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

Microsoft 365 협업&보안 Hands On Lab 워크샵

데이터에 가치를 더하여 고객의 성장에 공헌합니다.

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

M. Cloud Bridge
Specialized Consulting Firm in Data & AI

Agenda

2. Microsoft 365 & EMS 활용한 장치 보안, 계정 보안, 데이터 보안 환경 만들기

2. Microsoft 365 & EMS를 활용한 계정 보안, 장치 보안, 데이터 보안 환경 만들기

2-1. Microsoft 365 EMS 소개
2-2. 계정 보안 Hands On Lab(실습)
2-3. 장치 보안 Demo
2-4. 데이터 보안 Hands On Lab(실습)

2-1. Microsoft 365 EMS 소개

Microsoft 365의 보안은 Entra의 아이덴티티와 액세스 관리, 클라우드 인프라 권한 관리, 신원 검증을 사용하고, Intune으로 모바일 장치와 앱을 관리하고 보호하며, Purview로 데이터를 탐색하고 분류하고 보호하여, 다양한 위협으로 부터 데이터 자산을 안전하게 보호 할 수 있는 환경을 제공 합니다.

Microsoft 365 Enterprise Mobility Security

계정 보안(Entra)
강력한 보안 및 인증을 통해 계정을 보호

장치 보안(Intune)
모바일과 데스크톱 장치를 안전하게 관리하고 보호

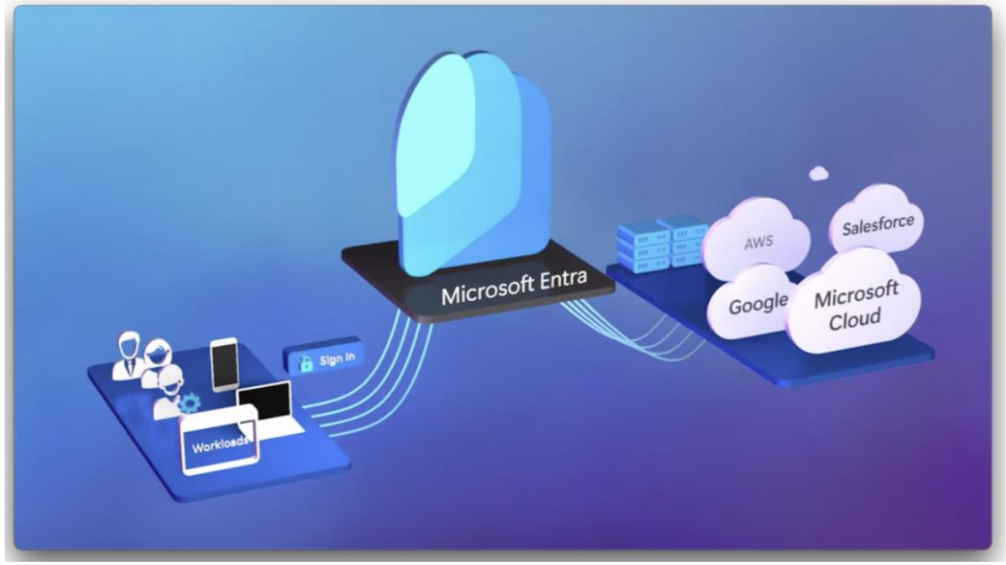
데이터 보안(Purview)
데이터의 보안과 개인 정보 보호 및 강화

Microsoft Entra는 모든 ID 및 액세스 기능을 포괄하는 제품군으로, Entra 제품군 내에는 Microsoft Azure AD(Azure Active Directory), Microsoft Entra Verified ID 및 Microsoft Entra Permissions Management가 있고, Microsoft Entra의 관리 센터를 사용하면 한곳에서 권한을 찾고 액세스를 관리할 수 있습니다.

Microsoft Entra(계정 보안)

모든 앱 또는 리소스에 대한 액세스 보호
모든 사용자의 모든 앱과 리소스에 대한 액세스를 보호하여 조직을 보호

필요한 액세스만 제공
권한 검색 및 크기 조정, 액세스 수명 주기 관리, 모든 ID에 대한 최소 권한 액세스 보장



경험 단순화
간단한 로그인 환경, 지능형 보안 및 통합 관리를 통해 사용자의 생산성을 유지

모든 ID 보안 및 확인
모든 환경에서 직원, 고객, 파트너, 앱, 장치 및 워크로드를 포함한 모든 ID를 효과적으로 보호

Azure Active Directory

사용자, 앱, 워크로드 및 디바이스 보호

권한 관리

CIEM(클라우드 인프라권한 관리) 제품으로 권한 위험을 발견, 교정 및 모니터링

인증된 ID

신원 자격 증명 확인을 자동화하고 조직과 사용자 간의 개인 정보 보호 상호 작용을 가능하게 함

Microsoft Intune은 다양한 플랫폼과 장치를 통합적으로 관리하고 보호할 수 있는 클라우드 기반의 서비스로, 조직의 자원에 대해 인증을 요구하는 보안 모델인 Zero Trust 보안 아키텍처를 강화 및 장치의 상태, 준수 등 보안 상태를 확인하여, 회사 데이터를 안전하게 보호할 수 있는 기능을 제공합니다.

Microsoft Intune(장치 보안)

Microsoft Intune

- ❖ 클라우드 기반 운영
- ❖ 중앙 집중식 관리
- ❖ 라이선스 관리와 소프트웨어 배포 통합
- ❖ 보안 및 규정 준수

엔드포인트 관리 통합

① 다양한 디바이스와 운영 체제를 중앙에서 앱 배포 및 정책 제어 관리

② 디바이스 등록, 애플리케이션 배포 설정 관리

보안 강화

① 디바이스 암호화,원격 데이터 삭제,액세스 제어 등 엔드 포인트 보안 강화

② 취약점 관리, 맬웨어 탐지 등 데이터 및 디바이스에 대한 보호 강화

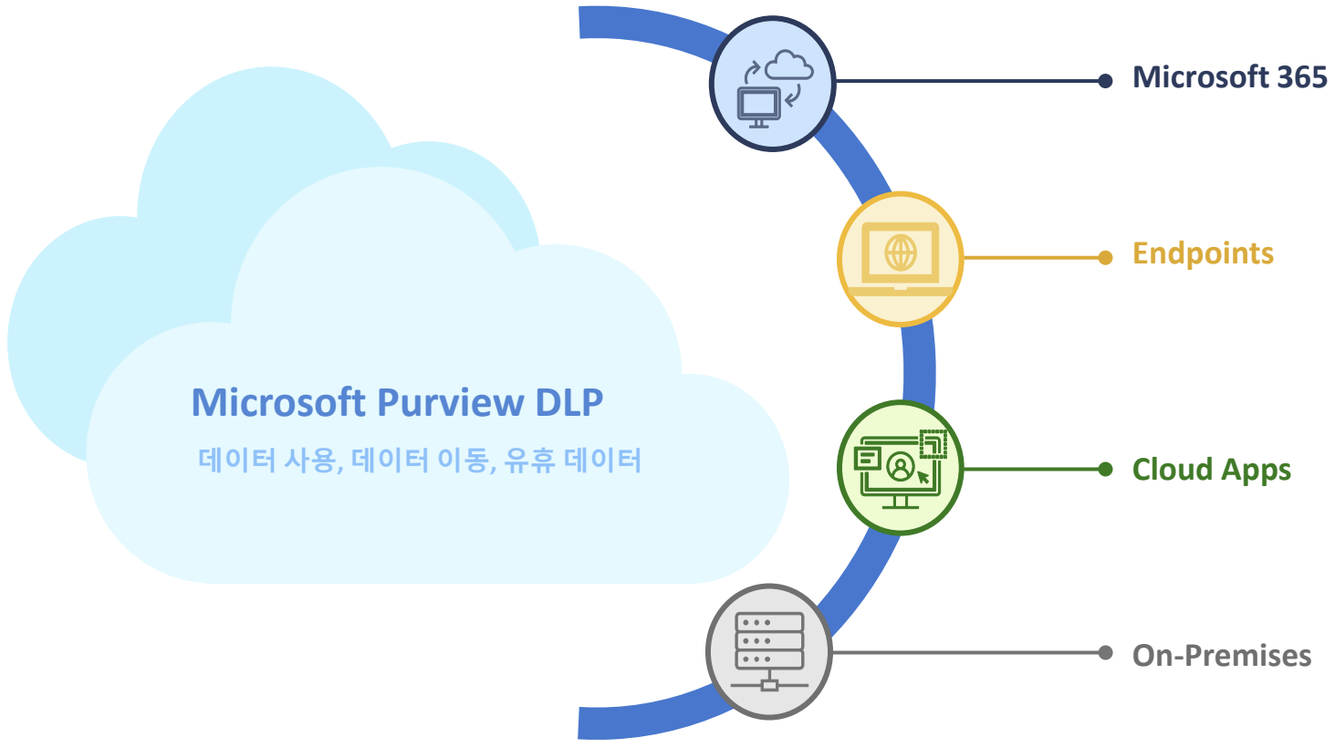
비용 절감

① 클라우드 기반으로 운영되어 하드웨어나 인프라 구축에 드는 비용을 절감

② 중앙 집중식 관리와 자동화된 기능을 통해 IT 관리자의 작업 시간을 절감

Microsoft Purview는 자동화된 데이터 검색, 중요한 데이터 분류 및 엔드투엔드 데이터 계보를 통해 데이터 환경에 대한 전체적인 최신 맵을 만들 수 있고, 데이터 큐레이터 및 보안 관리자가 데이터 자산을 안전하게 유지해 주고 데이터 소비자가 데이터를 쉽게 검색하여 사용 할 수 있게 지원 합니다.

Microsoft Purview(데이터 보안)



기업을 위한 DLP 활용 사례

회사 내 중요한 데이터를 효과적으로 보호하려면 다음 활용 사례를 참고 하세요

- ✓ 민감한 데이터 식별 및 분류
- ✓ 데이터 유출 방지 정책 설정
- ✓ 조직 내 외부 데이터 공유제어
- ✓ 보고서 및 감사

2-2. Microsoft 365 EMS 계정 보안 환경 만들기

다단계 인증이란 사용자가 웹사이트나 애플리케이션에 로그인할 때 암호 외에도 추가적인 인증 요소를 제공해야 하는 보안 방식으로, 이 방식은 사용자의 ID를 보다 정확하게 확인 및 비밀번호가 노출되거나 도용되더라도 계정을 보호할 수 있으며, 제로 트러스트 보안 모델을 구현하는 데 도움이 됩니다.

Multi-Factor Authentication

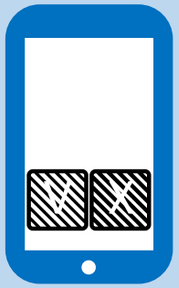
지식 기반

<사용자만 알고 있는 것>

패스워드
PIN

소유 기반

<사용자만 소유하고 있는 것>



문자 메시지
앱 푸쉬
USB토큰

속성 기반

<사용자만의 고유한 속성>

지문
얼굴 스캔
홍채 스캔

MFA로 가능한 인증 방법

MFA는 사용자의 신원을 확인하기 위해 여러 인증 요소를 요구하므로, 해킹, 불법 접근, 사회 공학적 공격 등의 보안 위협으로 부터 사용자를 보호하는 데 도움이 됩니다.

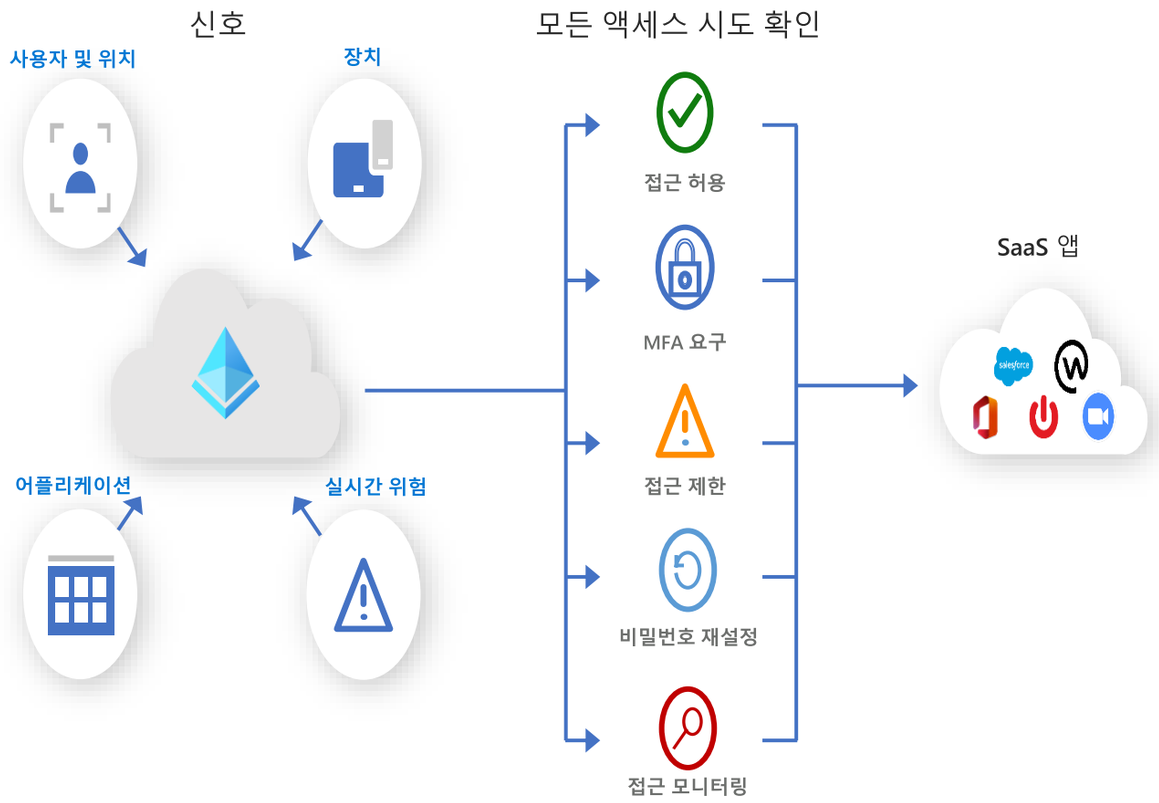
① **비밀번호**: 사용자의 기존 비밀번호를 입력하는 것으로 첫 번째 인증 요소입니다.

② **다양한 인증 방법**: 예를 들어, 스마트폰 앱으로 생성된 일회용 인증 코드, SMS로 전송된 코드, 하드웨어 토큰 등을 사용합니다.

③ **생체 인증**: Windows Hello를 통한 지문, 안면 인식 등과 같은 생체적인 특징을 사용하여 인증합니다

조건부 액세스란 사용자의 신원, 장치, 위치, 네트워크 등의 조건을 기반으로 애플리케이션 및 데이터에 대한 액세스를 허용하거나 제한하는 보안 기능으로, 조건부 액세스를 사용하면 조직은 보안 위험을 최소화하면서 사용자의 생산성과 편의성을 높일 수 있어 보다 안전한 업무 환경이 구성 됩니다.

조건부 액세스



조건부 액세스의 기능과 활용 사례

조건부 액세스 기능은 조직의 보안을 강화하기 위해 사용되는 기능입니다.
이 기능을 사용하면 **사용자가 클라우드 리소스에 접근하기 위해** 만족해야 하는 조건을 정의할 수 있으며, 이 조건은 사용자의 **위치, 사용하는 디바이스의 상태, 사용자의 역할** 등과 같은 다양한 요소에 기반하여 설정할 수 있습니다.

① **위치 기반 액세스 제어**: 회사의 보안 정책상 특정 국가 이외에서의 액세스를 차단하고자 합니다.

② **MFA 강제 사용**: 관리자 권한을 가진 사용자에게 추가적인 보안 인증을 요구하기 위해 MFA를 강제로 사용하도록 설정합니다.

③ **시간 기반 액세스 제어**: 회사의 업무 시간 외에는 액세스를 차단하고자 합니다. 따라서, 조건부 액세스를 설정하여 업무 시간 내에만 액세스를 허용합니다.

④ **조건 추가**: 특정 디바이스에서만 액세스를 허용할 수 있습니다.

Identity Protection는 로그인 및 액세스 패턴을 분석하고 이상한 활동이나 잠재적인 보안 위협을 탐지하며 알려진 위협과 사용자의 이전 행동을 비교하여 보안 이벤트를 분석하고, 경고를 생성하고, 악의적인 사용자의 액세스를 차단하거나, 사용자에게 추가적인 인증 단계를 요청할 수 있습니다.

Identity Protection

수조 개의 신호로 구동되는 고유한 인사이트

자동 생성
- 고품질 heuristic 기반 탐지
- 다른 것으로부터 탐지

전문가 생성
- 보안 연구원
- 고객지원
- 전문적인 인력 할당

최종 사용자 생성
- 피드백 루프/구축
- 사용자/관리자/보안 운영팀
- 오류제거

실시간 엔진 위험 평가

위험한 사용자

위험한 로그인

위험한 앱

정책 강제 실행 및 통합 조사 경험을 통한 안전한 액세스

위험 기반 CA 정책을 사용한 자동복구

계정 보호 위험 보고 대시보드와 Microsoft Graph API

Azure 모니터 및 Azure Sentinel과 통합

제3자 SIEM으로 위험 경고 라우팅

계정 보호 정책

Azure AD 조건부 액세스는 로그인 위험 및 사용자 위험이라는 두 가지 위험 조건을 제공합니다. 조직은 이러한 두 가지 위험 조건을 구성하고 액세스 제어 방법을 선택하여 위험 기반 조건부 액세스 정책을 만들 수 있습니다.

로그인 위험 기반: 사용자의 로그인 활동과 관련된 위험을 평가하기 위해 사용되는 접근 방식입니다.
① 액세스 차단
② 액세스를 허용하지만 암호변경 필요

사용자 위험 기반:사용자의 행동 패턴과 특성을 분석하여 사용자의 보안 위험

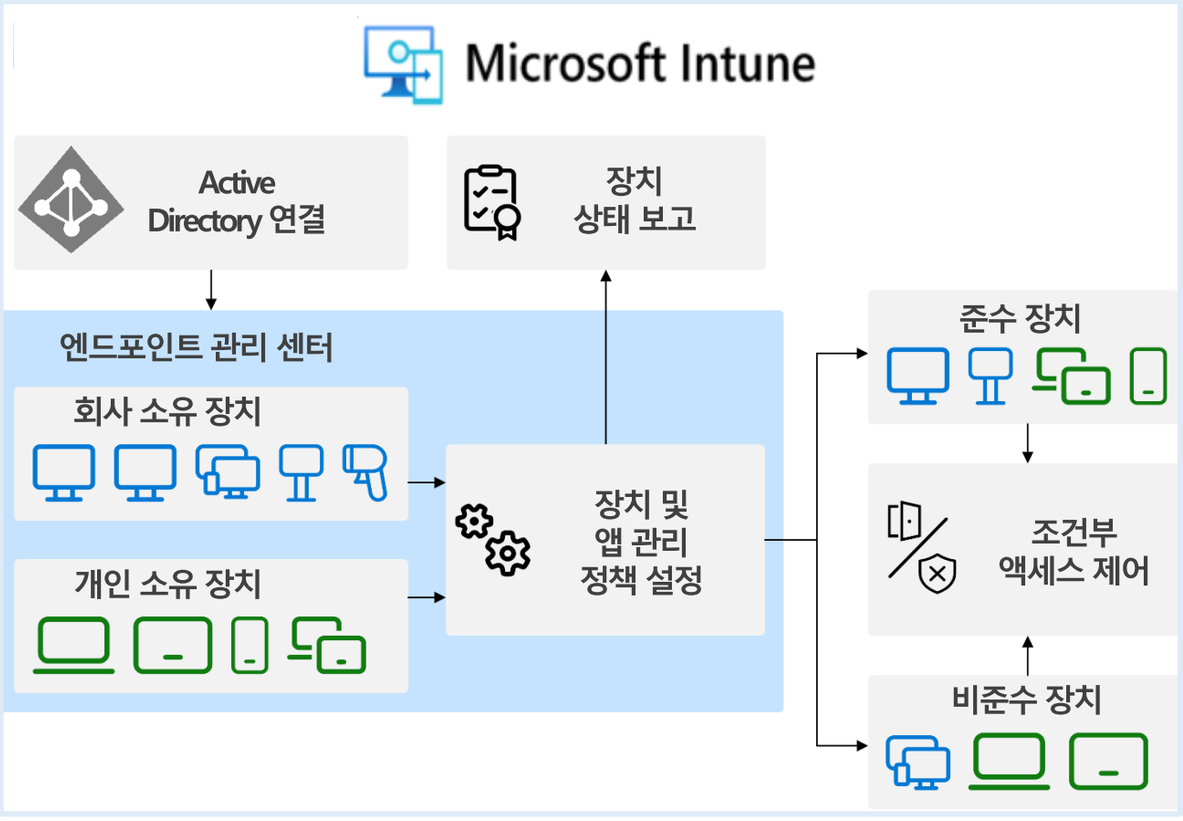
① 수준을 평가하고 필요한 조치를 취할 수 있습니다.
② 로그인 실패, 다중 계정 사용, 이상한 로그인 위치 등의 이상적인 활동을 감지

Microsoft 365 EMS 계정 보안 Hands On Lab(실습)

2-3. Microsoft 365 EMS 장치 보안 환경 만들기

Microsoft Intune은 클라우드 기반의 엔드포인트 관리 도구로 Azure Active Directory를 통한 조건부 액세스와 직접 통합하여 구성원의 장치가 회사 정책을 준수하고 있는지 식별할 수 있으며 모바일, 데스크톱 및 다양한 엔드포인트의 사용자별 접근 제어와 보안 정책을 간소화하여 관리할 수 있습니다.

Microsoft Intune



Intune 주요 기능 및 이점

① **장치 통합 관리:** 조직이 소유한 장치 및 사용자 개인 소유의 장치 정보를 확인하고 관리할 수 있습니다.

② **앱 배포 간소화:** 앱 배포, 업데이트 및 제거를 비롯한 기본 제공 앱 환경을 사용하여 사용자의 관리를 간소화합니다.

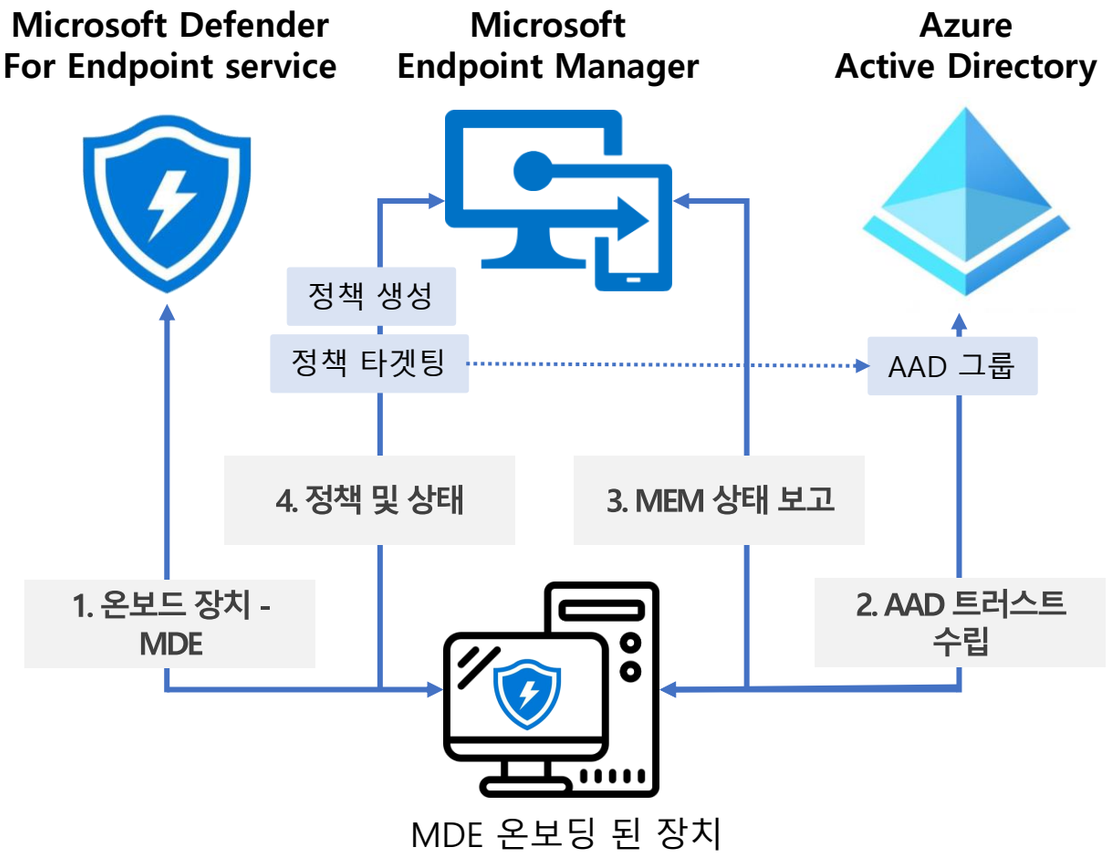
③ **정책 자동화:** Intune 앱, 보안, 디바이스 구성, 규정 준수, 조건부 액세스 등에 대한 정책 적용을 자동화할 수 있습니다.

④ **장치 보안 강화:** 보안 정책을 활성화하여 사이버 공격을 감지 및 차단하고, 위협에 해당되는 내용을 보고서로 확인할 수 있습니다.

⑤ **액세스 제어:** 조건부 액세스와 결합하여 비준수 장치에 대한 접근을 제어할 수 있습니다.

엔드포인트용 Microsoft Defender는 실시간으로 디바이스에 대한 악성 소프트웨어, 악성코드, 스파이웨어, 랜섬웨어 등 다양한 형태의 위협을 감지하며 이러한 감지기능들을 통해 장치와 기업의 데이터를 신뢰할 수 있는 상태로 유지하고 다른 보안 위협으로 부터 보호하는 역할을 합니다.

엔드포인트용 Microsoft Defender



Defender for Endpoint 주요 기능

Intune에 가입된 장치를 Microsoft 365 Defender에 온 보딩 하면 장치에 엔드포인트 센서가 동작하게 됩니다. 이 센서는 디바이스에서 동작신호 및 특이사항 Microsoft Defender로 보내게 됩니다.

Defender for Endpoint의 핵심 기능은

① 디바이스의 잘못된 구성이나 보안상태를 모니터링합니다

② 악성 IP주소, 도메인 및 URL에 대한 액세스에 대한 네트워크 보호를 합니다.

③ Microsoft Defender는 모든 유형의 새로운 위협을 포착하도록 설계된 차세대 보호 기능을 사용합니다.

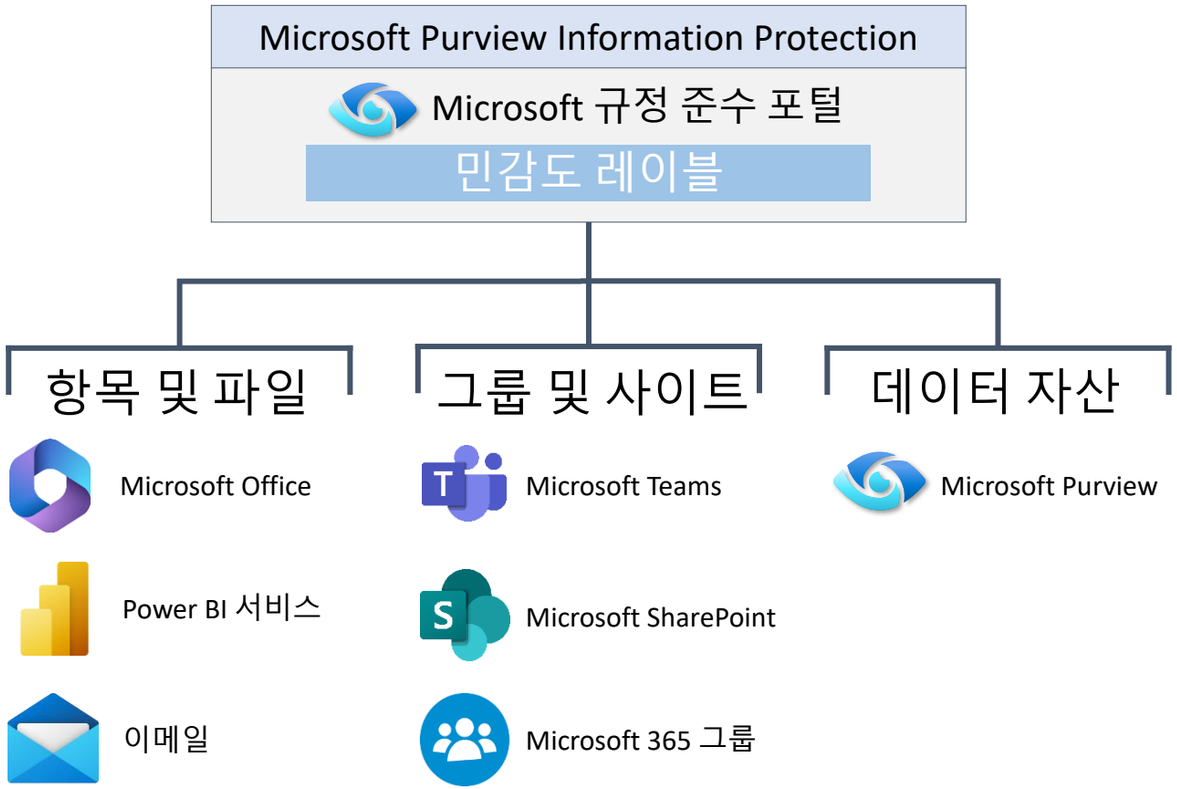
④ 지능형 공격에 신속하게 대응할 수 있는 기능과 엔드포인트용 Microsoft Defender는 규모에 따라 몇 분 만에 경고 볼륨을 줄이는 데 도움이 되는 자동 조사 및 수정 기능을 제공합니다.

Microsoft 365 EMS 장치 보안 Demo

2-4. Microsoft 365 EMS 데이터 보안 환경 만들기

민감도 레이블은 중요한 정보 유형에 따라 문서와 메일을 분류하며, 보안 정책에 따라 접근 권한 설정과 외부 액세스 제한, 문서 액세스 제어 등 다양한 작업을 수행할 수 있습니다. 이를 통해 회사는 신용카드나 주민번호와 같은 개인정보부터 기밀 정보까지 다양한 민감한 정보를 보호할 수 있습니다.

민감도 레이블



민감도 레이블의 기능과 활용 사례

민감도 레이블은 조직 내에서의 제한된 액세스와 권한 설정, 외부로 데이터 공유 보호를 지원합니다, 이를 통해 조직은 데이터 보안을 강화하고 민감한 정보의 노출을 방지할 수 있습니다.

① 조직 내의 사용자만 문서나 메일을 열 수 있습니다.

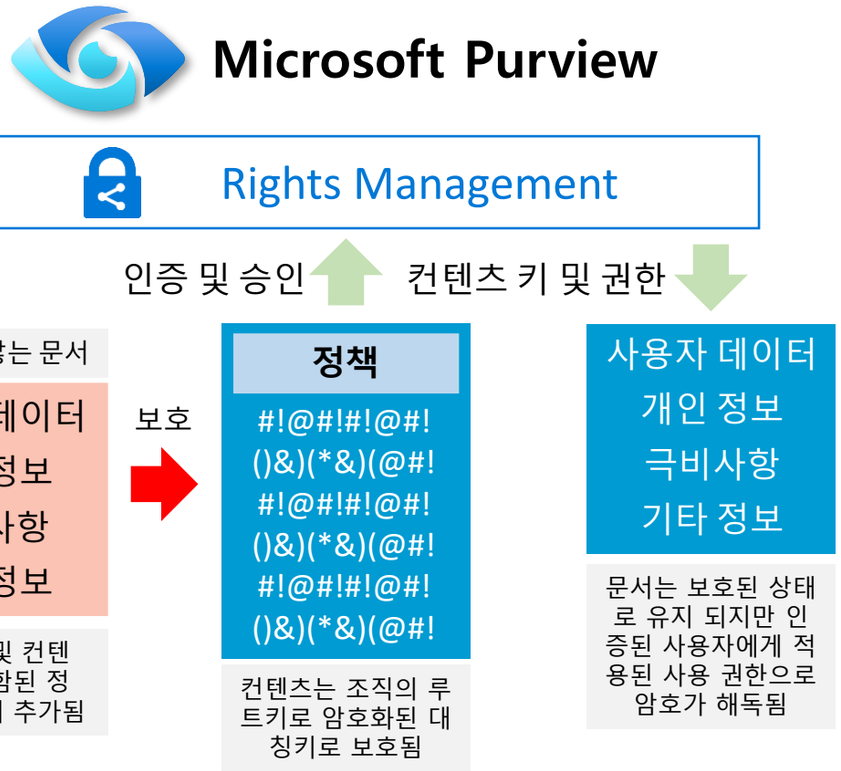
② 마케팅 부서 사용자는 문서 및 메일을 편집하고 다른 부서 사용자는 읽기만 가능합니다.

③ Power BI로 확장이 가능하며 서비스 외부에 저장된 데이터를 보호 할 수 있습니다.

④ Teams, Microsoft 365 그룹 및 SharePoint 사이트 등 개인 정보 설정, 외부 사용자 액세스 및 외부 공유, 관리되지 않는 장치의 액세스를 설정 가능합니다.

민감도 레이블 암호화는 문서, 전자 메일 및 모임 초대를 암호화하여 액세스를 제한합니다. 민감도 레이블의 암호화 설정에 따라 권한이 있는 사용자만 암호를 해독할 수 있으며, 파일의 이름이 변경되더라도 암호화된 상태가 유지됩니다. 또한, 작동 중단 시나 전송 중에도 모든 콘텐츠가 암호화됩니다.

민감도 레이블 암호화



민감도 레이블 기능과 암호화 동작 방식

문서, 전자 메일 또는 모임 초대가 암호화되면 콘텐츠에 대한 액세스가 제한되므로 다음을 수행합니다.

① 레이블의 암호화 설정에 따라 권한이 있는 사용자만 암호를 해독할 수 있습니다.
② 파일의 이름이 바뀌더라도 조직의 내부 또는 외부에 관계 없이 암호화된 상태로 유지됩니다.
③ 작동 중단 시(예: OneDrive 계정에서) 및 전송 중에 모두 암호화됩니다.

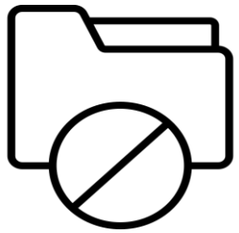
중요한 정보 유형은 조직내 문서 또는 메일에 중요한 정보 유형에 해당하는 데이터 패턴, 키워드, 규칙 등을 정의하고, 이를 기반으로 분류 규칙을 설정합니다. 예를 들어, "개인정보"라는 레이블을 가진 문서는 주민등록번호나 개인 식별 정보와 관련된 패턴을 감지하여 자동으로 분류할 수 있습니다.

중요한 정보 유형

키워드 규칙 생성

패턴 자동 감지

관리자 알림



액세스 차단

중요한 정보 유형의 기능과 활용 사례

데이터 관리 및 분석 플랫폼으로, 조직의 데이터 자산을 관리하는 도구이며 다양한 정보 유형을 인식하고 분류하여 조직 내에서 중요한 데이터를 식별할 수 있습니다. Word, Excel, PPT, Outlook등 해당되는 파일에 패턴과 일치하면 해당 파일은 중요한 정보 유형으로 분류하게 됩니다.

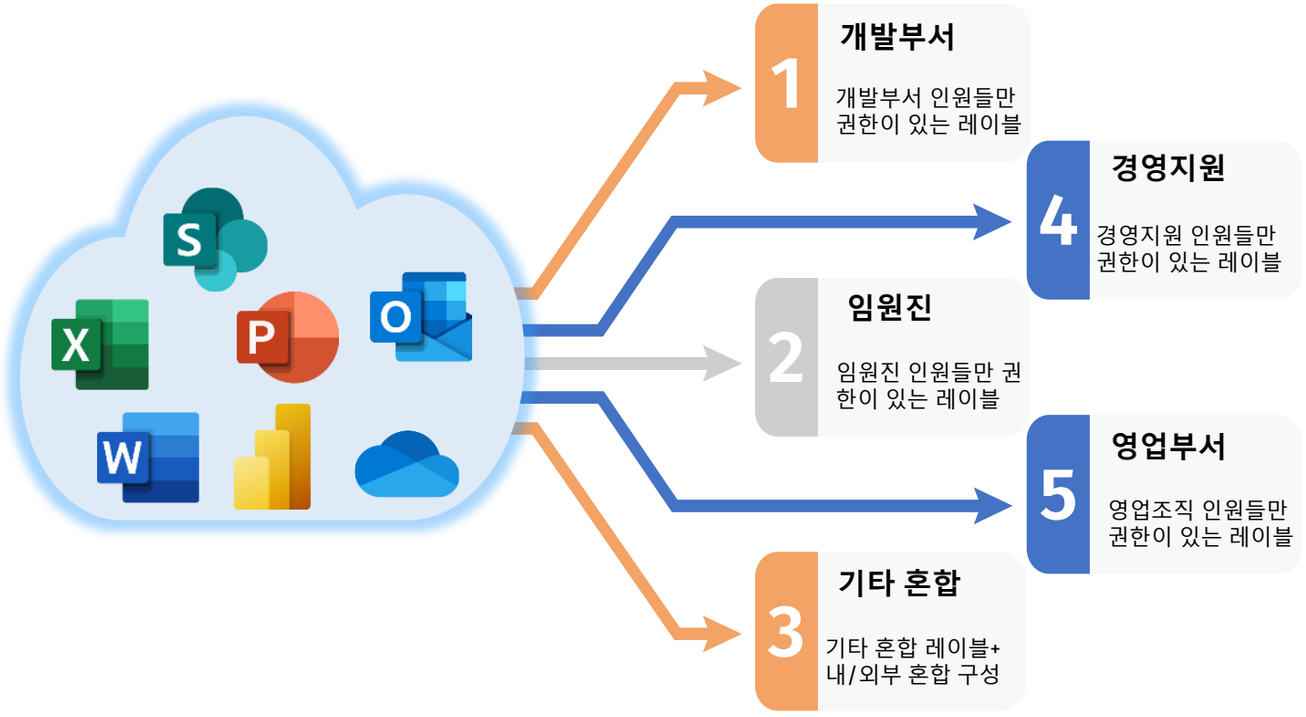
다음은 Microsoft 365 Purview에서 중요한 정보 유형의 활용 사례 입니다.

① 주민등록번호, 신용카드 번호, 전화번호
② 저작권, 특허, 상표 등과 같은 지적재산
③ 은행 계좌 정보, 금융 거래 등 재무 관리와 회계 정보
④ 거래 기록, 주문 정보, 판매 데이터
⑤ 환자 기록, 의료기록, 건강 정보

자동 라벨링은 Microsoft 365 Purview의 기능 중 하나로, 사용자가 수동으로 레이블을 할 필요 없이 민감한 정보를 자동으로 보호하는 기능입니다. 이 기능을 사용하면 중요한 정보가 포함된 전자 메일 메시지, OneDrive 파일 및 SharePoint 파일에 자동으로 민감도 레이블을 적용할 수 있습니다.

Auto-Labeling

자동 레이블 패턴 감지를 통해 다음과 같은 시나리오를 수행 가능



자동 라벨링 이점

콘텐츠에 민감도 레이블을 자동으로 적용하는 이 기능은 다음과 같은 이유로 중요합니다.

① **보안 강화**: 민감한 정보나 기밀성이 필요한 콘텐츠를 식별하고 레이블을 자동으로 적용함으로써, 조직 내 보안을 강화할 수 있습니다.

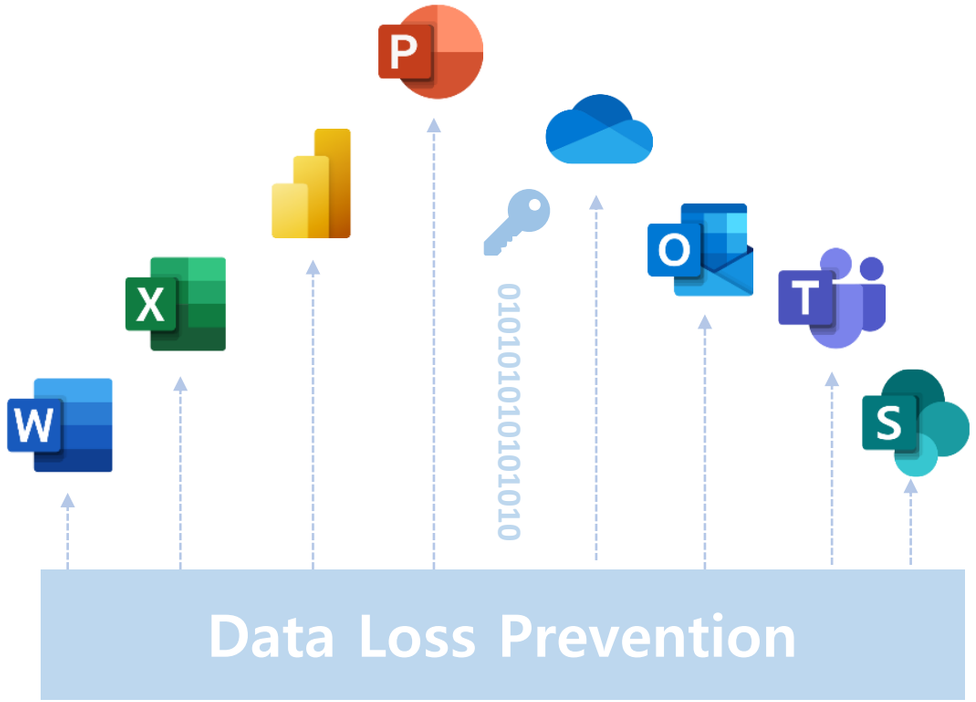
② **사용자 교육 필요 감소**: 사용자에게 콘텐츠를 분류하고 레이블을 지정할 필요가 없으므로, 사용자 교육에 대한 부담이 줄어듭니다

③ **정확성** : 사용자에게 의존하지 않고 자동으로 콘텐츠를 분류하면, 사람의 실수나 주관적인 판단으로 인한 오류를 줄일 수 있습니다.

④ **시간과 비용 절감**: 수동으로 콘텐츠를 분류하고 레이블을 지정하는 작업은 시간과 비용이 많이 소요됩니다. 자동으로 민감도 레이블을 적용하면 이러한 작업에 소요되는 인력과 비용을 절감할 수 있습니다

Data Loss Protection(DLP)는 Microsoft 365 앱 서비스에서 자동으로 데이터를 검사하고, 민감한 정보 패턴을 탐지하여 데이터 유출 위험을 평가하고 데이터 보안을 강화하기 위한 도구입니다. 이를 통해 조직은 개인 신원 정보, 금융 정보, 지적 재산 등과 같은 중요한 데이터를 보호할 수 있습니다.

Microsoft Purview DLP



DLP의 기능과 활용 사례

Microsoft Purview에서는 DLP 정책을 정의하고 적용하여 데이터 손실 방지를 구현합니다. DLP 정책을 사용하면 다음에서 중요한 항목을 식별, 모니터링 및 자동으로 보호할 수 있습니다.

① Teams, Exchange, SharePoint 및 OneDrive 계정과 같은 Microsoft 365 서비스

② Word, Excel 및 PowerPoint와 같은 Office 애플리케이션

③ Windows 10, Windows 11 및 macOS 엔드포인트

④ 온-프레미스 파일 공유 및 온-프레미스 SharePoint

⑤ Power BI

Microsoft 365 EMS 데이터 보안 Hands On Lab(실습)

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