



Microsoft 365
Copilot

AI 보안 필수 요소

Microsoft 365 Copilot에 대한 CEO 가이드



목차

01 /
보안 기능이 우선



02 /
개인 맞춤형 경험



03 /
기업 맞춤형 보안



04 /
데이터와 인텔리전트한
정보를 위한 게이트웨이



05 /
책임 있는 AI의 원칙



06 /
최전선의 보안





01 /

보안 기능이 우선

내장된 보안 기능은 Microsoft 제품에서 오랫동안 우선 순위로 여겨져 왔으며, Microsoft 365 Copilot에서도 예외는 아닙니다. 기존 Microsoft 365용 보안 기능에 의존하는 기능부터 Copilot 자체의 작동 방식에 이르기까지 Copilot은 데이터, 인프라 및 개인 정보를 보호하는 동시에 기존 시스템과 통합되도록 설계되었습니다.

특히 Copilot 보안의 강점은 데이터 처리 방식, 내장된 개인정보 보호 제어 기능, AI 모델 자체의 학습 방식에 뿌리를 두고 있습니다. Copilot을 통해 데이터를 안전하게 보호하고 비공개로 유지하는 방법을 살펴보면서 이러한 주제와 기타 관련 주제에 대해 자세히 살펴보세요.

02 /

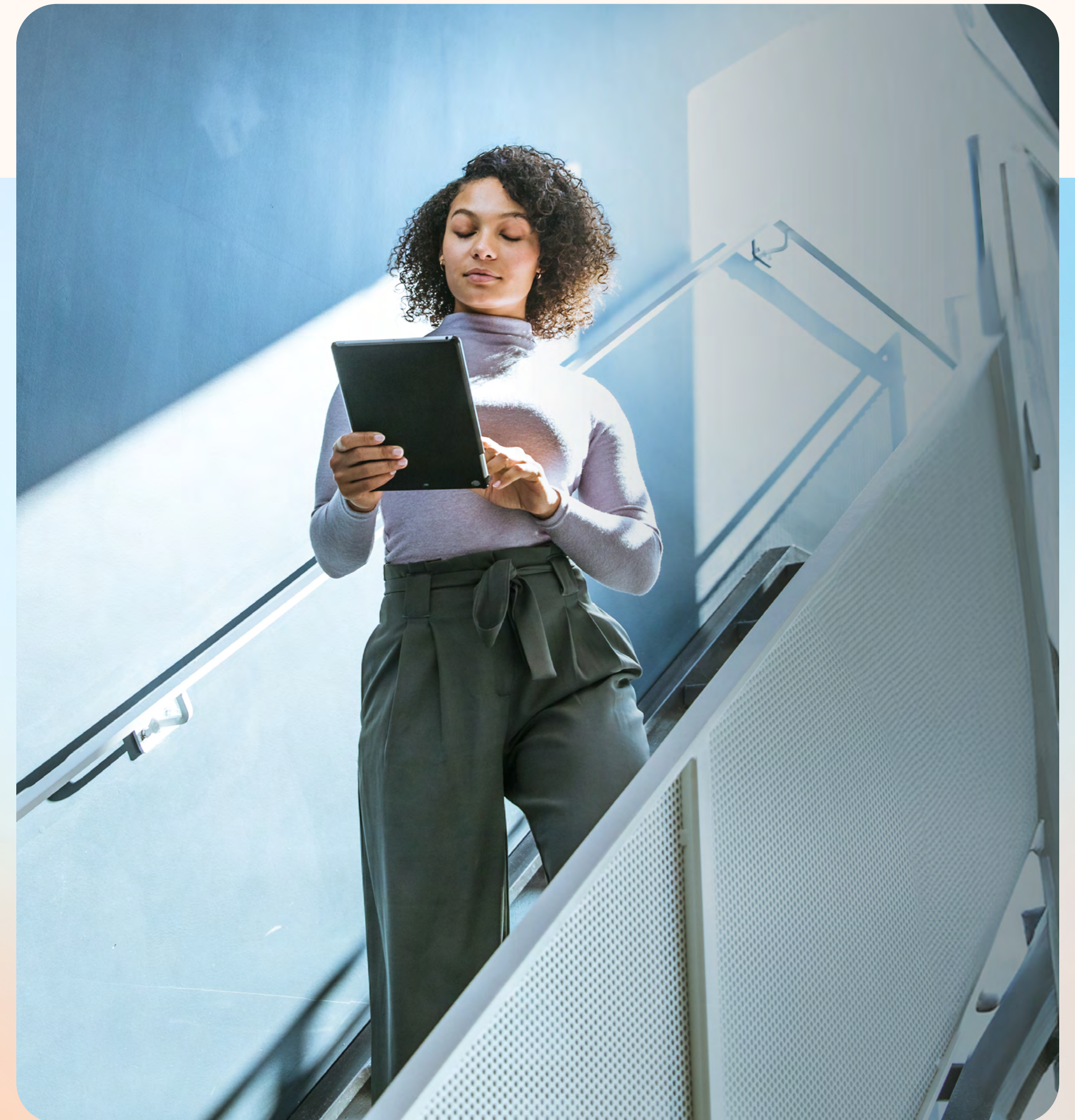
개인 맞춤형 경험

Microsoft Copilot은 생산성과 창의성을 높이는 데 도움이 될 뿐만 아니라 개인화된 방식으로 이를 수행할 수 있도록 설계되었습니다. 여러분이 상호 작용하는 Copilot 인스턴스는 회사의 모든 사람이 연결되는 중앙 집중식 리소스가 아닙니다. 여러분만의 고유한 리소스입니다.

Copilot은 여러분이 진행 중인 프로젝트, 우선 순위, 글쓰기 스타일, 가장 자주 협업하는 사람 등을 통해 인사이트를 얻습니다. 즉, 이메일과 미팅을 요약하고, 실행 항목을 파악하고, 문서 콘텐츠 작성을 도와주는 등 개인화된 경험을 제공합니다. Copilot을 더 많이 사용할수록 쿼리에 응답하고 작업을 수행하는 데 더 유용하고 정확하게 사용할 수 있습니다.

하지만 Microsoft를 포함하여 그 누구도 Copilot 데이터에 액세스할 수 없다는 점을 명심하세요. 그 이유는 Copilot이 조직의 기존 Microsoft 365 보안, ID 및 규정 준수 정책을 상속하기 때문입니다. 즉, 설계상 사용자가 액세스할 수 있는 데이터와 동일한 데이터에만 액세스할 수 있습니다.

이는 사실상 기존 보안 아키텍처를 Copilot을 중심으로 확장하는 것으로, Microsoft 365용 Copilot과의 통합의 또 다른 장점입니다. 또한 보안 기능을 더 쉽게 구성하고 관리할 수 있는 동시에 Copilot 자체를 더 안전하게 만들 수 있습니다.



03 /

기업 맞춤형 보안

Microsoft 보안 지원

보안, 개인 정보 및 ID에 대한 Microsoft의 포괄적인 접근 방식은 고급 암호화 기능, 강력한 도구, 제로 트러스트 프레임워크에 대한 옹호 및 지원, 규정 준수 기능, 투명성에 대한 약속, 책임 있는 AI 원칙을 결합하여 조직에서 Copilot이 안전하고 윤리적으로 사용될 수 있도록 보장합니다.

암호화

Copilot은 Microsoft 365에 포함되어 있으므로 데이터를 저장하거나 사용하는 동안 데이터를 보호하는 내장된 암호화 기능의 이점을 누릴 수 있습니다. "미사용" 데이터는 암호화되며, Copilot 구성 요소와 서비스 간에 전송 중인 데이터는 TLS 암호화를 통해 보호됩니다.

앞서 언급했듯이 조직의 권한 및 액세스 정책에 따라 Microsoft 365 테넌트 내의 사용자만 데이터에 액세스할 수 있습니다. 따라서 IT 조직은 Microsoft 365 서비스에서 제공되는 사용 권한 모델을 사용하여 조직 외부의 사용자를 포함한 적절한 사용자 또는 그룹이 적절한 데이터에 액세스할 수 있도록 해야 합니다.

사용자가 제어하는 데이터

생산성 향상을 위해 데이터에 액세스하고 공유할 수 있는 앱과 기술을 제어하는 것은 데이터 보안을 유지하는 데 있어 중요한 부분입니다.

Microsoft는 사용자가 명시적으로 권한을 부여하지 않는 한 사용자의 데이터를 타사와 공유하지 않습니다. Copilot은 사용자가 동의하지 않는 한 LLM을 교육하거나 다른 제품을 개선하기 위해 액세스할 수 있는 데이터를 사용하지 않습니다. 입력한 프롬프트와 해당 응답은 다른 사용자도 액세스할 수 없습니다. 특정 파일이나 폴더를 Copilot 액세스에서 제외하여 응답의 컨텍스트로 사용하지 않도록 할 수도 있습니다.

데이터 제어에 대한 Microsoft의 접근 방식은 정보를 안전하게 보호하는 데 도움이 되지만, 사용자에게 제어 권한을 부여함으로써 성공적인 채택에 필수적인 신뢰를 구축하는 데 도움이 됩니다. 사용자가 자신의 Copilot 데이터를 제어할 수 있고 책임감 있게 처리된다는 사실을 알면 데이터를 신뢰하고 데이터를 최대한 활용할 가능성이 높아집니다.

데이터 스토리지

Copilot은 Microsoft Azure 클라우드 내에서 완전히 실행되며 기업의 데이터 보안 및 개인 정보 보호에 대한 최신 Microsoft의 약속에 부합하도록 구축되었습니다.

Microsoft는 이 규정이 발효된 이후 모든 제품과 서비스가 GDPR을 준수하도록 최선을 다하고 있습니다. 따라서 Copilot의 운영 방식은 GDPR은 물론 EU 및 기타 데이터 경계 표준도 준수합니다.

기타 중요한 보안 및 개인정보 보호 사항은 다음과 같습니다.

- Copilot은 Microsoft Entra ID를 인증에 사용하며, 업무용 계정을 사용하여 엔터프라이즈급 데이터 보호가 적용된 사용자만 액세스할 수 있습니다.
- 채팅 세션이 시작될 때 Entra ID 사용자의 테넌트 및 사용자 정보가 채팅 데이터에서 제거됩니다. 이 정보는 사용자가 엔터프라이즈급 데이터 보호를 받을 자격이 있는지 여부를 판단하는 데만 사용됩니다.

제로 트러스트 적용

Copilot의 보안 기능을 극대화하기 위한 방법 중 하나는 제로 트러스트 프레임워크에 통합하는 것입니다. 제로 트러스트는 각 사용자 세션에 대한 명시적 인증, 사용자에게 해당 시점에 필요한 최소한의 네트워크 및 데이터 액세스 권한을 제공하는 최소 권한 액세스, 보안 사고 발생 시 영향을 최소화하기 위한 침해 가정 태세 등의 원칙을 기반으로 구축된 기업 보안 전략입니다. 따라서 Copilot이 이러한 원칙에 부합하는지, 그리고 기업에서 이를 어떻게 구현하고 있는지 확인하는 것이 중요합니다.

제로 트러스트 원칙

- **명시적 검증:** 항상 사용 가능한 모든 데이터 요소를 기반으로 인증하고 권한을 부여합니다.
- **최소 권한 액세스 활용:** 적시에 적절한 액세스 권한, 위험 기반 적응 정책 및 데이터 보호로 사용자 액세스를 제한합니다.
- **침해 가정:** 피해 반경을 최소화하고 액세스를 세분화합니다. 엔드 투 엔드 암호화를 확인하고 분석 기능을 사용하여 가시성을 확보하고, 위협을 탐지하며, 방어를 개선합니다.

다음 단계는 제로 트러스트 원칙을 적용하는 방법에 대한 높은 수준의 지침을 제공하면서 Microsoft 365용 Copilot 환경을 준비하는 방법을 알려 줍니다.

1

데이터 보호를 배포하거나 검증합니다.

2

ID 및 액세스 정책을 배포하거나 유효성을 검사합니다.

3

앱 보호 정책을 배포하거나 검증합니다.

4

디바이스 관리 및 보호를 배포하거나 유효성을 검사합니다.

5

위협 보호 서비스를 배포하거나 검증합니다.

6

Teams를 사용하여 안전한 협업을 배포하거나 검증합니다.

7

데이터에 대한 사용자 권한을 배포하거나 유효성을 검사합니다.



규정 준수

다른 기업 활동 및 데이터와 마찬가지로 Copilot과 같은 AI 기반 기술도 보안 및 규정 준수 관리가 필요합니다. Copilot은 Microsoft 365와 통합되어 있으므로 Microsoft Purview 규정 준수 기능을 사용하여 다음과 같은 위험 및 규정 준수 요구 사항을 지원할 수 있습니다.

- 민감도 레이블
- 데이터 분류
- 고객 키
- 커뮤니케이션 규정 준수
- 감사
- 콘텐츠 검색
- eDiscovery
- 보존 및 삭제
- 고객 Lockbox

04 /

데이터와 인텔리전트한 정보를 위한 게이트웨이

Copilot의 가장 가치 있는 이점 중 하나는 Microsoft Graph에 대한 액세스입니다. 따라서 보안, 개인정보 보호 및 규정 준수와 관련하여 이 둘의 관계와 그 관계를 이해하는 것이 중요합니다.

Microsoft Graph란?

Microsoft Graph는 Microsoft 에코시스템 내에서 여러 서비스, 디바이스 및 해당 데이터를 연결하는 안전하고 통합된 API 개발자 플랫폼입니다. Microsoft 365 Copilot의 경우 일정 데이터, 이메일 파일 및 조직 구조가 포함됩니다.

Copilot과 가장 관련이 깊은 Microsoft Graph는 ID 및 액세스 관리, 생산성 및 협업, 사람 및 워크스페이스 인텔리전트한 기능을 향상하기 위한 몇 가지 옵션을 제공합니다.



ID 및 액세스 관리

Microsoft Entra ID Governance를 사용하면 적절한 사람이 적절한 리소스에 적시에 적절한 액세스 권한을 갖도록 보장할 수 있습니다. 여기에는 사용자, 그룹, 애플리케이션이 포함될 수 있으며 사용자는 직원, 비즈니스 파트너, 공급업체 또는 계약업체를 지칭할 수 있습니다.

액세스 검토, 권한 관리, 수명 주기 워크플로, 권한 있는 ID 관리 및 사용 약관과 같은 Microsoft Graph의 ID 거버넌스 API를 사용하여 프로그래밍 방식으로 Microsoft Entra ID Governance 기능을 관리합니다.

Microsoft Entra ID Protection API 및 워크로드 ID API는 손상이 발생하기 전에 ID 기반 위험을 감지하고 완화하는 데 도움이 됩니다. 또한 피싱 방지 방법을 포함한 다중 인증을 구성하여 손상된 자격 증명과 관련된 위험을 줄일 수 있습니다.

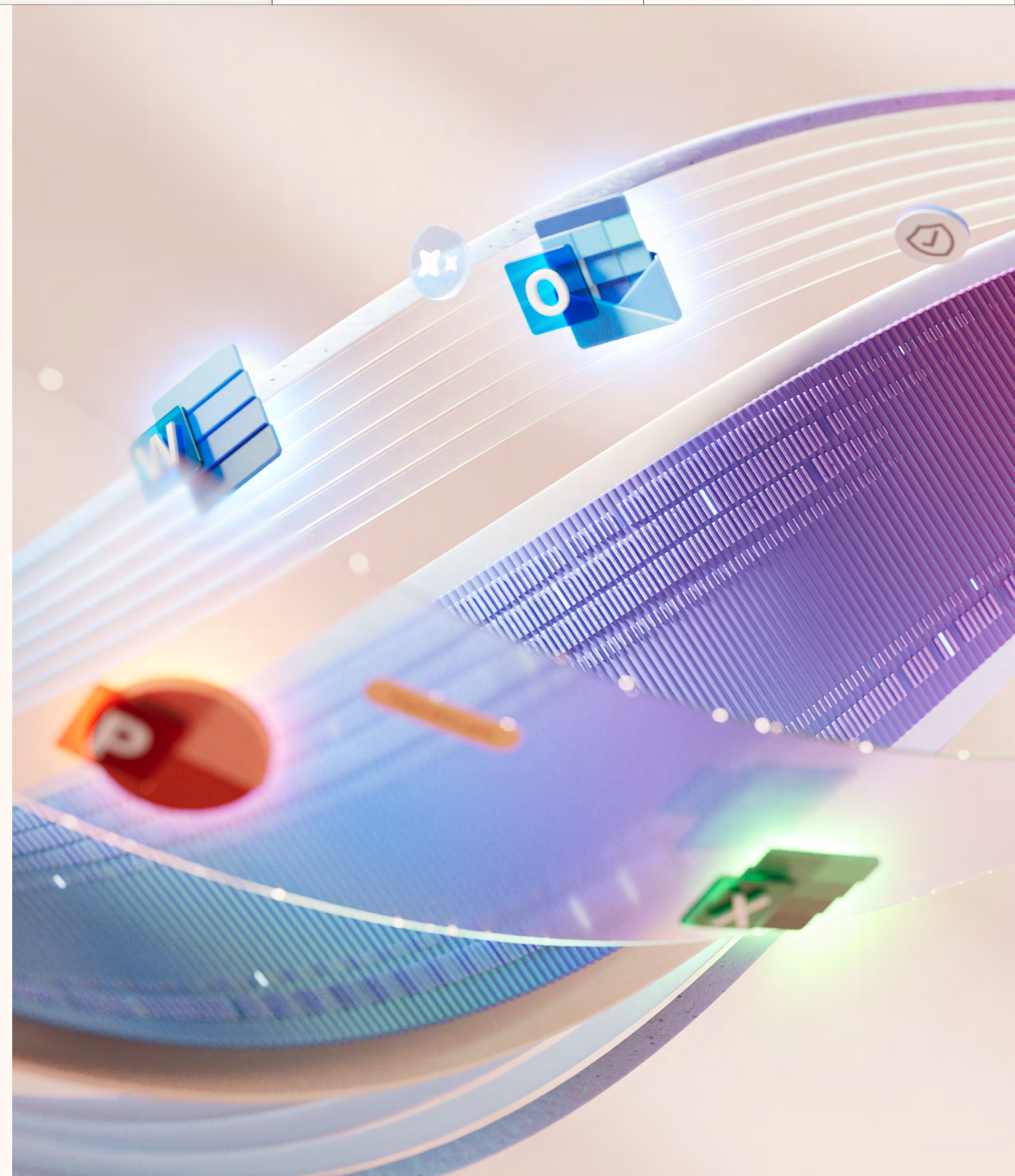
생산성 및 협업

Microsoft Graph는 Microsoft 365와의 통합을 지원하며 사람 중심의 가치 있는 데이터와 인사이트에 액세스할 수 있는 REST API 및 클라이언트 라이브러리를 제공합니다. Microsoft Graph를 사용하면 비즈니스 리소스와 사용자 데이터를 보호하면서 사용자 생산성, 창의성 및 팀 협업을 향상시키는 안전한 애플리케이션을 빌드할 수 있습니다.

Microsoft Graph 보안 커넥터는 통합 스키마를 사용하여 다양한 Microsoft 및 파트너 보안 제품 및 서비스를 연결할 수 있도록 도와줍니다. 보안 운영을 간소화하고 위협 보호, 탐지 및 대응 기능을 개선합니다.

사람 및 워크스페이스 인텔리전스

Microsoft Graph 커넥터를 사용하면 비정형 비즈니스 데이터를 Microsoft Graph로 수집할 수 있습니다. 이 데이터는 Microsoft Graph의 일부가 되어 Microsoft 365 Copilot이 엔터프라이즈급 콘텐츠를 추론할 수 있게 해줍니다.



개발자는 다음 Microsoft Graph 커넥터 API를 사용하여
사용자 맞춤형 커넥터를 빌드하여 특수한 Copilot 앱과
기능을 만들 수 있습니다.

사람 API

사람과 관련된 사용자 데이터에
액세스하기 위한 더 스마트한
앱을 구축할 수 있습니다.

인사이트 API

사용자 활동 및 상호 작용에
대한 인사이트를 제공합니다.

프로필 API

사용자 프로필 및 관련 정보에
액세스합니다.

프로필 카드 API

사용자의 프로필 카드
데이터를 검색합니다.



05 /

책임 있는 AI의 원칙

Copilot과 같은 AI 솔루션을 배포할 때 신뢰를 구축하는 또 다른 중요한 부분은 윤리적 AI 의사 결정과 책임 있는 사용 사례 측면에서 조직의 가치를 지원하는지 확인하는 것입니다. Microsoft는 이러한 요구 사항과 기타 여러 잠재적인 문제를 해결하기 위해 책임 있는 AI 표준을 개발했습니다.

따라서 Copilot은 AI 제품으로서 Microsoft 연구, 정책 및 엔지니어링 팀에서 개발한 책임 있는 AI 원칙에 따라 개발되었으므로 조직에 AI를 통합하려는 방식과 어떻게 일치하는지 더 잘 파악할 수 있습니다.



책임 있는 AI 사용을 위한 Microsoft의 5가지 원칙

책임	투명성	공정성	개인정보 보호 및 보안	포용성
AI 시스템을 평가하여 사람, 조직, 사회에 중대한 악영향을 미칠 수 있는 경우와 해당 시스템에 추가적인 감독 및 요건을 적용해야 하는지 여부를 파악할 수 있도록 합니다.	Microsoft는 이해 관계자가 해당 시스템에 대해 정보에 입각한 선택을 할 수 있도록 지원하기 위해 AI 시스템이 수행할 수 있는 작업과 수행할 수 없는 작업에 대한 정보를 제공합니다. 시스템 자체는 사용자가 AI 시스템과 상호 작용하고 있거나 진짜인 것처럼 보일 수 있는 이미지, 오디오 또는 비디오 콘텐츠를 생성하거나 조작하는 시스템을 사용하고 있음을 사용자에게 알리도록 설계되어 있습니다.	Microsoft AI 시스템은 편견을 차별하거나 지속시키지 않도록 설계되었으며, 소외된 그룹을 포함하여 식별된 인구 통계 그룹에 대해 유사한 품질의 서비스를 제공하고 고정 관념, 비하 또는 삭제 가능성을 최소화하도록 설계되었습니다.	Microsoft AI 시스템은 Microsoft 개인 정보 보호 표준에 따라 개인 정보를 보호하고 Microsoft 보안 정책에 따라 보안을 유지하도록 설계되었습니다.	Microsoft AI 시스템은 Microsoft 접근성 표준에 따라 포괄적으로 설계되었습니다.

06 /

최전선의 보안

AI 솔루션은 생산성과 창의성을 향상시킬 수 있는 잠재력을 가지고 있지만, 이러한 기능 중 많은 부분이 Copilot에 내장되어 있어 더욱 안전하게 사용할 수 있습니다. Microsoft의 지원을 받는 Copilot은 데이터 및 디바이스 보안, 개인 정보 보호 또는 규정 준수를 손상하지 않는 환경에서 안심하고 AI의 잠재력을 실현할 수 있도록 도와줍니다.

Copilot이 데이터 보안을 유지하면서 직원들의 역량을 강화하는 데 어떻게 도움이 되는지 자세히 알아보세요.