copilot 활용 방법



Good

Copilot에게 보다 구체적이고 명확하게 지침을 내리세요

Copilot은 때때로 실수할 수 있습니다.
정확성을 위해 Copilot의 응답을 항상 확인하세요

Copilot에게 피드백을 요청하면
관련성 있고 창의적인 사본을 제공하는데 도움이 됩니다.

Copilot에게 올바른 구두점, 대문자 및 문법을 사용하여
프롬프트를 작성하세요

정확하고 일관된 응답을 생성하는 데 도움이 되는
상황별 세부 정보를 Copilot에게 제공합니다.

친절하고 정중한 언어 사용은
AI의 응답성과 성능을 향상시키는데 도움이 됩니다.



Bad

Copilot에게 모호한 언어를 사용하지 않고
가능한 명확한 지침을 내리세요

부적절하거나 비윤리적인 내용을 요구하면
Copilot의 응답 제공이 어려울 수 있습니다.

동일한 프롬프트에서 여러 개의 정보 또는 충돌하는 정보를
포함하는 작업을 수행하면 부정확한 결과를 제공합니다.

속어, 전문용어, 격식을 차리지 않은 용어를 사용하면
전문적이지 않은 응답이 제공될 수 있습니다.

갑자기 화제를 끊거나 바꾸면
Copilot의 작성 과정이 중단될 수 있습니다.

중요한 작업을 Copilot에게만 의존하지 않고
반드시 작업 결과를 감독하는 것이 필요합니다.

Microsoft 365 Copilot의 필요사항은 M365 Business Standard, Premium, E3, E5 및 Office E3, E5 구독 라이선스를 사용하고 있으면서 추가적으로 Copilot 라이선스를 보유하고, M365 데이터 보안과 새로운 Outlook 및 M365 App 업데이트의 설정이 필요합니다.

Microsoft 365 Copilot 필요사항

Microsoft 365 구독 라이선스



- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5
- Office 365 E3
- Office 365 E5

데이터 보안



Copilot의 제한된 데이터 접근을 위하여 데이터 보안(Microsoft Purview)의 정책 적용이 필요합니다.

Microsoft 365 Copilot 라이선스



- Microsoft 365 Copilot
(단독 라이선스 사용은 불가능)

M365 설정 옵션



새로운 Microsoft 365 클라이언트로 업데이트가 필요하며, 현재 및 월별 엔터프라이즈 채널의 업데이트 구성이 필요합니다.

Microsoft 365 Copilot의 보안 필요성은 점점 더 새로워지는 사이버 침해 공격 대응을 위해 사용자 ID를 중심으로 계정의 인증 액세스를 강화하고 디바이스 보안과 기밀 데이터의 조회 및 유출을 보호해야 하며 Microsoft 365 Copilot의 무분별한 데이터 접근 제어가 필요합니다.

Microsoft 365 Copilot 보안 필요성

계정, 장치, 데이터 보안에 대한 보안 우려



ID 인증 액세스 관리
및 보안 구성의 필요



외부 공격과 침해
대응 및 관리 요구



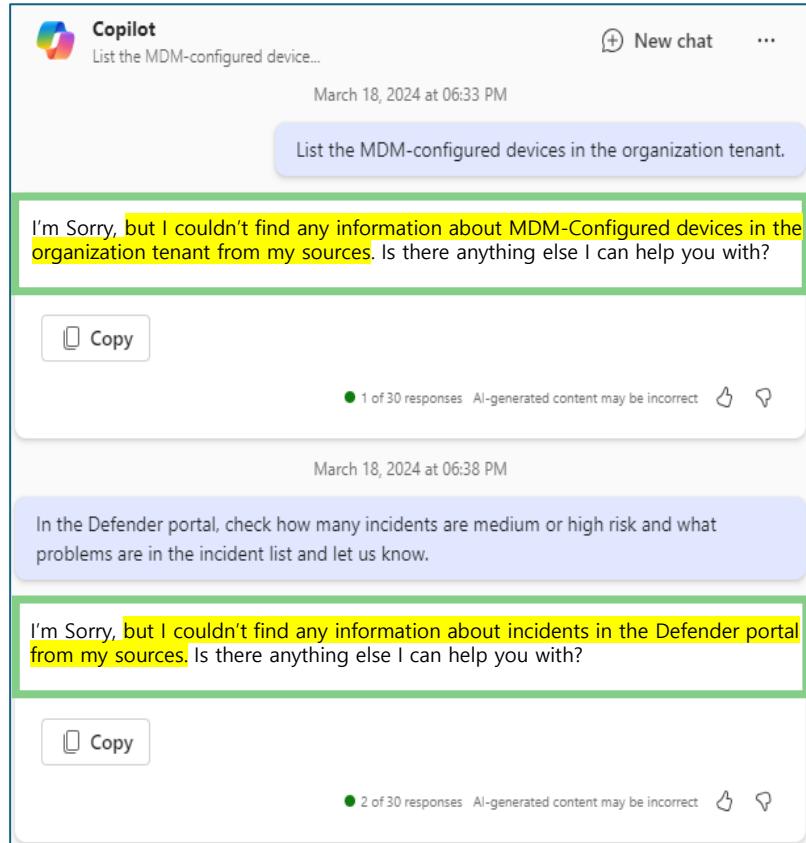
기밀 비즈니스
데이터 보호 필요

Microsoft 365 Copilot 데이터 보호

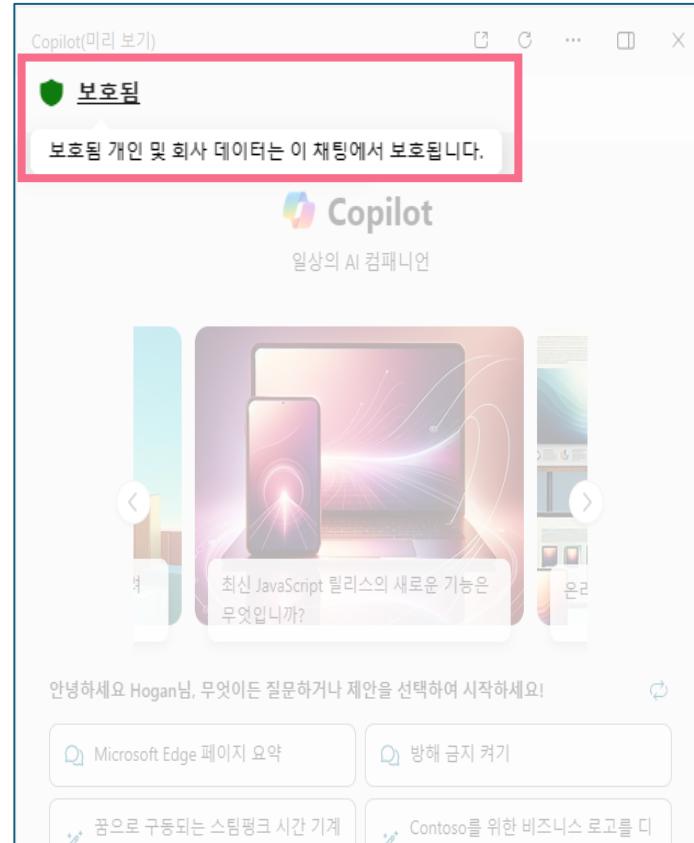


분리 되어있는 Copilot 작업 공간은 각 버전에 맞는 Copilot이 작동 하는 공간이 따로 분리 되어있어, 개인 및 회사 데이터에 대한 보호, 사용자 생성물에 대한 분리, 보안 플랫폼 접근 여부 등 엄격한 내부 분리 제어를 받고 있기 때문에 모두 각 버전에 맞는 공간에서만 작동 됩니다.

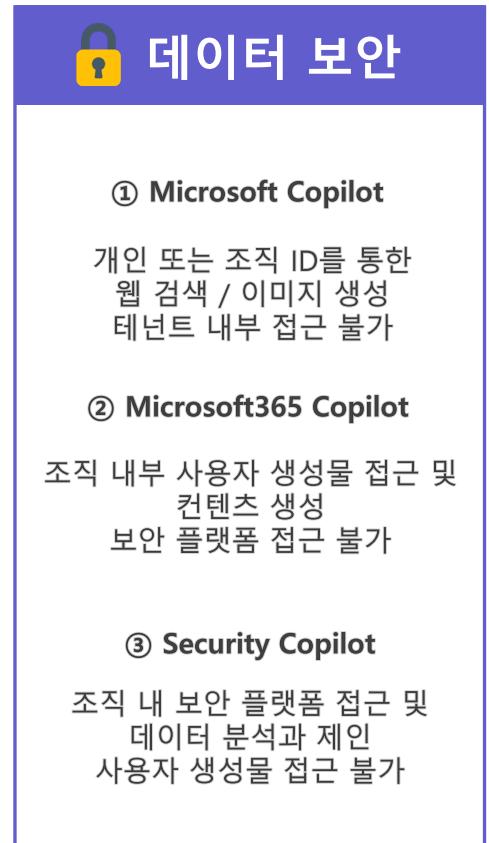
분리 되어있는 Copilot 작업 공간



The screenshot shows two separate Microsoft Copilot conversations. The top conversation is for 'Copilot' and the bottom is for 'Copilot(미리 보기)'. Both conversations are about listing MDM-configured devices in an organization tenant. The responses are identical: 'I'm Sorry, but I couldn't find any information about MDM-Configured devices in the organization tenant from my sources. Is there anything else I can help you with?'. Each conversation has a 'Copy' button and a note that the response is AI-generated.



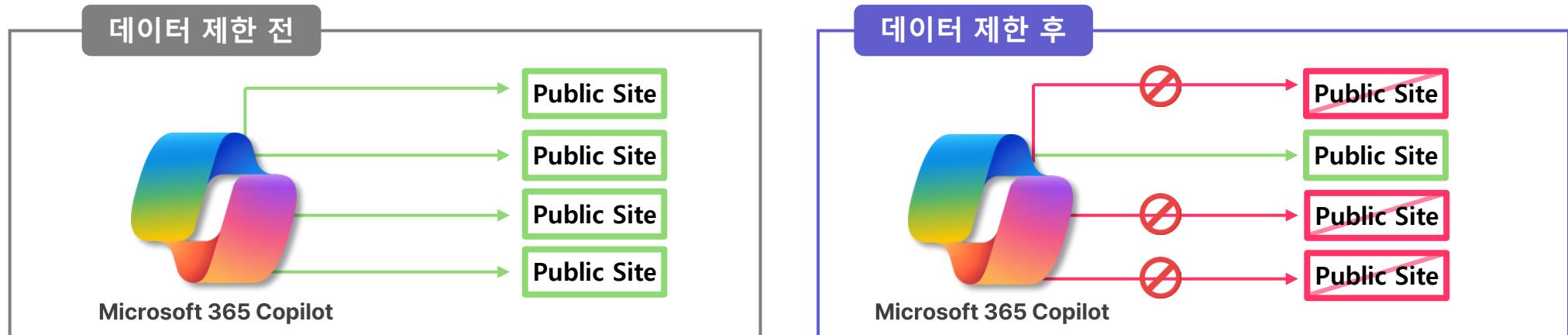
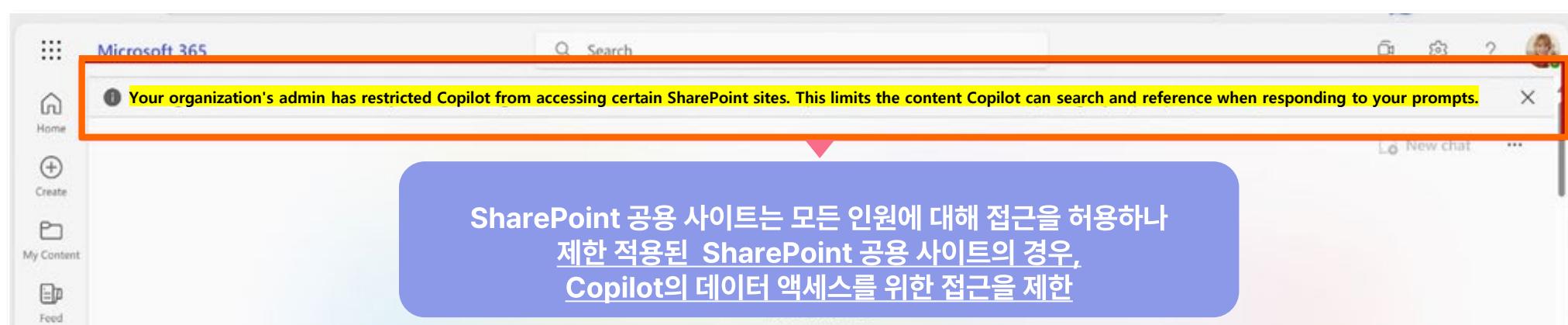
The screenshot shows the Microsoft Copilot interface with a preview message: '보호됨' (Protected) and '보호됨 개인 및 회사 데이터는 이 채팅에서 보호됩니다.' (Protected personal and company data is protected in this chat). Below this, there is a preview of a Copilot card with a lock icon and the text 'Copilot' and '일상의 AI 컴퍼니언'. The card also shows a smartphone and a laptop, and a message about the latest JavaScript release.



The screenshot shows a '데이터 보안' (Data Security) section. It includes three numbered sections: ① Microsoft Copilot (Personal or organizational ID protection), ② Microsoft365 Copilot (Internal user generation protection), and ③ Security Copilot (Internal security platform protection). Each section has a brief description and a link to a Microsoft Edge page.

제한된 SharePoint 검색은 묵시적으로 모든 사용자가 접근 할 수 있는 SharePoint 공용 사이트의 데이터를 Microsoft 365 Copilot에서 접근하는 보안 문제를 해결하고자 설정될 수 있는 고급 설정 기능으로 공용 데이터 검색을 제한하여 데이터 초과 공유를 방지할 수 있습니다.

제한된 SharePoint 검색



Microsoft 365 Copilot의 확장은 조직 테넌트 내 Microsoft 365 앱의 데이터 뿐만 아니라 온프레미스, 클라우드 저장소, 외부 서비스와 같은 다양한 플랫폼의 데이터를 조직 데이터셋에 확장 연결하여 더 넓은 영역의 데이터를 수집하여 유연한 문서 작업의 생산성을 제공합니다.

Microsoft 365 Copilot 확장

테넌트 내부 조직 데이터

Microsoft 365 Apps
Excel, Word, PowerPoint,
SharePoint, OneDrive,
Exchange Online,



테넌트 외부 조직 데이터

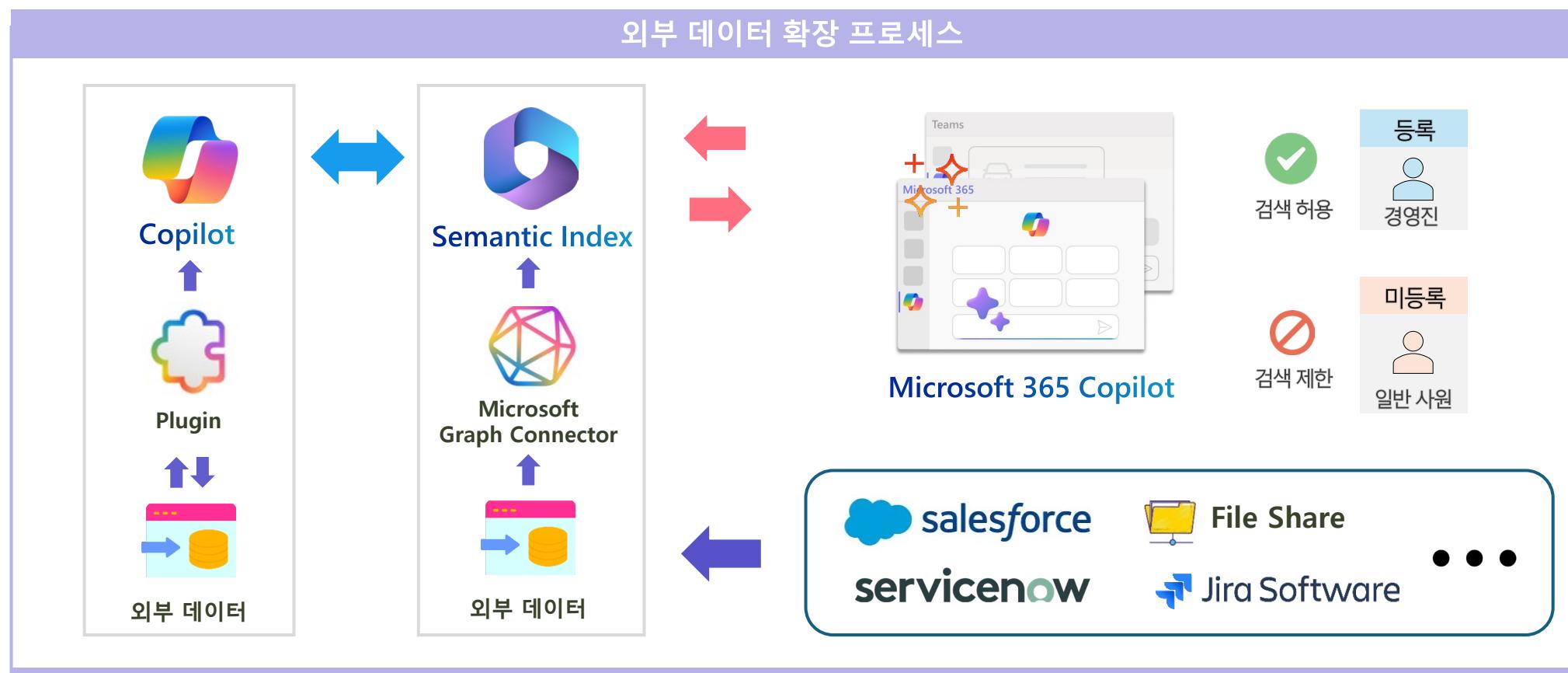
Windows FileShare,
ServiceNow, Salesforce,
Jira, SAP ...



Microsoft Graph Connector를 이용한 Copilot 확장으로 다른 플랫폼의 더 많은 조직 데이터를 액세스

Microsoft 365 Copilot의 확장 프로세스는 Graph Connector를 통해 온-프레미스 및 클라우드 서비스에서 호스팅 되는 외부 데이터를 인덱싱해 Copilot의 데이터 검색 결과를 확장함과 동시에 사용자의 액세스 권한이 있는 콘텐츠만 Copilot에게 지시할 수 있도록 구성합니다.

Microsoft 365 Copilot 확장 프로세스



5

Microsoft Security(EMS)

Microsoft 365 EMS(Enterprise Mobility + Security)는 Microsoft 365 사용자의 ID 계정과 디바이스 그리고 비즈니스 데이터를 보호하기 위한 보안 솔루션의 집합체로써, 외부 침입으로부터 조직 내 보안 대응과 추적, 거버넌스 및 규정 준수를 통합 관리할 수 있습니다.

What is Microsoft 365 EMS



Microsoft Defender

모든 환경에서의
위협을 통합 보호



Microsoft Entra ID

클라우드 기반 ID로
사용자의 접근 통제



Microsoft Purview

데이터 거버넌스 제어로
조직 데이터 보호



Microsoft Intune

모바일 및 PC시스템의
중앙 관리 제어



Microsoft 365 EMS(Enterprise Mobility + Security)는 Entra ID를 통한 사용자 인증 및 조건부 액세스 정책 관리와 Intune을 통한 디바이스 및 앱 관리 그리고 Purview를 통한 데이터 및 문서 보호 제어 구성을 통해 문서 접근과 데이터 유출에 대한 보안 환경을 제공합니다.

Microsoft 365 보안 솔루션(EMS)

계정 보안



Microsoft Entra ID
ID 및 액세스 관리 & ID 기반 보안

[주요 기능]

- 강력한 패스워드 정책 설정 및 중앙 관리 가능
- 보안 강화를 위한 다중 & 추가 인증 적용 (MFA, 문자, ARS 앱 인증 등)
- 비인가 디바이스에 대한 제한적 액세스 권한 설정 가능
- 타사 클라우드 제품과 통합 인증 체계 구현 가능

장치 보안



Intune
디바이스 및 앱 관리

[주요 기능]

- 디바이스 분실 시, 데이터 유출 방지를 위한 자체 암호화 구성 가능
- 업무용 소프트웨어에 대한 중앙 자동 배포 가능
- 디바이스 분실 시, 데이터 초기화 가능
- 특정 소프트웨어 설치 및 실행 차단 가능

데이터 보안

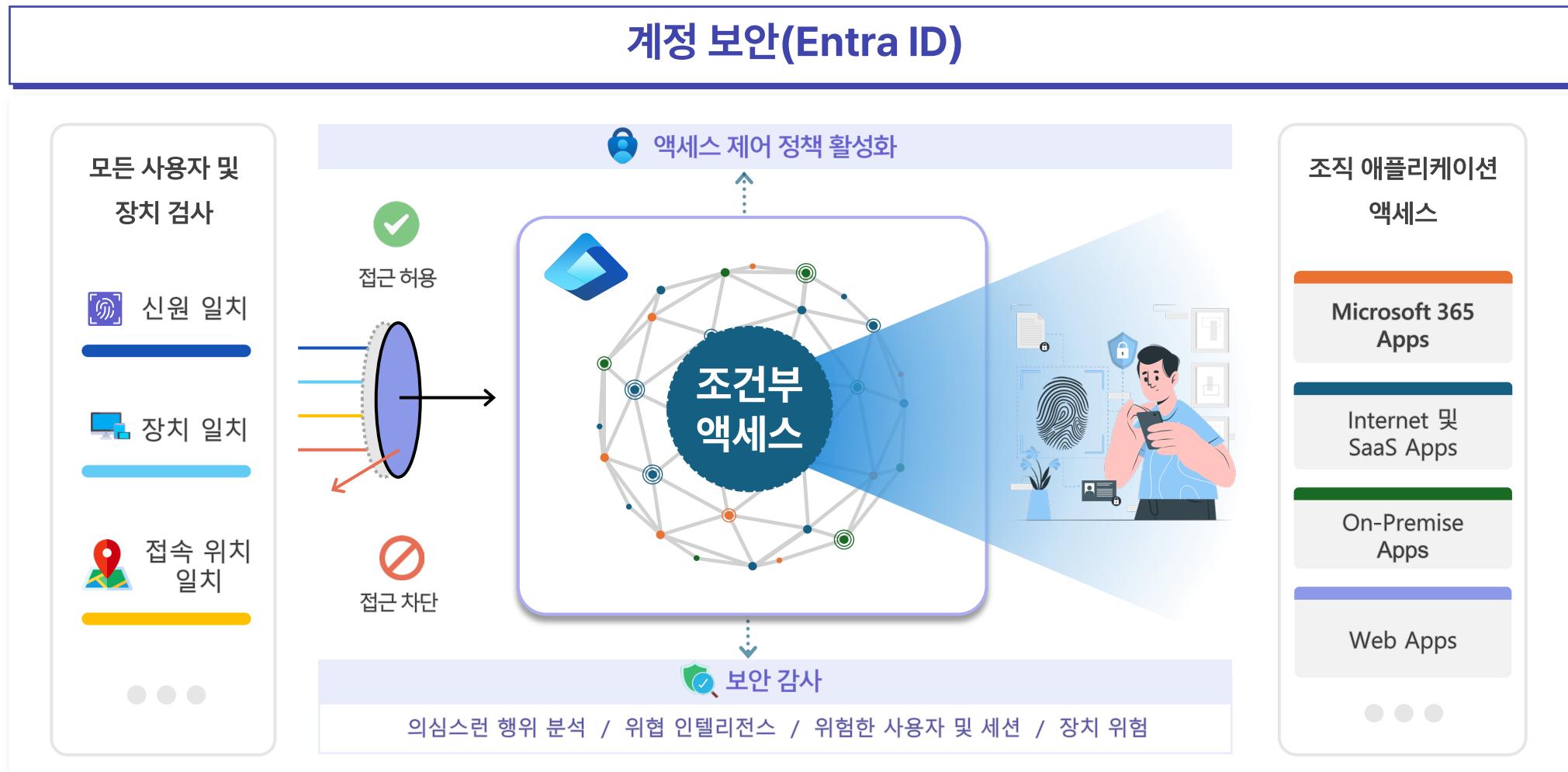


Purview
데이터 정보 및 문서 보호

[주요 기능]

- 사용자 권한 설정 세분화로 문서 유출 보호 가능
- 사내 문서 보안레벨 규정에 따른 등급 설정 및
- 레이블 정의 가능
- 회사 업무 관련 데이터에 대한 차단 기능으로 데이터 유출 방지

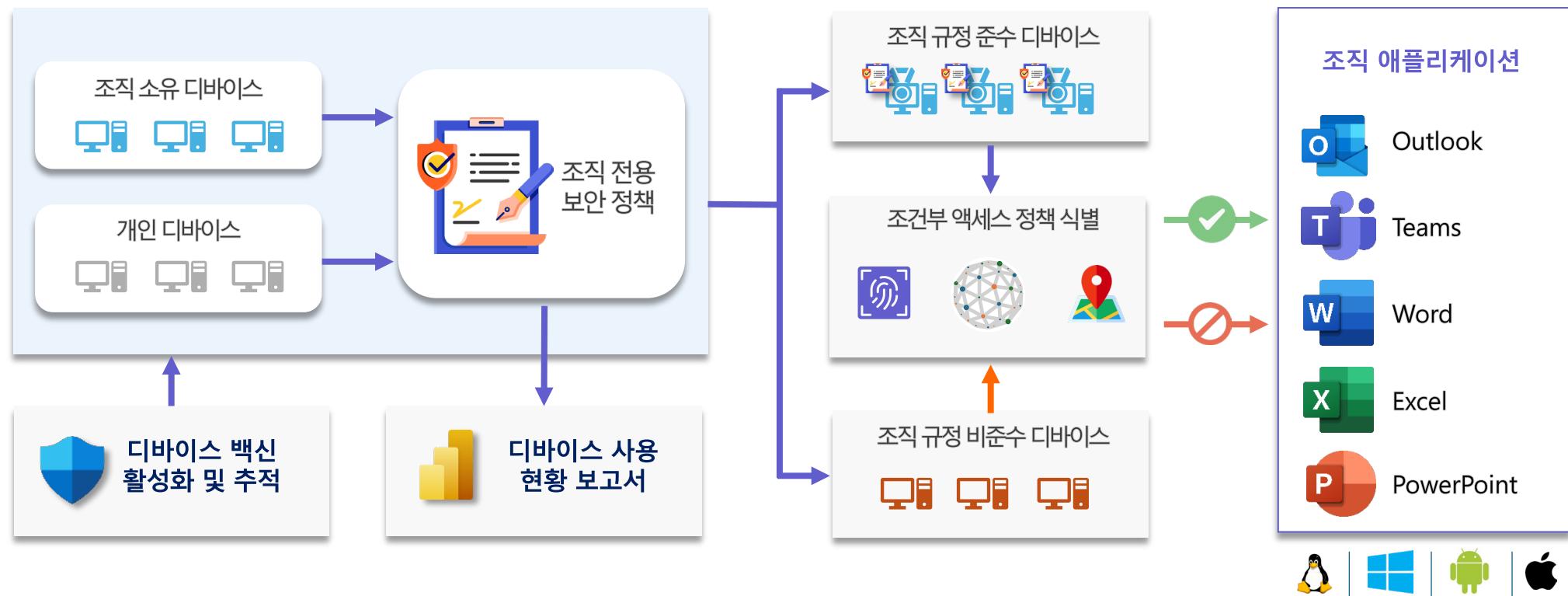
계정 보안 플랫폼인 **Entra ID**는 조건부 액세스를 통해 모든 사용자와 장치가 조직의 보안 정책을 충족하는 경우에만 M365 리소스에 액세스할 수 있도록 보호 지원하며, 이에 해당되지 않는 경로의 행위를 즉각 차단하여 비즈니스 데이터의 소실과 유출을 보호할 수 있습니다.



장치 보안 플랫폼인 **Intune**은 클라우드 기반의 모바일 및 데스크톱 장치 관리 솔루션으로서, 소유한 장치 별로 사용자의 시스템 설정과 규정 준수, 하드웨어 규격 등에 대하여 중앙 관리하고, BI를 통한 현황 보고서를 제작하거나 보안 프로그램을 배포하여 보안을 강화할 수 있습니다.

장치 보안(Intune)

Microsoft Intune

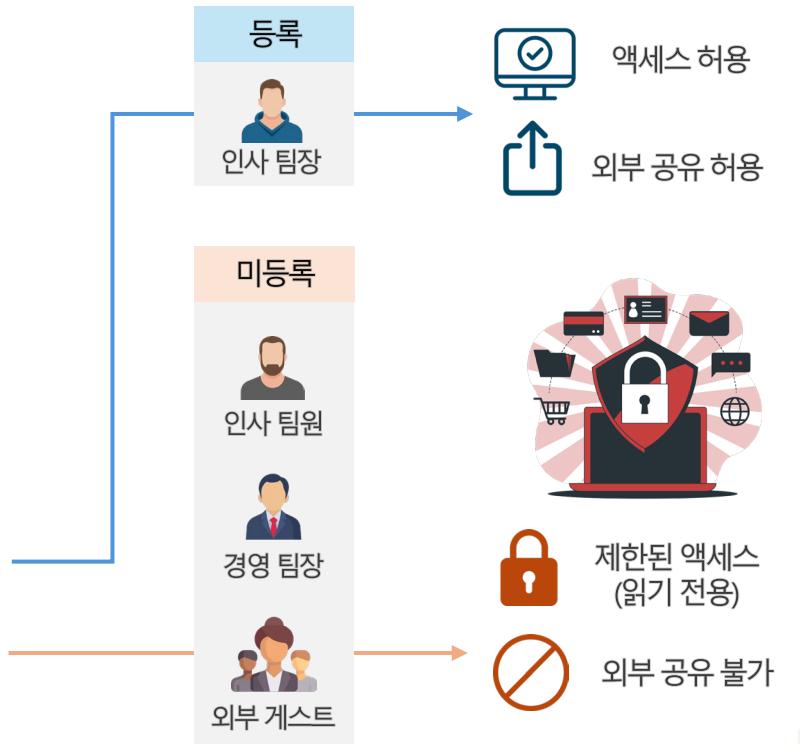
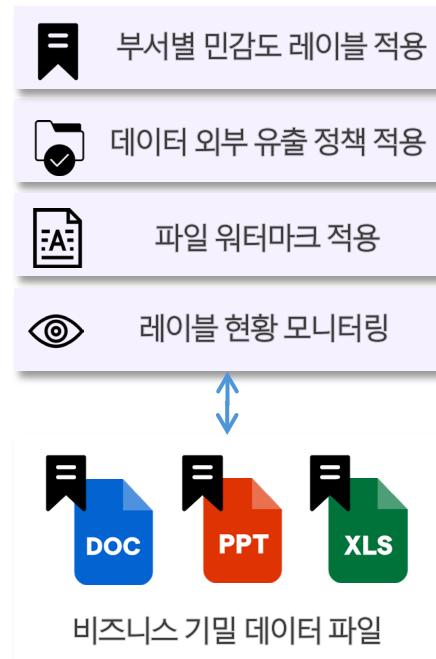


데이터 보안 플랫폼인 **Purview**는 데이터 거버넌스, 개인 정보 보호 및 데이터 규정 준수를 위한 보안 플랫폼으로서, 조직 내 데이터의 접근, 분류, 외부 공유에 관한 정책을 관리하여 비즈니스 데이터의 손실과 유출을 보호하고, 데이터 보안 감사율 통해 취약점을 파악할 수 있습니다.

데이터 보안(Purview)



데이터 보안 감사



조직의 데이터 거버넌스 중앙 관리 센터

조직의 문서 데이터 규정준수 설정

접근 대상 식별

식별된 대상의 문서 접근 제어

민감도 레이블 적용 시나리오는 Copilot이 문서에 민감도 레이블이 걸려있지 않다면 무분별하게 데이터를 액세스하여 사용자에게 제공하기 때문에, 이러한 상황을 막기 위해 민감도 레이블 정책을 배포하면 Copilot은 요청자의 권한을 인식하여 접근 가능한 데이터만 액세스 합니다.

민감도 레이블 적용 시나리오

데이터 보호 미지정으로 Copilot이
무분별하게 모든 데이터를 액세스 함으로써
기밀 데이터 및 불필요한 정보 공유



민감도 레이블 미설정으로
모든 데이터를 무분별하게 액세스



데이터 보안 문제 발생



모든 비즈니스 데이터

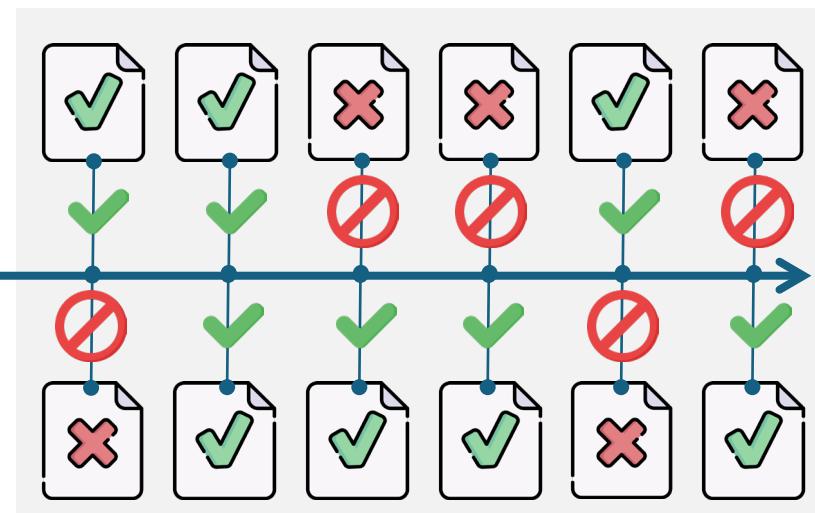
요청자의 액세스 권한에 따라 Copilot이
액세스 할 수 있는 문서가 나누어지므로
데이터 누출 안전 및 불필요한 공유 차단



✓ 권한 있는 비즈니스 데이터
액세스 가능

✗ 권한 없는 비즈니스 데이터
액세스 불가

부서별/사용자별
민감도 레이블 적용

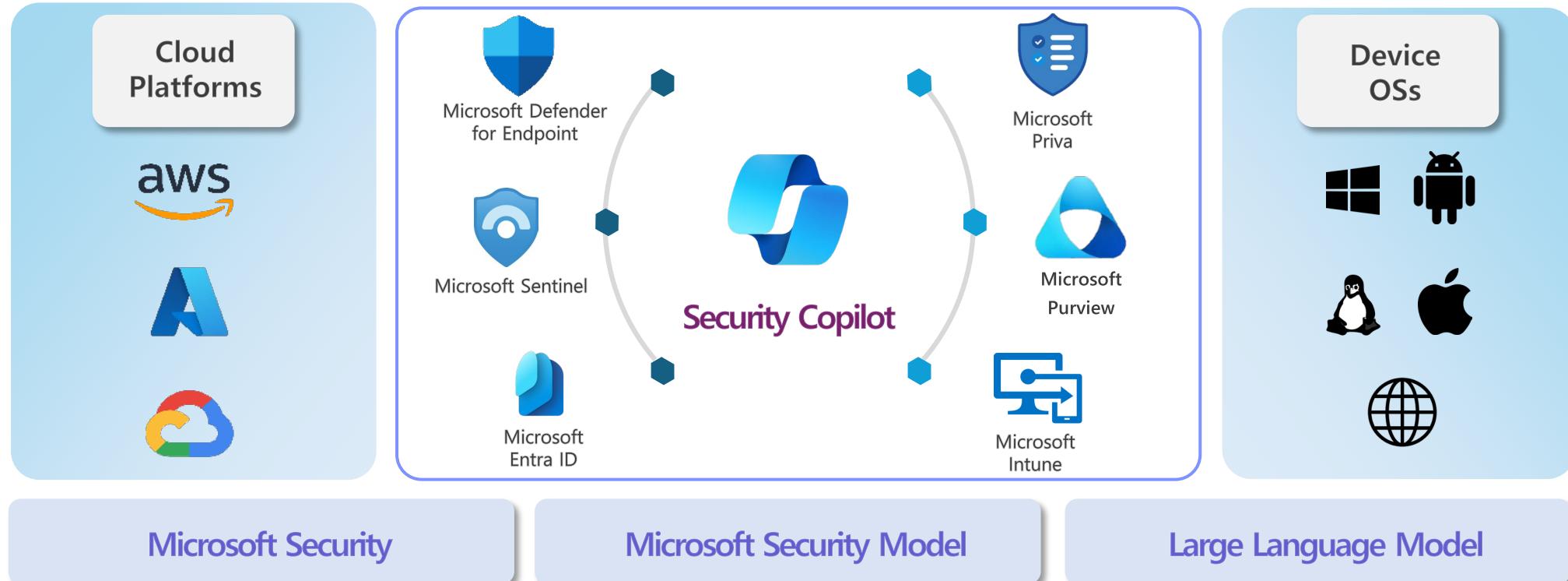


6

Security Copilot

Security Copilot은 사이버 보안 공격의 대응, 위협 추적, 인텔리전스 수집, 상태 관리 등을 보안 전문가를 대신하여 안내하거나 분석 지원할 수 있도록 설계되어 Microsoft 보안 제품을 포함하여 온프레미스, 타 클라우드 서비스들과도 통합되어 손쉽게 관리할 수 있습니다.

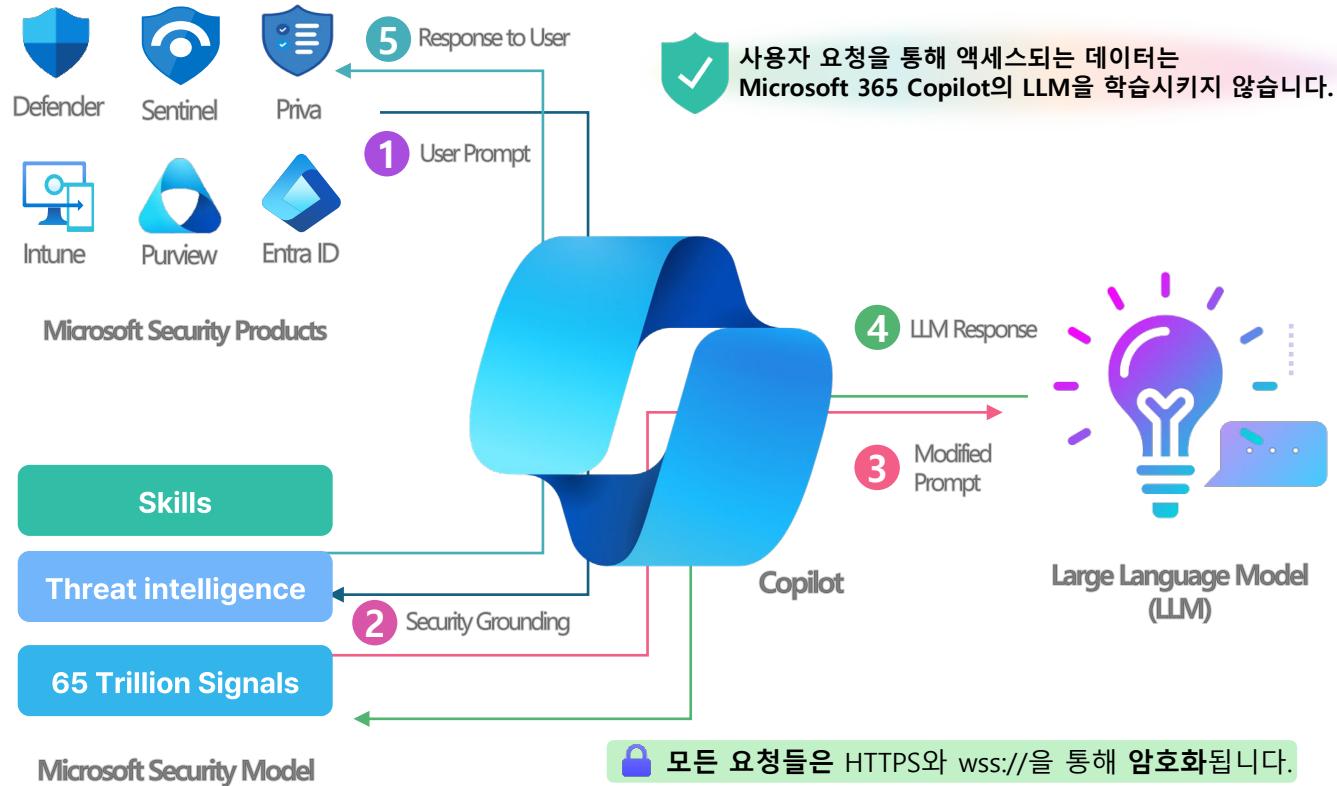
What is Security Copilot



현재 전 세계적으로 보안 인력이 약 350만 명 정도 부족한 상황, 이러한 보안 인력 부족 문제를 AI 보안 플랫폼으로 해결

Security Copilot은 대규모 보안 이벤트의 분석, 위협의 심각도를 평가하고 보안 위협에 대해 신속하게 대응하거나 사후 분석을 진행하여 공격 재발을 방지하거나 사내 보안 특이점을 파악하여 보안 담당자의 업무를 대신하거나 보조하여 보안 태세 계층을 한 층 더 향상 시킵니다.

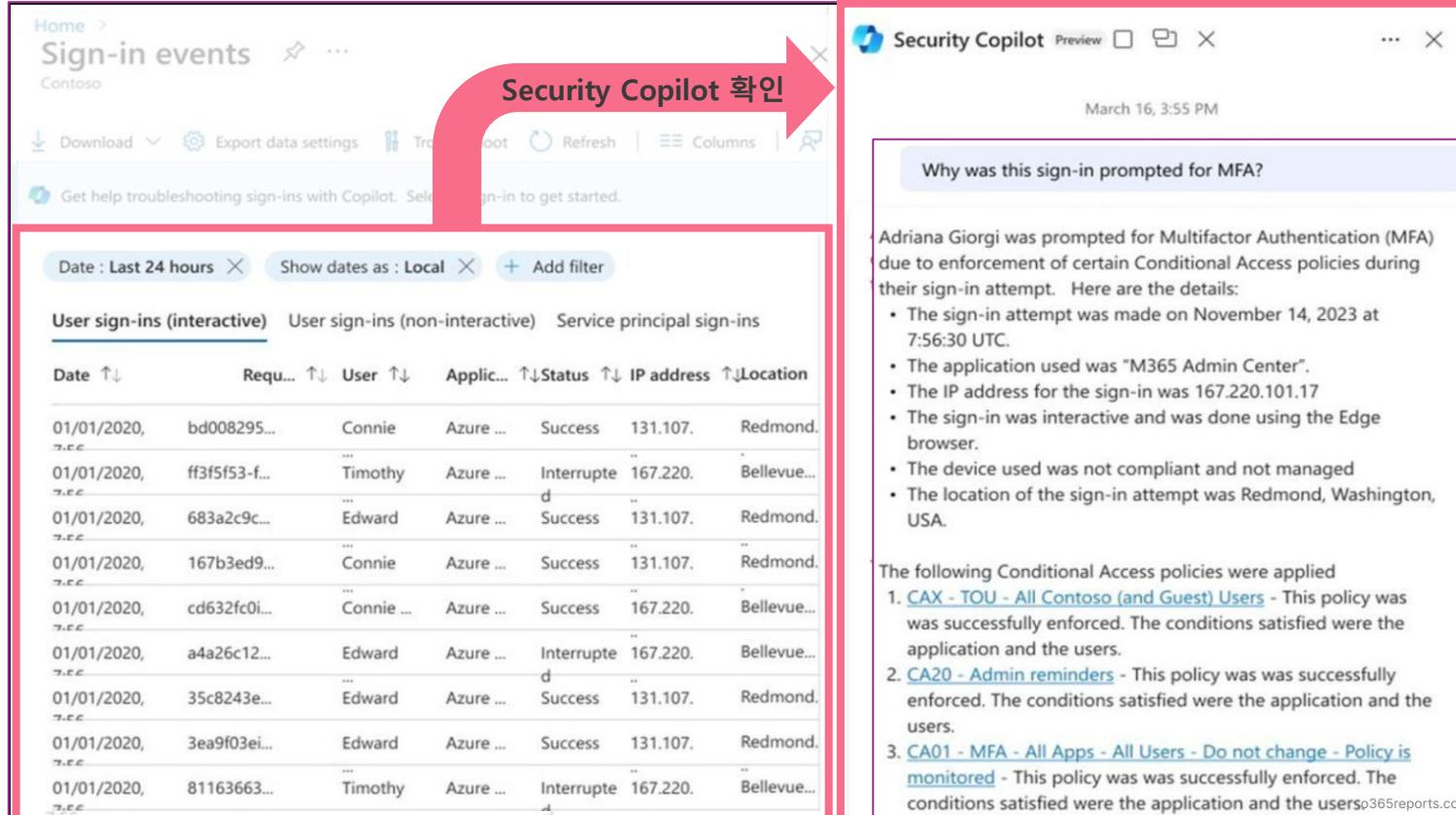
Security Copilot 동작 방식



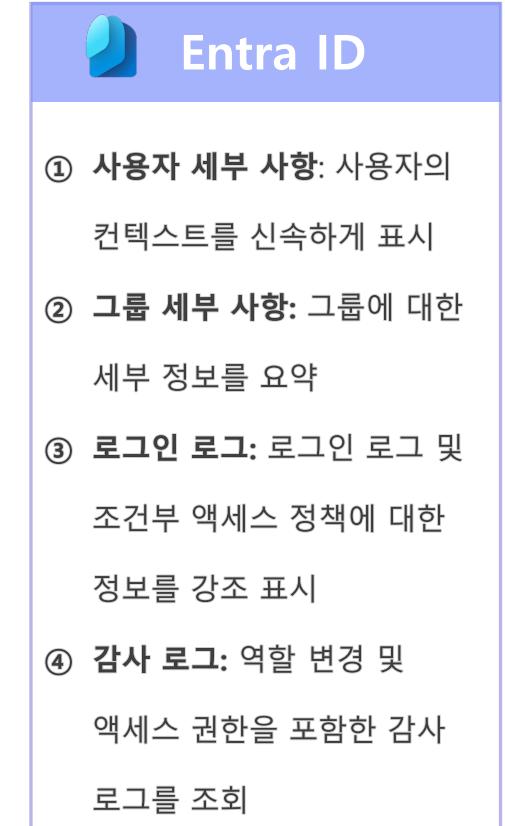
- 1 **Copilot 프롬프트 입력**
Microsoft Security 제품군에서 각 프롬프트를 Copilot에 전달됩니다.
- 2 **Microsoft Security 연결**
그라운딩을 위해 Copilot이 Microsoft Security Model에 접근합니다.
- 3 **LLM 자연어 처리**
Copilot이 수정된 프롬프트를 LLM에 전달합니다.
- 4 **Copilot 체크 및 리뷰**
Copilot이 LLM 응답의 체크 및 리뷰를 위해 Microsoft Security Model에 접근합니다.
- 5 **사용자 응답 반환 및 제안**
사용자와 제품군에 답변과 제안을 전달합니다.

Entra ID의 Security Copilot은 자연어 프롬프트를 통해 담당자가 쉽게 사용자 및 그룹의 세부 사항과 계정 로그인 및 감사 로그 등의 정보를 확인 할 수 있으며, 이 정보를 바탕으로 보안 사고를 해결하는 방법에 대한 권장 사항과 함께 사용자 위험 수준을 분석하게 도와줍니다.

Security Copilot(Entra ID)



The screenshot shows two main windows. The left window is a 'Sign-in events' dashboard for 'Contoso' with a red box highlighting the 'Security Copilot' button. The right window is a 'Security Copilot Preview' window with a red box highlighting the main content area. The content area shows a detailed analysis of a sign-in attempt for Adriana Giorgi on November 14, 2023, at 7:56:30 UTC, using the 'M365 Admin Center' application from an IP address 167.220.101.17. The analysis includes a list of Conditional Access policies applied, such as 'CA01 - MFA - All Apps - All Users - Do not change - Policy is monitored'.



① 사용자 세부 사항: 사용자의 컨텍스트를 신속하게 표시

② 그룹 세부 사항: 그룹에 대한 세부 정보를 요약

③ 로그인 로그: 로그인 로그 및 조건부 액세스 정책에 대한 정보를 강조 표시

④ 감사 로그: 역할 변경 및 액세스 권한을 포함한 감사 로그를 조회

Intune의 Security Copilot은 자연어 프롬프트를 통해 조직 내 디바이스 하드웨어의 정보, 정책별 필터링 그리고 할당된 정책의 부서 및 사용자의 세부 정보를 표시하는 데이터 인사이트를 장치 담당자 대신하여 안내해주기 때문에 쉬운 사용성과 관리성을 지원할 수 있습니다.

Security Copilot(Intune)

The screenshot shows the Microsoft Intune interface. On the left, the navigation menu includes Home, Dashboard, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, Troubleshooting + support, and Show related admin centers. The main area is titled 'Devices | Configuration' and shows a list of policies. A red arrow points from the text 'Security Copilot 확인' to the 'Security copilot' search bar in the Intune interface. The Intune interface shows a policy titled 'Create a policy that blocks users from using any removable storage devices on Windows 11 laptops'. It details the policy settings, including 'Administrative Templates' and 'System > Removeable Storage Access'. A 'Create policy' button is also visible.

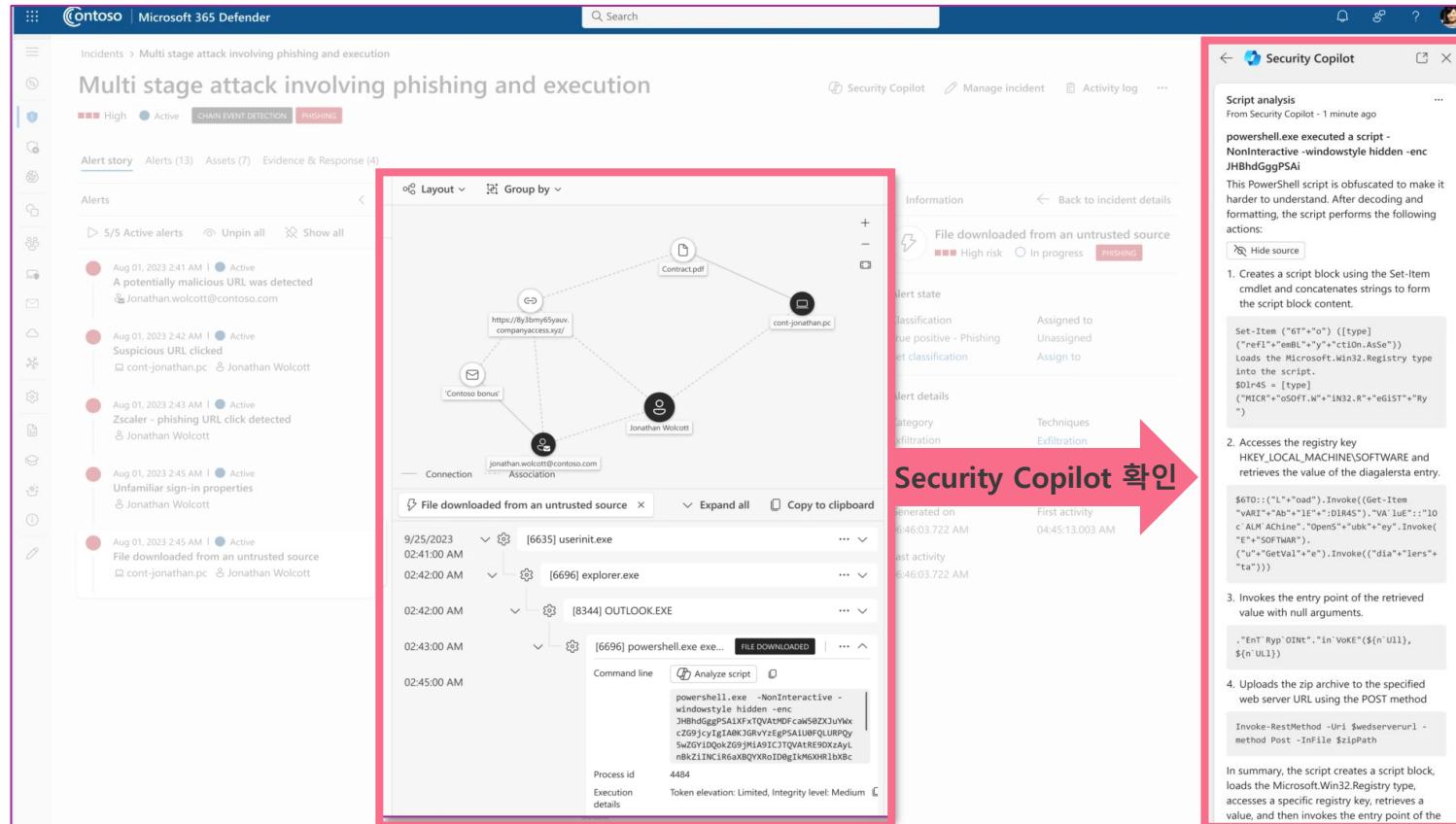
① 장치 하드웨어 확인:
사용자가 연결된 장치의 장치 정보를 표시

② 정책별 필터링: 사용자 및 그룹에 할당된 정책의 정보를 조회

③ 정책 대상: 특정 앱이 할당된 그룹 및 특정 앱이 할당된 사용자의 세부 정보 표시

Defender의 Security Copilot은 자연어 프롬프트를 통해 조직의 보안 취약점과 발생된 감염 경로를 추적하고 침해 사건을 요약하거나 보안 영향을 평가하는 등 보안 분석을 통해 현재 노출된 보안 취약점을 식별하고 신속하게 대처할 수 있도록 보안 지침을 안내할 수 있습니다.

Security Copilot(Defender)



Incidents > Multi stage attack involving phishing and execution

Multi stage attack involving phishing and execution

Alert story Alerts (13) Assets (7) Evidence & Response (4)

Alerts

5/5 Active alerts

Aug 01, 2023 2:41 AM | Active A potentially malicious URL was detected [jonathan.wolcott@contoso.com](#)

Aug 01, 2023 2:42 AM | Active Suspicious URL clicked [cont-jonathan.pc](#) Jonathan Wolcott

Aug 01, 2023 2:43 AM | Active Zsaler - phishing URL click detected [Jonathan Wolcott](#)

Aug 01, 2023 2:45 AM | Active Unfamiliar sign-in properties [Jonathan Wolcott](#)

Aug 01, 2023 2:45 AM | Active File downloaded from an untrusted source [cont-jonathan.pc](#) Jonathan Wolcott

Layout Group by

File downloaded from an untrusted source

9/25/2023 02:41:00 AM [6635] userinit.exe

02:42:00 AM [6696] explorer.exe

02:42:00 AM [8344] OUTLOOK.EXE

02:43:00 AM [6696] powershell.exe exe...

02:45:00 AM

Process id: 4484
Execution details: Token elevation: Limited, Integrity level: Medium

Information

File downloaded from an untrusted source (High risk)

Alert state: File positive - Phishing

Classification: Unassigned

Alert details: Category: Filtration

Techniques: Elevation

Script analysis

From Security Copilot - 1 minute ago

powershell.exe executed a script - NonInteractive -windowstyle hidden -enc JHBhdGgPSAiXx7QATMDFcaw50zXJuYwx cZ09jcytgIAK0KGRVzEgSALUBFQURQy SwZGY1D0okZG93M1A91CT7QATRt90zAxL nbK21INC1R6axBQYXr0ID0gIMK6XH1bKc

This PowerShell script is obfuscated to make it harder to understand. After decoding and formatting, the script performs the following actions:

- Creates a script block using the Set-Item cmdlet and concatenates strings to form the script block content.
- Accesses the registry key HKEY_LOCAL_MACHINE\SOFTWARE and retrieves the value of the diagalerast entry.
- Invokes the entry point of the retrieved value with null arguments.
- Uploads the zip archive to the specified web server URL using the POST method.

In summary, the script creates a script block, loads the Microsoft.Win32.Registry type, accesses a specific registry key, retrieves a value, and then invokes the entry point of the

Security Copilot 확인

① 실시간 멀웨어 분석: 복잡하고 난독화 된 PowerShell

스크립트를 분석

② 위협 인텔리전스 검사: 새로운 특정 사이버 위협이 현재 영향 받고 있는지 검사

③ 자연어로 쿼리 작성(KQL): 자동으로 Kusto Query

Language를 생성하여 시간 절약 및 보안 분석력 향상

Defender

Purview의 Security Copilot은 자연어 프롬프트를 통해 조직 내에서 이동 되는 데이터의 가시성을 제공하며, 이를 통해 복잡하고 어려운 보안 분석 시간을 단축하고 놓칠 수 데이터 보안의 취약점을 발견하여 정보 보호 담당자를 대신하여 보안 지침에 관해 안내할 수 있습니다.

Security Copilot(Purview)

The screenshot shows the Microsoft Purview Communication Compliance interface. A 'Security Copilot 확인' (Security Copilot Confirmation) pop-up is overlaid on the main screen. The main screen displays a list of policy violations under the 'Communication Compliance' section, specifically under the 'Inappropriate text policy'. A transcript of a Teams meeting between Nestor Wilke and Grady Archie is shown, with specific messages flagged as 'Gifts & entertainment'. The pop-up provides a detailed summary of these flagged messages and their context within the meeting transcript.

Purview

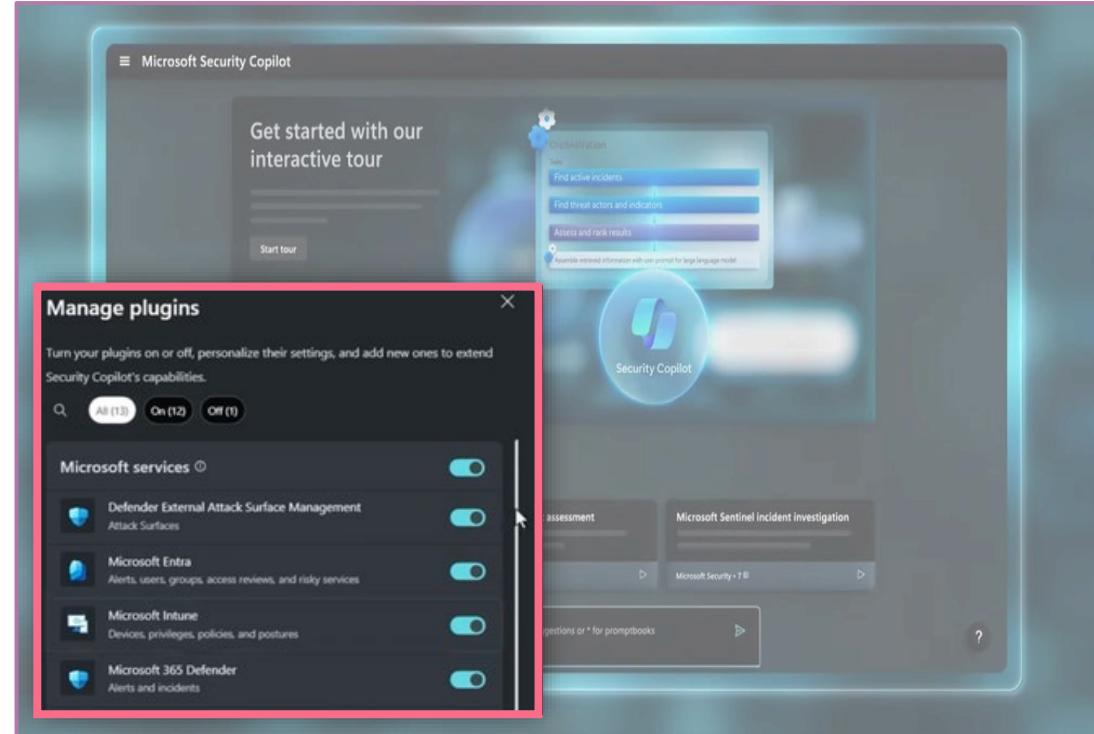
① 데이터 검색 및 감사: Copilot
사용 활동을 추적하고 검색하여
데이터 이동 이력을 파악

② 법적 및 규제 정보 수집:
eDiscovery 기능을 사용하여
Copilot에서 처리된 데이터 수집
분석

③ 민감도 레이블 분류: Copilot
에서 사용하는 데이터의 유형을
식별하고 분류하여 조회

Security Copilot 독립형은 자연어 프롬프트 방식으로 독립된 환경에서 Entra ID, Intune, Defender, Purview 같은 관리형 플러그인에 연결되어 보안 스크립트를 분석하고, 보안 취약점에 대한 영향을 평가하는 등 보안 담당자를 대신하여 보안 보고서를 생성할 수 있습니다.

Security Copilot 독립형



선택한 보안 영역에서만 데이터 보안 액세스

Write a report summarizing the investigation. Lead with a non-technical executive summary. Next provide the breakdown of the Defender incident report, the takeaways from the Sentinel Hunt, the Intune device state, and finally the threat intel summary.

> 3 steps completed 70s

Nov 3, 10:03 AM | 71.17s

Executive Summary

An investigation was conducted into a security incident involving user Lynne Robbins and the device PARKCITY-Win10S. The device was found to be noncompliant with the Defender for Endpoint - Device Risk policy. The Manatee Tempest threat actor group, known for its ransomware campaigns, was active during this incident.

Defender Incident Report

The incident involved initial access, command and control, and ransomware on multiple endpoints. Manatee Tempest activity was detected, and ransomware activity was observed. The device PARKCITY-Win10S was found to be noncompliant with the Windows10CompliancePolicy.DeviceThreatProtectionRequiredSecurityLevel setting.

높은 수준의 보안 요약 보고서 생성

7

결론

Microsoft 365 Copilot의 활용법으로 외부 악성 공격 대응과 데이터 유출 보호를 위한 Microsoft 365 EMS 구축이 필요하며, 사내 데이터 뿐 아니라 외부 데이터를 확장하는 Graph Connector, 복잡하고 난해한 보안 분석을 위한 Security Copilot을 활용할 수 있습니다.

Microsoft 365 Copilot의 활용법

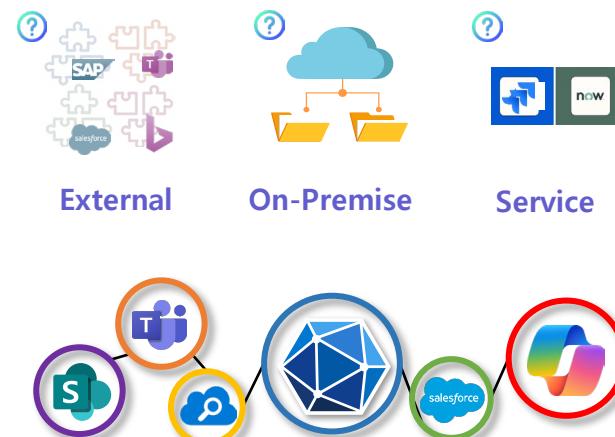
Data Security



계정 보안 장치 보안 데이터 보안

조직의 민감 데이터 암호화를 위한
Microsoft 365 EMS 보안 솔루션

Data Expansion



외부 데이터 확장하기 위한
Microsoft Graph Connector

AI Security Analyst



업무의 생산성과 효율성 향상을 위해 Microsoft 365 Copilot을 도입하여 AI를 활용한 업무 습관화와 인공지능의 올바른 학습 관리를 지도 감독하고, Microsoft 365 EMS 구축을 통해 데이터 접근 및 유출을 제어하면서 다양한 문서 생산성을 위해 데이터 확장 구성이 필요합니다.

업무의 생산성과 효율성 향상을 위한 Microsoft 365 Copilot



AI와 함께하는 업무 습관화

- AI를 통한 업무의 생산성을 향상하기 위해 일상에서 임직원들이 Copilot을 통해 업무 사용할 수 있도록 돋는 것이 필요합니다.



데이터 보안 정책 구성

- Copilot이 민감한 비즈니스 데이터를 내부 혹은 외부에 공유하거나 함부로 접근하지 못하도록 보안 정책을 구성하는 것이 필요합니다.



인공지능 학습 관리

- Copilot의 잠재력을 향상시키기 위해 명확하고 올바른 질의를 학습시키고, 답변할 수 있도록 관리하는 것이 필요합니다.



조직 데이터 확장 연결

- 조직의 비즈니스 앱인 Microsoft App 뿐만 아니라 외부 데이터에도 접근하려고 한다면 올바른 확장 연결 구성이 필요합니다.



Microsoft 365 EMS 및 Copilot 구축 프로젝트로 초기 단계에서 발생되는 기회 비용을 절감하고 고객의 투자 가치를 창출합니다.



Microsoft AI 플랫폼 활용 AI 업무 환경 구축 세미나

Thank You

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