Microsoft 365 보안 강화

- 클라우드 환경에서의 보안 강화를 위한 EMS 소개

한컴MDS 정혜진 Engineer

목차

1. Microsoft 365 소개
2. Microsoft 365 사내 보안 강화 (EMS)
3. Microsoft 365 제로 트러스트

1. Microsoft 365 소개

1. Microsoft 365 소개

- Office 365 + Windows 10 + Enterprise Mobility + Security
- 비즈니스 관리 및 운영 최적화

1. Microsoft 365 소개

1. Microsoft 365 소개

관리 센터 기능 및 설정

사용자, 그룹 및 암호 관리

전자 메일 및 일정 관리

도메인 관리

데이터 및 서비스 관리

구독 및 청구 관리

조직 보호

장치 및 앱 데이터 관리

2. Microsoft 365 사내 보안 강화 (EMS)

2. Microsoft 365 사내 보안 강화 (EMS)

- **EMS (Enterprise-mobility-security) : Microsoft 365 제품의 보안 기능 강화 위한 솔루션**

2. Microsoft 365 사내 보안 강화 (EMS)

- 다단계 인증 - 조건부 액세스 - 고급 보안 관리 - 권한 있는 사용자 ID 관리	- 모바일 APP 관리 - 통합 PC 관리	- 지속적인 데이터 보호 - 지능형 데이터 분류 및 라벨링 - 문서 추적 및 해지 - 규제 요구에 따른 암호화 키 관리	- Microsoft 지능형 위협 분석 - Microsoft 클라우드 앱 보안
ID & 액세스 관리	디바이스 및 앱 관리	정보 보호	ID기반 보안
EMS 기능	▪ Azure Active Directory ▪ Multi-Factor 인증	Intune	Azure Information Protection	▪ Cloud App Security ▪ Advanced Threat Analytics ▪ Defender for Identity

2. Microsoft 365 사내 보안 강화 (EMS)

- Single Sign-On
- Multi-Factor 인증
- 암호 재설정 등 제공

2. Microsoft 365 사내 보안 강화 (EMS)

- **AAD (Azure Active Directory) : M365 모든 제품은 Azure AD의 관리 역할로 관리 가능**

2. Microsoft 365 사내 보안 강화 (EMS)

- **AIP (Azure Information Protection) : 시용자별 권한 설정 및 문서 암호화 / 공유된 문서 추적 및 권한 회수 가능**

기존 DRM

솔루션 Agent 기반의 문서 암호화 방식

Agent 설치 필요

- 사내 : 문서 등급 (기밀, 대외비, 일반) 구분 없이 최초 작성자 무관하게 수정 가능
  공동 작업이나 외부 공유를 위해 문서 DRM 해제 작업 필요 (복호화)
- 내보내진 문서에 대해서 추적 및 조치 불가능

AIP

플랫폼 기반의 문서 단위의 권한 권리 방식 (AIP)

플랫폼 기반

- 문서 중앙화를 통해 보안 등급별 권한이 부여된 문서를 사내에서 지속 유지
  (권한 보유자 외 임의 변경 불가)
- 외부 유통 및 공유할 경우에도 대상자 등록 / 권한 지정
- 외부 공유 문서에 대한 제어 및 관리 가능

2. Microsoft 365 사내 보안 강화 (EMS)

- **AIP (Azure Information Protection)**

AIP 적용 순서

2. Microsoft 365 사내 보안 강화 (EMS)

- **AIP (Azure Information Protection)**

- 해당 문서 공유 시, AIP 에서 문서에 접근하는 사용자의 정보를 Azure AD 통해 식별

2. Microsoft 365 사내 보안 강화 (EMS)

- **AIP 도입 시 기대효과**
  - 암호화된 데이터는 누가(인증), 무엇을(권한), 언제까지(제어) 사용할 수 있도록 안전하게 공유

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

2. Microsoft 365 사내 보안 강화 (EMS)

- **ATA (Advanced Threat Analytics) : 여러 유형의 지능형 사이버 공격 및 내부자 위협으로부터 기업 보호**

2. Microsoft 365 사내 보안 강화 (EMS)

- **CAS (Cloud App Security) : SaaS 서비스의 클라우드 앱 데이터 보호**

- 3rd party SaaS 서비스도 승인된 앱으로 등록하여 데이터 보호
- 정책 설정을 통해 클라우드 앱 제어
- 클라우드 앱 상시 모니터링 통해 관리자에게 알림/경고 제공
- 앱의 이벤트, 파일 및 사용자 조사를 통해
  - SaaS 앱 전반에 걸친 모든 정책 위반,
  - 위협 감지 및 이상 징후 조사

3. Microsoft 365 제로 트러스트

3. Microsoft Zero-Trust

Zero-Trust 위한 세가지 원칙

Verify explicitly

Use least privilege access

Assume breach

3. Microsoft Zero-Trust

3. Microsoft Zero-Trust

Conditional Access

- **Microsoft Information Protection**
- **Data Loss Prevention**

Classification, Protection, Policy enforcement

- **Azure AD Defender for identity**

Protection, Monitoring and trust insight

- **Cloud App Security (CAS)**

- **Just-in-Time Access**
- **Just Enough-Administration**

- **Intune Defender for Endpoint**

Manage and protect devices

- **Azure Security Center**

Monitor, Report

Don't Trust devices on network
Protect by segmentation and always verify

3. Microsoft Zero-Trust

Connect all your users and apps (Single Sign-On)
Verify identities with Multi-Factor Authentication (MFA)

Identities

3. Microsoft Zero-Trust

- 장치 상태 및 규정 준수에 대한 가시성

Devices

장치(Device) 정보 감지
Malicious Apps
Device Manipulation
Network Exploits
Data privacy violations
Device Health
Encryption
OS version
Email Profile

3. Microsoft Zero-Trust

- 취약하고 손상된 장치에 액세스 제한

3. Microsoft Zero-Trust

- 취약 앱 검색 및 제어

3. Microsoft Zero-Trust

- 데이터 보호 (데이터 검색 및 보호)

Data

→ 보안 정책 정의
→ 여러 위치에서 문서, 이메일 자동 검사

3. Microsoft Zero-Trust

- 데이터 및 파일에 포괄적인 보호
- 데이터 유형, 위치, 민감도에 따라 엄격한 파일 보호

3. Microsoft Zero-Trust

- 제로 트러스트 전략으로 조직 보안

Visibility | Analytics | Automation

3. Microsoft Zero-Trust

- **Microsoft 365 Intelligent Security**

Identity and access management	Threat protection	Information protection	Cloud Security
Azure AD Premium • Azure AD Identity Governance	**Microsoft365 Defender** • Microsoft Defender for Identity • Microsoft Cloud App Security	**Microsoft Information Protection** • Unified Labeling • Microsoft Data Loss Protection	Microsoft Cloud App Security
Microsoft Endpoint Manager		Insider Risk Management	
		Communication Compliance	
		Microsoft Cloud App Security	

Thank you