Security – Azure Synapse Service

에샨트 가르그

데이터 엔지니어, 아키텍트, Advisor
eshant.garg@gmail.com

Azure Synapse Analytics

소개

출처: Microsoft

고급 데이터 보안

취약성 평가	• 잠재적인 데이터베이스 취약성을 발견, 추적 및 수정합니다.
데이터 검색 & 분류	• 모니터링 및 경고를 위해 민감한 데이터를 식별하고 레이블을 지정합니다.
지능형 위협 보호	• SQL Server 로그를 분석하여 비정상적인 동작 및 잠재적으로 유해한 시도를 감지합니다.

감사

• 데이터베이스 이벤트를 추적하고 기록합니다.

감사 로그로 이동하기

• 감사를 통해 데이터베이스 활동을 모니터링, 분석 및 조사하여 잠재적인 위협 또는 의심되는 남용 및 보안 위반을 식별할 수 있습니다.

네트워크 보안

- 방화벽 규칙은 IP 주소를 허용하거나 차단합니다.
- 포트 1433 사용
- 서버 방화벽 규칙만 해당
- 기본적으로 암호화된 연결

투명한 데이터 암호화

- 기본적으로 이동 중인 데이터는 항상 암호화됩니다 TLS(전송 계층 보안) 사용
- 미사용 데이터를 암호화하고 복호화합니다.
- AES-256 암호화 알고리즘 사용
- 암호화 키는 Azure Key Vault에 저장됩니다.

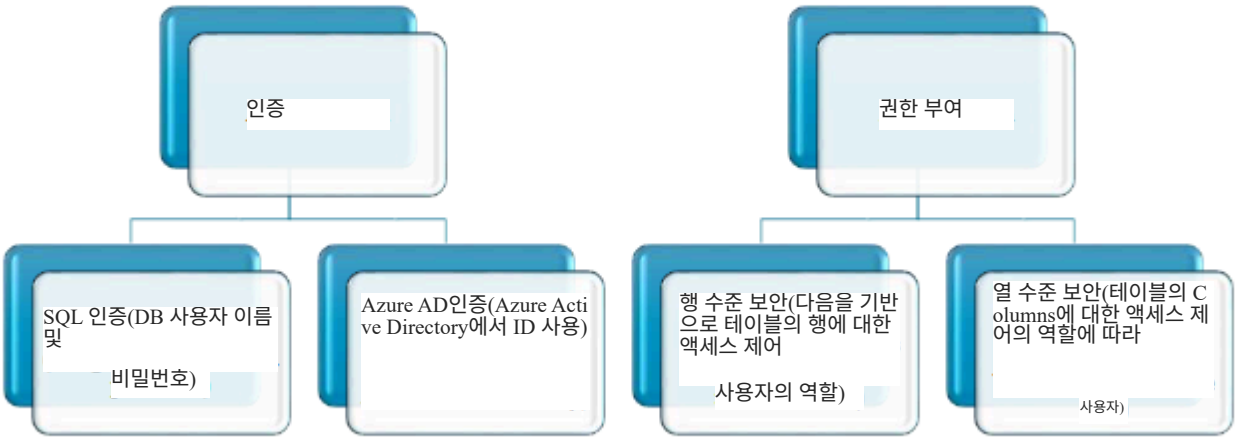
다이나믹 데이터 마스킹(DDM)

- 마스킹을 통해 민감한 데이터에 대한 노출 제한
  - Full – 전체 열이 마스킹됩니다.
  - Partial – 열 데이터의 시작 및/또는 끝 문자를 표시합니다.
    나머지는 사용자 지정 문자열로 마스킹합니다.
  - 이메일 – 열 데이터의 첫 번째 문자를 표시하고 나머지는 마스킹합니다.
    xxx@xxxx.com 와 함께
  - Random – 전체 열이 임의의 값으로 바뀝니다.

- 마스킹된 데이터를 쿼리에 표시
  - 데이터베이스의 데이터가 변경되지 않습니다.

- 데이터베이스 수준 적용
  - 응용 프로그램 수준에 영향을 미치지 않습니다.

접근 관리



행 수준 보안 – 사용 사례

- 병원에서는 간호사가 자신의 데이터를 볼 수 있습니다.
  환자 전용
- 은행은 역할별로 재무 데이터를 제한합니다.
- 다중 테넌트 응용 프로그램은 단일 테이블의 각 테넌트에 대해 논리적 분리를 적용합니다.

열 수준 보안 – 사용 사례

- 금융 회사는 계정 관리자 만 허용합니다.
  고객 SSN(사회 보장 번호), 전화 및 기타 PII에 액세스할 수 있습니다.
- 의료 서비스 제공자는 의사와 의사만 허용합니다.
  간호사가 민감한 의료 기록에 접근할 수 있어야 합니다.

요약

출처: Microsoft