Special Report

제로트러스트 보안전략 : 데이터 (Data)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

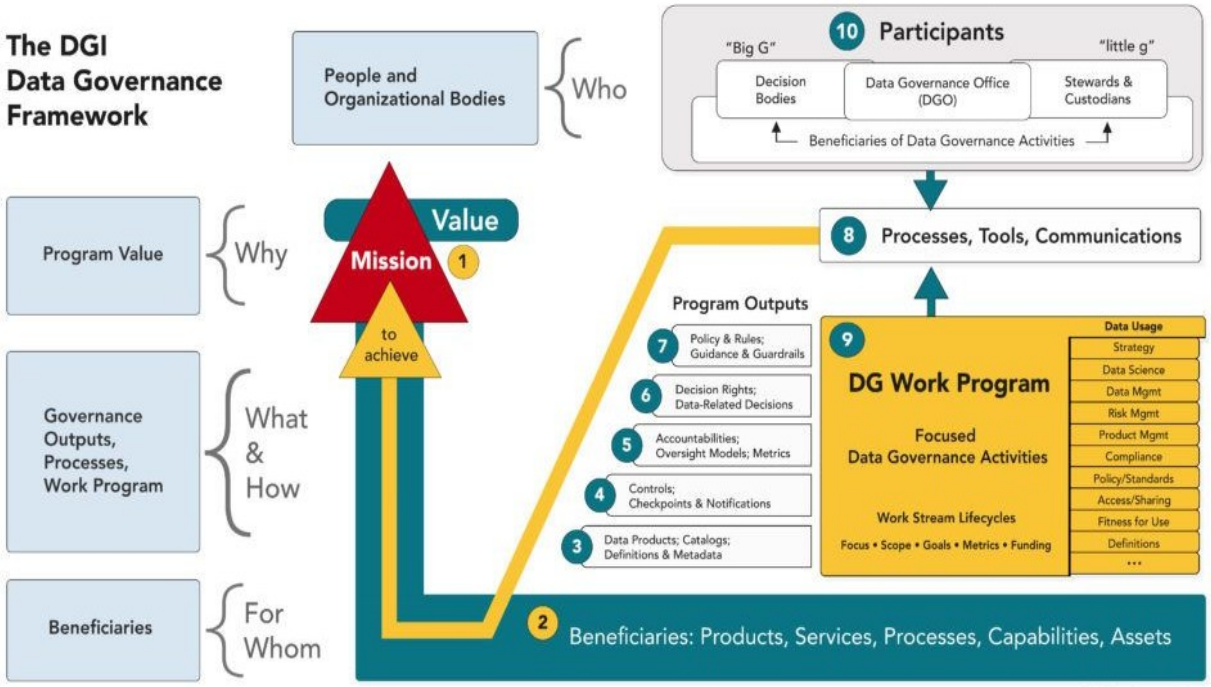
■ 데이터 (Data) 필러 개요

제로트러스트 아키텍처에서 데이터 필러는 온프레미스 서버, 클라우드 스토리지, 사용자 PC 등 모든 환경에 존재하는 각 조직의 핵심 리소스를 보호하는 역할을 한다. 데이터는 일반적인 정형 데이터부터 반정형, 비정형 데이터까지 형태가 매우 다양하다. 제로트러스트의 모든 필러(식별자, 네트워크 등)는 궁극적으로 이 데이터(조직의 리소스)를 보호하기 위한 통제 수단이라고 볼 수 있다.

제로트러스트 아키텍처 구현에 대한 접근 방식은 크게 두 가지 방향으로 논의되어 왔다. 첫 번째는 접근의 출발지가 되는 사용자(식별자)를 먼저 검증하고 단계적으로 보안을 적용해 나가는 방식이다. 두 번째는 최종 목적지에 해당하는 리소스(데이터) 자체를 먼저 식별하고 그 주위에 보안을 겹겹이 쌓아 올리는 방법이다. 현재까지 구현된 대부분의 사례는 기술적 상황을 고려하여 첫 번째 방식을 채택했다. 하지만, 근본적으로는 리소스, 즉 데이터 자체를 완벽히 식별하고 이를 기반으로 보안을 구축하는 두 번째 방식에 대한 연구와 기술 개발을 통해 적용되어야 한다.

과거에는 모든 데이터를 식별하고 분류하여 관리하는 것이 현실적으로 불가능하다는 의견이 지배적이었다. 그러나 최근 클라우드 서비스가 제공하는 다양한 데이터 식별 기능과 DSPM(데이터 보안 형상 관리) 같은 전문 시스템의 등장이 패러다임을 바꾸고 있다. 특히 AI 를 활용한 데이터 자동 식별 및 분류 기술이 실질적으로 적용되면서, 데이터 중심의 제로트러스트 구현이 현실화되고 있다.

이러한 기술들을 효과적으로 적용하기 위해서는 무엇보다 '데이터 거버넌스(Data Governance)' 수립이 가장 중요하다. 데이터 거버넌스는 데이터 표준 및 정책에 따라 데이터의 가용성, 유용성, 무결성, 보안을 관리하는 전사적 프로세스이다. 과거에는 IT 부서가 방화벽 뒤에서 데이터를 관리했지만, 빅데이터 시대가 열리고 데이터의 원천이 외부로 확장되면서, '전사적으로 동일한 기준에 의한 데이터 관리'의 필요성이 대두되었다. 이로 인해 기준정보 관리체계가 도입되고, 데이터 관리의 주체가 IT 부서에서 현업 부서로 확장되는 등 데이터 거버넌스는 점차 진화하고 있다.



출처 : DGI, "Data Governance Framework"

그림 1. The DGI Data Governance Framework

데이터 거버넌스의 중요성은 산업별 특성에 따라 다르게 나타난다. 예를 들어, 제조업에서는 기업 제품의 설계도가 가장 중요한 데이터가 되며, 금융 기업의 경우 고객의 개인정보나 디지털 자산 자체가 가장 중요한 데이터로 꼽힌다. 데이터 거버넌스는 바로 이러한 산업별 특성에 따라 데이터를 식별하고 분류하며, 보호의 우선순위를 정하는 기준이 된다. 최근 국내외 대기업들도 이러한 데이터 거버넌스 체계를 수립하기 위해 다양한 형태의 컨설팅과 자체적인 노력을 기울이고 있다.

국내 공공 부문에서는 최근 발표된 '국가망 보안체계 가이드라인'을 통해 기존의 망분리 체계에서 벗어나, 데이터를 C(기밀)/S(민감)/O(공개) 등급으로 분류하고 이에 맞춰 보안 체계를 차등 적용하는 데이터 중심 보안으로의 전환을 모색하고 있다. 민간 기업에서는 아직까지 데이터를 개인정보 포함 여부 정도로만 구분하여 관리하는 경우가 많지만, 이 역시 데이터 거버넌스의 중요한 시작점이라고 할 수 있다.

출처 : 국가사이버안보센터, "국가 망 보안체계 보안 가이드라인 1.0"

그림 2. 국가 업무정보 C/S/O 분류 기준

위와 같이 데이터에 대한 관리는 제로트러스트 환경에서 조직의 보안 체계를 수립하는 데 매우 중요하다. 단순히 기술을 도입하는 것을 넘어, 조직의 가장 핵심적인 자산인 데이터 자체를 이해하고 보호의 우선순위를 정하는 것이 모든 보안 활동의 출발점이 되어야 하기 때문이다.

이처럼 데이터 거버넌스는 제로트러스트 환경에서 데이터를 관리하는 가장 중요한 방향성을 제시한다. 명확한 데이터 거버넌스가 확립될 때, 비로소 조직은 데이터 관리를 위한 최신 기술을 활용하여 다양한 환경에 산재된 데이터를 효과적으로 식별하고 보호하며 관리할 수 있는 기반을 마련하게 된다. 아직까지 데이터에 대한 식별과 관리 자체가 많은 어려움을 수반하지만, 기술이 발전하고 최근 AI 가 실제 보안 영역에 적극적으로 활용되면서 데이터 중심의 제로트러스트 구현은 점차 현실화되고 있다.

■ 데이터 (Data) 필러의 주요 요소

데이터 필러는 제로트러스트 아키텍처에서 조직의 가장 핵심적인 자산인 '데이터' 자체를 보호하는 데 중점을 둔다. 하지만 데이터는 제로트러스트의 모든 필러 중 관리하기 가장 힘든 영역으로 볼 수 있다. 다양한 환경에 산재되어 있는 정형 및 비정형 데이터는 확장자부터 구성 형태까지 다양하고, 각기 특성에 맞는 관리 기술이 적용되는 등 복잡성이 존재하기 때문이다.

특히 제로트러스트 환경에서는 데이터가 저장된 '위치'(네트워크 경계)가 아닌, 데이터 자체의 '중요도'와 '민감도'를 기반으로 접근을 통제해야 한다. 데이터 인벤토리 관리 및 분류, 데이터 거버넌스, 접근 제어, 암호화, 데이터 손실 방지(DLP) 등 데이터 필러 기준의 여러 관리적·기술적 요소들이 상호 유기적으로 결합되어야만, 조직의 핵심 자산을 유출 위협으로부터 안전하게 보호할 수 있다. 이에 앞서 제로트러스트 기반의 데이터를 관리할 수 있는 주요 요소들에 대한 기준을 세우고 정의하는 것은 매우 중요하다.

아래는 데이터 필러의 주요 요소들과, 이를 구현하기 위한 구체적인 관리·기술 방안을 제로트러스트 성숙도 관점에서 정리한 내용이다.

1. 데이터 인벤토리

제로트러스트 환경에서 데이터 인벤토리 관리는 조직이 보호해야 할 최우선 리소스인 데이터를 식별하고 분류하는 가장 기본적인 출발점이다. 제로트러스트의 경계는 모호하다. 데이터 인벤토리 관리 범위는 온프레미스, 클라우드 및 사용자 접속 환경을 포함해야 한다. 구조화된 데이터와 비구조화된 데이터 또한 대상이다. 이 관리 체계는 초기 단계의 수동 식별 및 엑셀 기반 목록 관리에서, 점차 내부 저장소의 데이터를 일부 자동 식별하는 단계를 거친다. 최종적으로는 관리자 개입 없이 데이터의 라이프사이클을 완전 자동화하여 관리하는 수준으로 발전해야 한다.

인벤토리 구축과 병행되어야 하는 것은 데이터 소유자 관리이다. 이는 단순히 파일 작성자를 소유자로 지정하는 초기 단계를 넘어, 데이터를 중앙에서 관리하고 정책에 따라 소유자를 자동으로 매핑해야 한다. 나아가 소유자의 이상 행위까지 모니터링하여 신뢰도 데이터로 활용하는 단계로 고도화된다. 또한, 보호 우선순위를 정하기 위한 데이터 중요도 관리가 필수적이다. 수동으로 '상/중/하' 등급을 부여하는 방식에서, 개인정보 포함 여부나 수량 등 상세 지표를 산출식에 따라 주기적으로 계산하는 단계를 거쳐, 데이터나 내규 변경 시 중요도를 자동으로 재 산출하는 최적화 단계로 나아가야 한다.

데이터 인벤토리 관리를 위해서는 식별된 모든 데이터가 데이터 라벨링 및 태깅을 통해 보안 정책이 적용될 수 있는 상태가 되어야 한다. 관리자가 수동으로 라벨을 매핑하는 초기 단계를 넘어야 한다. 이후 구조화된 데이터를 중심으로 일부 프로세스를 자동화하고, 최종적으로는 데이터 생성 시점부터 전체 라이프 사이클 동안 관리되는 완전 자동화 체계를 갖춰야 한다.

2. 데이터 권한 관리

제로트러스트 환경에서 데이터 권한 관리는 '최소 권한 원칙'을 데이터에 직접 적용하는 핵심적인 통제 활동이다. 이는 먼저 데이터 공유 정책 관리에서 시작된다. 초기에는 별도 정책 없이 시스템 자체의 공유 기능을 활용하여 지정된 사용자에게만 공유하는 수준에 머무렀다. 그러나, 성숙한 제로트러스트 환경에서는 서비스에 꼭 필요한 공유만을 허용하는 '화이트리스트' 방식을 지향한다. 이를 위해서는 결재 시스템에서 관리자의 최종 확인이 완료된 건에 한해서만 공유를 자동 적용 및 해제하며, 나아가 머신러닝을 기반으로 공유 데이터에 접근하는 사용자의 행위를 지속 학습하여 공유 정책 자체를 동적으로 조정하는 단계로 발전해야 한다.

동시에 데이터 관리의 누락을 방지하기 위해 생성 시점부터 권한을 부여하는 데이터 권한 분류 체계가 필수적이다. 관리자가 주요 데이터만 수동으로 등록하는 단계를 넘어, 정형 데이터가 생성되면 최초 생성자에게 관리자 권한을 부여하고 신청/승인 프로세스를 통해 권한을 관리하는 체계를 갖추어야 한다. 궁극적으로는 정형 데이터뿐만 아니라 비정형 데이터까지 모두 포함하여 생성자에게 권한을 부여해야 한다. 또한, 사용자의 신뢰도 판단 데이터를 연동하여 신뢰도가 하락하면 부여된 권한을 자동으로 회수하는 고도화된 관리 체계가 필요하다.

특히 민감 정보가 집약된 데이터베이스의 SQL 질의어 권한 관리는 중요한 관리 요소이다. 단순히 DB 자체 기능으로 DDL, DML 등의 권한을 개별 부여하는 방식이, DB 권한 관리 시스템을 도입해 사용자별로 권한을 할당하는 단계로 진화해야 한다. 더 나아가, 사전 정책에 따라 DB 의 중요도 수준별로 최소한의 권한을 자동으로 매핑하고 예외 처리를 통해 관리해야 한다. 최종적으로는 머신러닝이 부여된 SQL 권한의 사용 행태를 지속적으로 학습하여 이를 신뢰도 데이터로써 활용하는 수준으로 발전해야 한다.

이러한 모든 권한은 영구적으로 부여되는 것이 아니라 상시 검증되고 갱신되어야 한다. 체계적인 권한 설정 및 회수 프로세스는 동반되어야 한다. 퇴직이나 인사이동 같은 신상정보 변경 시 관리자가 수동으로 권한을 확인하고 변경하는 단계를 지나, 시스템이 변경을 인지하여 기존 권한을 우선 회수하고 사용자가 신청 시스템을 통한 결재로 신규 권한을 적용 받는 프로세스가 필요하다. 더 나아가, 변경된 인사 정보에 따라 새로운 직무의 권한이 자동 매핑되어 적용되야 한다. 궁극적으로는 머신러닝이 데이터 권한 사용 패턴을 지속 학습하여 이 데이터를 기반으로 권한의 설정 및 회수까지 자동화하는 지능형 체계를 갖추어야 한다.

3. 데이터 접근 제어

제로트러스트 환경에서 데이터 접근 제어는 식별되고 분류된 데이터에 대해 '누가, 어떻게' 접근할 수 있는지를 정책에 따라 실시간으로 통제하는 핵심 실행 단계이다. 데이터 접근 관리는 보호 대상 데이터가 존재하는 개별 시스템별로 관리자가 접근 권한을 수동으로 설정하는 방식에서, 중앙화된 시스템을 통해 데이터에 접근할 대상자를 관리자가 등록하여 관리하는 방식으로 발전해야 한다. 모든 데이터에 대해 사전에 접근 정책을 설정하고 접근 대상자가 등록되면 정책에 따라 자동으로 권한이 관리되어야 하는 단계는 그 다음이다. 궁극적으로는 데이터에 접근하는 사용자의 신뢰도 판단 데이터를 기반으로 접근 정책을 상시 검증하고 확인하여 접근 권한을 동적으로 자동 관리하는 수준까지 고도화돼야 한다.

이러한 모든 접근 시도는 사후 보안 관리와 실시간 탐지를 위해 투명한 데이터 접근 이력 관리를 통해 기록되어야 한다. 초기에는 관리자가 개별 시스템의 로그를 수동으로 확인하는 수준에 그치지만, 점차 통합 로그 관리 시스템(SIEM)을 통해 이력 로그를 수집하고 검색하는 체계를 갖추어야 한다. 여기서 더 나아간다면 제로트러스트 관점으로 보호 대상 데이터에 대한 접근 이력을 모니터링해야 한다. 특이사항이 발생하면 담당자에게 알람을 전송하고, 최적화된 환경에서는 이 모든 접근 이력 정보를 통합적으로 수집, 관리하여 이를 사용자 신뢰도 판단 데이터로 생성한다. 해당 정보를 IAM, ICAM 등과 연동해 보안 정책에 반영하는 방향으로 고도화할 수 있다.

데이터 접근은 정해진 경로로만 이루어져야 하므로 데이터 우회 접속 차단 체계 또한 마련되어야 한다. 이는 단순히 DB 자체 기능으로 IP 나 포트를 제어하는 단계를 넘어야 한다. 시스템(서버) 대상으로 PAM, 마이크로세그멘테이션 시스템 등을 도입하여 우회 접속 시도를 로깅하고 관리하며, 이 로그를 통합 로그 및 모니터링 시스템으로 전송하여 위협 분석을 수행해야 한다. 최종적으로는 이 분석 내역을 신뢰도 판단 데이터로 생성하여, 사용자의 신뢰도가 하락하면 접근을 차단하는 등 동적 정책에 활용하는 수준으로 고도화할 수 있다.

4. 데이터 암호화

제로트러스트 환경에서 데이터 암호화는 정보 유출이 발생하더라도 데이터를 보호할 수 있는 핵심적인 방어 체계로, 저장 중인 데이터와 전송 중인 데이터 모두를 대상으로 한다. 초기에는 조직 내 민감한 데이터(개인정보, 기밀문서 등)에 한해 암호화를 적용하는 방식이었다. 이후, 데이터의 종류와 무관하게 생성 시점부터 암호화하여 관리하고, 나아가 조직 전체에서 보유하고 있는 모든 암호화 데이터를 통합 관리하는 체계로 발전했다.

이러한 암호화 체계의 핵심은 암호키 관리에 있다. 암호키를 수동으로 관리하는 방식에서 벗어나, 전사적 보안 정책을 수립하고 개별 암호화키 관리 시스템(KMS) 등을 통해 접근 정책을 제어하는 단계를 거쳐야 한다. 이중화되고 분리된 통합 암호화키 관리 시스템을 통해 접근 시 다중 인증(MFA) 및 지속적인 인증이 이루어져야 하는 것이다. 궁극적으로는 사용자의 신뢰도 데이터를 기반으로 데이터 소유자별 암호화 키를 발급하는 수준까지 고도화되어야 한다.

암호화된 데이터는 안전한 데이터 복호화 정책을 통해 사용되어야 한다. 필요시 중요 데이터를 수동으로 복호화하여 사용하는 방식이 아니라, 암복호화 시스템로 승인된 데이터에 대해서만 정책 기반으로 복호화가 이루어져야 한다. 또한, 복호화 시 다중 인증을 요구하거나 이상 행위가 탐지될 경우 추가 인증을 포함해야 하며, 사용자 상태 변경이나 비정상적인 복호화 시도 같은 신뢰도 판단 데이터를 기반으로 복호화 강도를 차등 적용하는 동적 정책으로 발전해야 한다.

데이터 활용 시 정보 유출을 사전에 방지하기 위해 데이터 마스킹도 병행되어야 한다. 민감 데이터를 수동으로 선별해 마스킹 처리하는 방식에서 벗어나야 한다. 시스템을 통해 데이터 조회 시에만 원본 데이터를 마스킹 처리하거나 출력 시 민감 데이터 영역을 자동 구분하여 처리하는 체계로 전환해야 한다. 최종적으로는 머신러닝과 인공지능(AI)를 활용해 전사적인 민감 데이터를 식별하고 자동 마스킹 처리 후 출력하는 방식으로 구현되어야 한다.

5. 데이터 카탈로그 위험평가

데이터 인벤토리를 통해 자산을 식별하고 권한 및 암호화 체계를 갖추었다면, 이 데이터 자산을 위협으로 보호하기 위한 실질적인 위험 평가와 통제 전략이 필요하다. '데이터 카탈로그 위험평가'는 식별된 데이터(카탈로그)를 대상으로 유출, 유실, 오용 등 발생 가능한 위험 시나리오를 정의하고, 이에 대응하는 보호 통제 수단을 마련하는 활동을 의미한다. 이는 구조화된 정형 데이터의 유출 방지, 문서나 파일 등 비정형 데이터의 유출 방지, 그리고 데이터 유실 방지를 위한 백업 및 복구 체계 수립을 모두 포괄한다.

정형 데이터 유출 방지는 관리자가 개별 시스템에서 접근 권한을 수동으로 관리하는 방식에서, 일부 중요 데이터를 암호화하고 반출 시 승인 프로세스를 도입하는 단계를 거쳐야 한다. 나아가 전체 정형 데이터를 암호화하고 민감도에 따라 등급을 구분해야 한다. 상위 등급 데이터는 접근부터 반출까지 추가 인증 및 승인을 통해 관리하고, 하위 등급은 반출 시에만 승인하도록 차등 관리해야 한다. 최종적으로는 접근하는 사용자의 신뢰도 데이터를 기반으로 데이터에 대한 모든 권한을 실시간으로 자동 변경 및 회수하는 수준으로 발전해야 한다.

비정형 데이터 유출 방지 역시 정해진 프로세스에 따라 관리자가 수동으로 확인하는 방식에서 벗어나, 반출 신청 시 파일을 업로드하여 승인자가 직접 확인하는 체계를 갖추어야 한다. 더 나아가 해시값(Hash)으로 파일 위변조를 확인하고 네트워크상에서 파일 업로드를 원천 차단해야 한다. 또한, 반출 관련 로그를 수집하고 정해진 규칙에 따라 분석하여 이상 행위 탐지 시 관리자가 소명을 요청하거나 권한을 회수해야 한다. 궁극적으로는 중앙 보관 장소에서 비정형 데이터 관리 필수, 그리고 사용자의 신뢰도 데이터를 기반으로 접근 및 변경 권한을 재인증하거나 회수하고, 원본 반출 대신 링크를 통한 임시 접속 권한을 부여하는 방식 등으로 고도화되어야 한다.

데이터 유출 방지뿐만 아니라 유실 방지를 위한 데이터 백업도 중요하다. 관리자가 시스템별로 데이터를 수동 백업하는 방식은 지양한다. 중요 데이터로 분류된 항목을 백업 시스템을 통해 관리하고, 나아가 설정 정보, OS, DB 등 시스템별로 데이터를 분류하여 중앙에서 관리하고, 별도의 소산 백업센터에 보관해야 한다. 최종적으로는 조직 내 모든 데이터를 분류하여 백업하고, 다중 소산 백업센터 및 DR(재해 복구) 구성을 통해 완벽한 복구 체계를 갖추어야 한다.

6. 데이터 모니터링 및 분석

제로트러스트 환경에서 데이터 모니터링 및 분석은 생성, 변경, 삭제 등 데이터의 전체 라이프 사이클에 걸쳐 발생하는 모든 활동을 추적하고 분석하여 보안 태세를 강화하는 핵심적인 활동이다. 데이터 모니터링은 개별 시스템 로그에서 필요시 데이터 흐름을 확인하는 단계를 넘어, 파일 전송 시스템이나 네트워크 패킷 수집 시스템을 통해 데이터 흐름을 저장하고 확인할 수 있어야 한다. 궁극적으로는 조직 내 전체 데이터의 흐름을 실시간으로 모니터링하고, 사전에 정의된 정책에 따라 이상 발생 시 자동으로 알람을 발생하는 체계로 발전해야 한다.

사후 추적보다 선제적 조치가 중요하므로, 이상 징후 모니터링 체계 또한 반드시 필요하다. 개별 시스템 로그를 수동으로 확인하는 방식에서 사전 정의된 정책에 따라 시스템이 이상 징후를 모니터링하고 알람을 보내는 방식으로 발전해야 한다. 최종적으로는 머신러닝과 AI 기반의 데이터 로그를 분석하여 이상 행위 확인 시 해당 데이터에 대한 접근 차단 등 자동화된 조치를 수행하는 수준으로 고도화되어야 한다.

이러한 모든 모니터링 활동은 실시간으로 가시성을 확보해야 의미가 있다. 각 시스템 로그를 추출하여 수동으로 현황 자료를 작성하는 방식은 안된다. 개별 서비스의 중앙 관리 시스템을 통해 데이터별 가시성을 확보하고, 나아가 전체 데이터 흐름을 수집하는 중앙 관리 시스템에서 이기종 시스템 간의 상관관계를 분석하여 종합적인 가시성을 확보하는 방향으로 나아가야 한다. 이렇게 확보된 가시성은 효과적인 데이터 분석을 발휘할 수 있는 기반이 된다. 필요시 저장된 데이터를 검색하고 분석하는 단계를 넘어, 사전 정의된 정책에 따라 모니터링된 내용을 이벤트화하여 분석해야 한다. 궁극적으로는 사용자 영역에서 평소와 다른 유형의 활동이 모니터링되면 이를 자동으로 이벤트화하여 심층 분석하는 지능형 분석 체계를 갖추어야 한다.

7. 데이터 관리 및 프로세스

제로트러스트 환경에서 데이터 관리 정책은 모든 데이터 보호 활동의 근간이 되는 최상위 거버넌스 체계이다. 이는 단순히 관리 정책이 없는 상태에서 데이터의 생성/삭제 정책만을 수립하는 단계를 넘어, 생성, 삭제뿐만 아니라 '변경'까지 포함하는 관리 정책을 수립해야 한다. 나아가 조직의 내규와 법규를 기초로 데이터의 형태, 규모, 전송, 저장 등 데이터 전반에 대한 포괄적인 관리 정책을 수립하고 관리하는 방향으로 고도화되어야 한다. 이러한 데이터 거버넌스는 데이터의 품질, 보안, 가용성에 중점을 두고, 데이터 수집, 소유권, 저장, 처리 및 사용에 대한 정책, 표준, 절차를 정의하고 구현함으로써 데이터의 무결성과 보안을 보장한다.

명확한 데이터 거버넌스 프레임워크는 조직의 핵심 데이터 자산을 관리하기 위한 구조와 프로세스를 정의한다. 여기에는 전사적 전략을 감독하는 거버넌스 위원회(운영 위원회), 특정 데이터 도메인의 품질과 정확성을 책임지는 데이터 소유자(Data Owner), 그리고 데이터의 일상적인 관리를 담당하는 데이터 관리자(Data Steward) 등 명확한 역할과 책임(R&R) 정의가 포함되어야 한다. 제로트러스트 환경에서 이러한 역할 정의는 데이터 접근 권한을 부여하고(RBAC/ABAC), 규정 준수를 감사하며, 데이터 품질을 유지하는 모든 자동화 프로세스의 기반이 된다.

이렇게 수립된 정책은 프로세스 자동화를 통해 실질적으로 구현되어야 관리 누락을 방지할 수 있다. 데이터의 생성 및 삭제를 수동으로 관리하는 방식은 지양해야 한다. 데이터의 생성, 저장, 사용, 보관, 삭제에 이르는 전체 데이터 라이프 사이클을 관리하는 워크플로우를 시스템으로 구축해 각 데이터별 관리자가 등록하는 단계로 가야 한다. 최종적으로는 이 워크플로우 시스템이 데이터 거버넌스 도구와 연계해야 하는 것이다. 데이터의 자동 검색 및 분류, 보호 규칙 적용, 메타데이터 관리 등을 수행하며, 개별 데이터 시스템들(DB, 데이터 레이크 등)과 연동되어 데이터의 전체 라이프 사이클이 자동으로 관리되는 체계를 갖추어야 한다.

이처럼, 인벤토리, 암호화, 접근 제어 등은 DSPM, DLP, DRM 과 같은 시스템(솔루션)으로 맵핑될 수 있다. 데이터는 다양한 환경에 산재되어 있어 적용 범위가 조직마다 다르게 정의되거나 기능이 중복될 수 있으므로 명확한 접근이 필요하다. 따라서 조직은 먼저 보호해야 할 데이터의 범위를 식별하고, 위에서 다룬 주요 요소들을 기반으로 일관된 정책과 프로세스를 수립하는 것이 무엇보다 중요하다.

데이터 필러의 고도화는 조직의 전체 데이터의 라이프 사이클(생성, 저장, 활용, 폐기)에 제로트러스트 원칙을 일관되게 적용할 수 있는 관리 체계와 기술적 토대를 마련하여, 각 데이터 단위에서 발생할 수 있는 유출 및 유실 위협을 사전에 방지하고 신속하게 대응할 수 있는 환경을 실현할 수 있다. 또한, 이 필러의 효과적인 구현은 조직 내 가장 민감한 정보가 처리되는 지점을 직접적으로 보호하고, 내·외부의 고도화된 위협으로부터 조직의 핵심 자산을 안전하게 방어하는 데 필수적인 역할을 수행할 수 있다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템은 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 한다. 이를 실현하기 위해 각 시스템 별 상태를 확인하고, 지속적으로 검증하며, 최소 권한 접근을 보장을 수행할 수 있는 시스템이 필수적이다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당한다. 이들 시스템은 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.

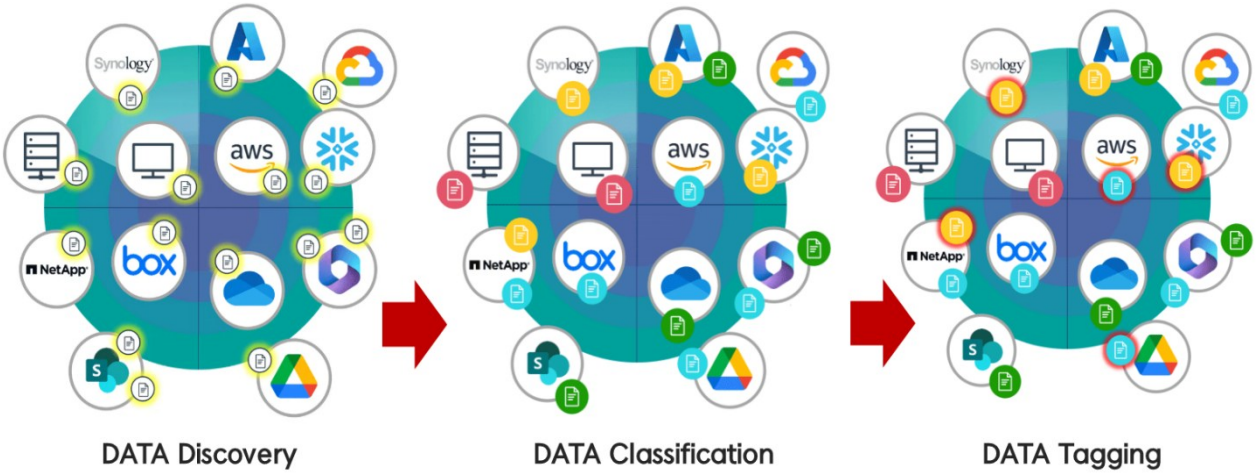
출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 3. 데이터 필러 주요 시스템

1. DSPM (Data Security Posture Management, 데이터 태세 관리)

DSPM 은 조직 내에 존재하는 방대한 데이터 자산을 체계적으로 탐색, 식별, 분류, 태깅하고, 이 정보에 기반하여 실시간 가시성, 위험 평가, 자동화된 정책 집행 및 규제 대응까지 구현하는 데이터 중심의 통합 보안 관리 시스템이다. 기존의 데이터 보안이 단일 시스템이나 파일 단위의 단편적 관리에 머물렀다면 제로트러스트 아키텍처에서 DSPM 은 온프레미스·클라우드·SaaS 등 모든 환경에 걸쳐 민감 데이터의 위치, 상태, 권한, 활용 맥락을 지속적으로 자동 파악하고 관리해야 한다. 이를 통해 DSPM 은 데이터 필러에서 제로트러스트 원칙을 실현하는 핵심 시스템으로 기능할 수 있다.

DSPM 은 크게 아래의 세 가지 핵심 기능을 통해 제로트러스트 원칙을 구현한다.



출처 : Sealpath "Data Security Posture Management and other Data-Centric Security Tools"

그림 4. DSPM 핵심 기능

(1) 데이터 탐색 (Data Discovery)

파일 서버, 클라우드 스토리지, 데이터베이스 등 조직 내 모든 저장소에 분산된 정형 및 비정형 데이터를 자동으로 스캔하여 식별한다. 이는 조직이 인지하지 못했던 'Shadow Data'를 포함한 모든 데이터 자산의 현황을 파악하는 DSPM 의 첫 번째 단계이다.

(2) 데이터 식별 (Data Classification)

탐색된 데이터의 내용을 분석하여 개인정보(PII), 기밀정보, 금융정보 등 조직의 정책 및 컴플라이언스 기준에 따라 민감도와 유형을 자동으로 분류한다. 이 분류 등급(예: 기밀/민감/공개)은 데이터 보호 정책을 차등 적용하는 기준이 된다.

(3) 데이터 태깅 (Data Tagging)

분류된 데이터에 소유자, 보존 기간, 규제 요건, 반출 금지 등 다양한 정책 속성(메타데이터)을 동적으로 부여하는 과정이다. 이 태그 정보는 DLP, DRM, 접근 제어 시스템과 연동되어 보안 정책이 자동으로 집행되도록 하는 실질적인 기반으로 작동한다.

위의 핵심 기능들로 데이터를 관리하고, 데이터에 대한 가시성을 추가로 확보할 수 있다. 데이터는 조직의 환경에 따라 다양한 형태가 있을 수 있고 데이터의 양도 방대할 수 있기 때문에, DSPM 이 효과적으로 동작하기 위해서는 AI 활용이 필수적이다. AI 를 활용하여 자동화된 데이터 탐색, 분류, 태깅 기능이 적용돼야 한다. DSPM 도입 초기에는 오탐과 누락이 많이 발생할 수 있으나, 정책을 고도화하고 AI 기반의 지속적인 학습을 통해서 DSPM 이 발전되면 데이터 생성부터 폐기까지 전 라이프사이클에 대한 자동화를 구현할 수 있다.

출처 : ForcePoint "ForcePoint DSPM 소개자료"

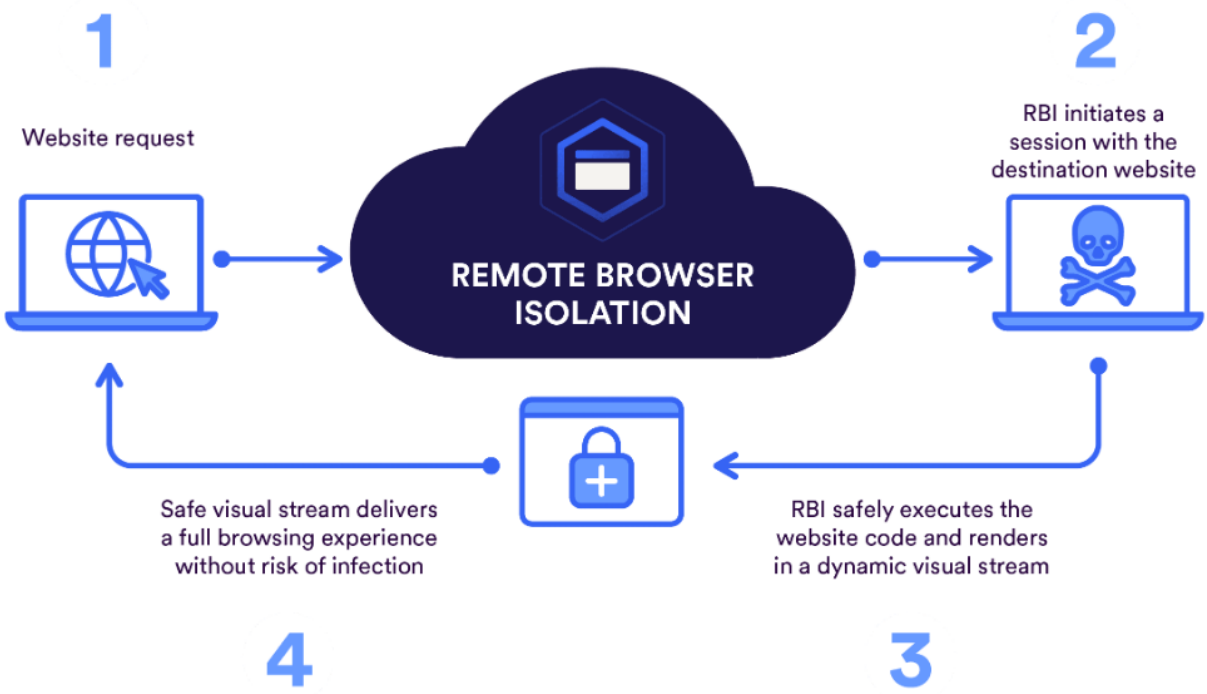
그림 5. AI Mesh For DSPM

DSPM 은 단독으로 동작하지 않으며, DLP 시스템과 연동되어 정책을 시행하고 eDRM, MIP(Microsoft Information Protection) 등 데이터 암호화 시스템들과 연동하여 데이터 라벨 기반으로 동작할 수 있다.

기존의 데이터 보안이 단일 시스템이나 파일 단위의 단편적 관리에 머물렀다. 제로트러스트 아키텍처에서 DSPM 은 온프레미스·클라우드·SaaS 등 모든 환경에 민감 데이터의 위치, 상태, 권한, 활용 맥락을 지속적으로 자동 파악하고 관리할 수 있어야 한다. DSPM 은 데이터 필러에서 제로트러스트 원칙을 실현하는 핵심 시스템으로 역할한다.

2. RBI (Remote Browser Isolation, 원격 브라우저 격리)

RBI 는 웹 브라우저를 통해 발생하는 다양한 보안 위협(악성코드, 피싱, 랜섬웨어 등)에 근본적으로 대응하기 위한 보안 시스템이다. 사용자의 PC 나 네트워크 내에서는 브라우저가 직접 인터넷 자원을 실행하는 대신, 격리된 원격 환경(서버·클라우드)에서 브라우저 세션을 대신 실행하고, 최종 렌더링 화면만 사용자에게 안전하게 전달한다. 이는 위협이 사용자의 엔드포인트나 내부망으로 유입되는 것을 원천적으로 차단한다.



출처 : Skyhigh Security, “Minimize Your Cloud Attack Surface”

그림 6. RBI Operation Method

RBI 는 제로트러스트 아키텍처 확산 및 국내 망분리 환경 변화에 따라, 조직의 브라우저 보안의 핵심 시스템으로 다시 주목받고 있다. 온프레미스와 SaaS 형태로 모두 지원되지만, 온프레미스형은 실제 구현 시 웹 브라우저의 속도 저하나 웹 가용성의 한계가 발생할 수 있어 SaaS 형태로 권장되는 추세이다.

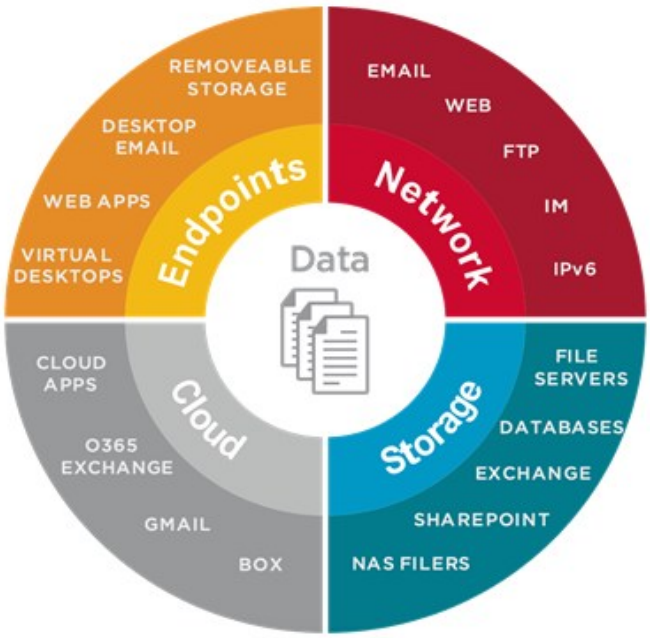
RBI 를 도입하면 일반적으로 기존 브라우저의 직접 사용을 제한하고, 격리된 브라우저를 통해서만 웹 접속이 이루어진다. RBI 는 브라우저 환경에서 발생 가능한 모든 보안 위협에 대한 통합 대응 기능을 제한다.

주요 기능으로는 악성코드, 랜섬웨어, 스크립트 공격의 원천 차단이 있다. 또한 유해 사이트 접속을 제한하고 의심 파일을 자동으로 무해화(CDR)하며, 파일 다운로드/업로드, 확장자, 민감정보 검사 등 데이터 이동에 대한 세부 제어를 수행한다. 또한 클립보드 사용, 복사/붙여넣기, 화면 캡처를 통제하고, ChatGPT 와 같은 생성형 AI 서비스의 사용 및 데이터 입력까지 관리할 수 있다. 이 모든 기능은 사용자별 정책에 따라 적용되며, 모든 행위 로그가 기록되어 가시성을 확보할 수 있다.
이러한 기능으로 RBI 는 제로트러스트 환경에서 브라우저를 통한 모든 웹 접근과 행위를 중앙에서 일관되게 관리하고 자동화해 조직의 브라우저 보안 수준을 강화하는 핵심 시스템으로 동작한다.

3. eDLP (Enterprise Data Loss Prevention, 엔터프라이즈 데이터 유출 방지)

제로트러스트 아키텍처에서 eDLP 는 기존에 엔드포인트 DLP 와 네트워크 DLP 로 구분되어 동작하던 데이터 유출 방지 체계를 통합하여, 단일 정책으로 관리 및 수행하는 발전된 보안 시스템이다.

제로트러스트 환경에서는 모든 데이터 경로를 신뢰하지 않는다. 그러므로, 엔드포인트(로컬 저장소, USB, 클립보드, 프린터)와 네트워크(클라우드 업로드, 이메일 첨부)에서 발생하는 모든 데이터 반출 시도를 실시간으로 탐지하고 정책에 따라 차단, 경고, 암호화 등 대응 조치를 수행한다. 제로트러스트 환경에서 eDLP 의 목적은 데이터의 위치·이동 경로·사용 행위에 따라 실시간으로 유출을 방지하고, DSPM/eDRM 등과 연계된 정책 기반 자동화 통제로 제로트러스트 아키텍처 내 데이터 유출 방지를 실현하는 것이다.



출처 : Symantec "Guide to DLP Security"

그림 7. DLP 주요 기능 및 범위

기존 환경에서 DLP 은 엔드포인트에 에이전트로 설치해 기업 내 데이터가 USB 나 외장하드 등으로 외부 유출되는 것을 방지하거나, 개인정보와 기밀정보 같은 민감정보 관리, 워터마크 등으로 출력물 관리하는 기능을 제공했다. 네트워크 단에서는 이메일이나 메신저 등을 통해 데이터유출을 방지하는 형태로 제공됐다. 제로트러스트 환경에서는 기존 DLP 의 기능을 포함하여 다양한 환경(클라우드, SaaS, 네트워크, 엔드포인트 등)을 통합하여 데이터 유출을 방지하고 데이터 유출 시도가 발생할 시 이러한 내용을 타 시스템과 연동하여 리스크 기반의 통제를 반영할 수 있는 엔터프라이즈 DLP 로 진화하고 있다고 볼 수 있다.

eDLP 의 핵심은 단독으로 동작하는 것이 아니라, 다른 데이터 보안 시스템과의 유기적 연동에 있다. 특히 DSPM 을 통해 사전에 식별되고 '외부반출금지' 또는 'GDPR 적용' 등으로 태깅된 데이터가 엔드포인트나 네트워크 경계를 벗어나려 할 때, eDLP 는 이 태그를 인지하여 정책을 자동으로 집행(조치)한다. 또한 MIP 와 같은 eDRM(엔터프라이즈 디지털 권한 관리) 시스템과 연동해 반출이 허용되더라도 해당 데이터를 자동으로 암호화해야 한다. 그리고 열람, 편집, 전송에 대한 세부 권한을 적용함으로써 데이터의 지속적인 보호를 보장할 수 있다.

4. eDRM (Enterprise Digital Rights Management, 엔터프라이즈 디지털 권한 관리)

eDRM 은 조직 내 민감한 디지털 정보를 보호하기 위한 체계적인 접근 방식이다. 국내에서는 DRM 을 주로 '문서 암호화' 시스템으로 인식하는 경향이 있으나, 이는 콘텐츠 저작권 보호에 중점을 둔 전통적인 DRM 과 구분된다. eDRM 은 기업 환경에 특화되어 있다. 문서, CAD, 소스 코드, 음성 등 기업의 지적 재산(IP), 금융 데이터, 고객 기록 등 광범위한 내부 자산을 보호하는 데 중점을 둔다.

제로트러스트 환경에서 eDRM 의 핵심 기능은 강력한 파일 암호화를 기반으로, 세분화된 사용자 접근 제어(UAC)를 적용하는 것이다. 이는 단순히 파일을 열람하는 것을 넘어, 인쇄 횟수 제한, 보기 만료 기한 설정, 화면 캡처 방지, 그리고 사용자의 ID 나 회사 이름이 포함된 동적 워터마킹 삽입 등을 포함한다. 데이터가 조직 외부로 공유된 이후에도 파일 자체에 적용된 정책을 기반으로 접근을 제어하고, 사용 현황을 추적하며, 필요시 원격에서 접근 권한을 폐기도 가능케 해야 한다.

제로트러스트 아키텍처 측면에서 eDRM 은 다양한 환경에 분산된 데이터 자체를 보호하는 핵심 역할을 수행한다. eDRM 은 단독으로 동작하기보다 DSPM, eDLP 등 다른 데이터 보안 시스템과 유기적으로 연동되어야 한다. 예시로 DSPM 이 데이터를 식별하고 데이터에 태그를 부여하면, eDLP 가 해당 파일의 외부 반출이나 이메일 전송을 감지한다. 그 후, MIP 나 eDRM 이 자동으로 해당 파일에 암호화 및 권한 정책을 적용하여 데이터의 전체 라이프 사이클에 걸쳐 일관된 보안 및 가시성 관리를 실현할 수 있다.

5. DB 암호화 (Database Encryption)

DB 암호화는 제로트러스트 환경 이전부터 데이터베이스에 저장된 민감한 정형 데이터(개인정보, 금융정보, 기밀정보 등)를 보호하기 위해 널리 사용되어 온 핵심적인 보안 기술이다. 데이터베이스 암호화는 기술적 신뢰성 측면에서 데이터를 보호하는 가장 중요하고 근본적인 방법 중 하나다. 데이터 유출 시에도 원본 정보의 기밀성을 유지하는 것을 목표로 한다.

DB 암호화를 구현하는 방식에는 여러 가지가 있다. DBMS 자체에 암복호화 모듈을 설치하는 플러그인(Plug-in) 방식, 애플리케이션 레벨에서 API 를 호출하여 암복호화를 수행하는 API 방식, 애플리케이션과 DBMS 사이에 프록시 서버를 두는 시큐어 프록시(Secure Proxy) 방식, 그리고 운영체제(OS) 커널 수준에서 DB 데이터 파일 자체를 암복호화하는 커널(Kernel) 방식(TDE)이 대표적이다. 각 방식은 성능, 보안성, 관리 편의성 등에서 장단점을 가지므로 조직의 시스템 환경과 비즈니스 요구사항에 맞춰 적절한 방식을 선택해야 한다.

효과적인 DB 암호화 시스템은 단순히 데이터를 암호화하는 것을 넘어 다양한 기능을 제공해야 한다. 테이블 전체, 특정 컬럼, 다양한 데이터 유형에 대한 부분 또는 전체 암호화를 지원하고, 동일한 원본 데이터라도 항상 다른 암호문으로 생성되도록 초기화 벡터(IV) 기능을 지원하여 추측 공격을 방지해야 한다. 또한, DB 사용자, 애플리케이션, IP 주소, 시간 등으로 세분화된 암복호화 접근 제어가 가능해야 하며, 암호화 키는 PKI 기반으로 안전하게 생성, 전송, 관리되어야 한다.

제로트러스트 관점에서 DB 암호화는 단순히 저장된 데이터를 보호하는 것을 넘어, 데이터 접근 제어, PAM 과 연계되어야 한다. 예를 들어, 컬럼 레벨 암호화를 적용하면, 인가된 사용자만 특정 민감 정보 컬럼을 복호화하여 볼 수 있도록 DB 수준에서 접근 제어를 강화할 수 있다. 또한, 암호화로 인한 성능 저하 우려가 있지만, 이는 기술 자체의 문제이기보다는 시스템에 대한 이해 부족이나 잘못된 애플리케이션 설계 때문인 경우가 많아, 전문가의 도움을 받아 보안과 성능의 균형을 맞추는 것이 중요하다. DB 암호화는 제로트러스트 아키텍처 내 다른 보안 시스템(접근 통제, 키 관리 등)과 연계되어 데이터 중심 보안을 구현하는 핵심 요소로 기능할 수 있다.

6. ECM (Enterprise Content Management, 문서 중앙화)

ECM 시스템은 기업 내 모든 문서 콘텐츠를 개인 단말기가 아닌 중앙 서버(혹은 클라우드 스토리지)에 통합 저장하고, 접근, 공유, 보관, 폐기에 이르는 문서의 전체 라이프사이클을 일관된 정책으로 관리하는 것을 말한다. 이로써 조직은 비정형 데이터의 가장 큰 부분을 차지하는 문서 자산을 중앙에서 통합 관리하여 데이터 분산을 방지하고, 보안성과 업무 효율성을 동시에 높일 수 있다.

ECM 의 주요 기능은 모든 문서를 개인 단말기에 저장하지 않고 중앙 서버에 저장하는 것에서 출발한다. 또한, 문서 변경에 대한 상세한 기록을 남겨 변경 이력을 관리하고, 사용자 별 또는 역할 별로 문서 접근 권한을 세밀하게 부여할 수 있다. 보안 기능 측면에서는 내재된 DRM 기능으로 문서 자체를 암호화하거나, DLP 기능과 연동하여 민감 정보 유출을 통제한다. 아울러 백업 및 복구, 랜섬웨어 대응 기능까지 제공하여 문서 자산을 안전하게 보호한다. 동시에 안전한 문서 공유 및 협업 기능을 제공하여 업무 생산성 향상에도 기여한다.

최근 기업 환경에서는 ECM 시스템이 독립적으로 운영되기보다, Microsoft OneDrive 나 Google Drive 와 같은 클라우드 스토리지 서비스와 연동하여 하이브리드 형태로 동작하는 경우가 많다. 또한, 단순히 중앙 서버에만 문서를 저장하는 것을 넘어, 정책에 따라 사용자 PC(로컬 환경)에 저장되는 문서에 대해서도 암호화 및 접근 통제를 적용하여 로컬 환경에서의 데이터 유출 위험까지 관리하는 기능을 제공한다.

제로트러스트 아키텍처 관점에서 ECM 은 단순히 문서를 저장하는 시스템을 넘어, 데이터 중심 보안을 구현하는 핵심 허브로 동작할 수 있다. 문서가 생성될 때 ECM 을 통해 중앙에서 관리되며, DSPM 을 통해 식별된 민감도에 따라 eDRM 정책이 자동으로 적용되고, IAM, ICAM 시스템과 연동하여 사용자의 역할과 신뢰도에 기반해 접근 권한이 매핑된다. 이후 문서의 이동이나 공유 시도는 eDLP 에 의해 통제되며, 모든 활동 기록은 SIEM 으로 전송되어 지속적인 모니터링과 이상 행위 분석에 활용된다. 이처럼 ECM 은 제로트러스트의 다른 보안 시스템들과 유기적으로 연동되어 비정형 데이터의 전체 라이프 사이클에 걸쳐 일관된 보안 정책과 가시성을 제공할 수 있다.

위와 같은 시스템들을 통해 데이터 필러는 제로트러스트 아키텍처에서 조직의 가장 민감한 자산인 데이터 자체를 보호하는 데 중점을 둔다. DSPM 을 중심으로 데이터의 위치와 상태에 대한 가시성을 확보하고, eDLP 와 eDRM 을 통해 데이터의 유출을 방지하고 사용 권한을 지속적으로 통제한다. 또한 DB 암호화와 ECM 시스템을 통해 저장된 정형 및 비정형 데이터를 보호하며, RBI 를 통해 웹 브라우저를 통한 데이터 유출 경로까지 차단하는 심층 방어 체계를 구축할 수 있다.

데이터 필러의 주요 시스템들은 식별자 필러의 IAM/ICAM, 네트워크 필러의 ZTNA, 가시성 영역의 SIEM 등 다른 필러의 핵심 시스템들과 유기적으로 연동된다. 이러한 상호 연동을 통해 온프레미스와 클라우드를 아우르는 복잡한 환경에서도 데이터의 생성부터 활용, 폐기에 이르는 데이터 라이프사이클을 관리할 수 있다. 이를 통해 제로트러스트 원칙인 '지속적인 검증'과 '최소 권한' 원칙을 일관되게 적용하고 강화할 수 있다.

■ 맺음말

제로트러스트 아키텍처에서 데이터 필러는 조직의 가장 핵심적인 자산인 '데이터=리소스' 보호가 최종 목표 지점이라 할 수 있다. 식별자, 기기, 네트워크 등 다른 모든 필러는 궁극적으로 이 데이터를 안전하게 보호하기 위한 통제 수단으로 기능하며, 데이터 필러는 이러한 통제를 데이터의 전체 라이프 사이클에 걸쳐 직접 적용하는 역할을 수행한다. 하지만 다양한 형태와 위치에 산재된 데이터의 복잡성으로, 데이터 필러는 제로트러스트 구현에 있어 가장 어렵고 도전적인 영역으로 남아있다.

이러한 어려움을 극복하기 위한 핵심 열쇠는 바로 '데이터 거버넌스'에 있다. 명확한 데이터 거버넌스 체계를 통해 조직의 데이터를 식별하고 분류하며 보호 우선순위를 정하는 것이 모든 데이터 보안 활동의 출발점이 된다. 이를 기반으로 DSPM 과 같은 시스템을 활용하여 데이터 인벤토리와 가시성을 확보하고, eDLP 와 eDRM 으로 데이터 유출을 방지해 사용 권한을 지속적으로 통제해야 한다. 또한, DB 암호화와 ECM 을 통해 저장된 데이터를 보호하고, RBI 와 같은 기술로 웹을 통한 유출 경로까지 차단하는 등 다층적인 방어 체계를 구축해야 한다.

데이터 필러의 주요 시스템들은 식별자 필러의 IAM/ICAM, 네트워크 필러의 ZTNA, 가시성 영역의 SIEM 등 다른 필러의 핵심 시스템들과 유기적으로 연동될 때 비로소 제로트러스트 원칙을 완벽하게 실현할 수 있다. 이러한 상호 연동을 통해 온프레미스와 클라우드를 아우르는 복잡한 환경에서도 데이터의 생성부터 활용, 폐기에 이르는 전체 데이터 라이프 사이클에 걸쳐 '지속적인 검증'과 '최소 권한' 원칙을 일관되게 적용하고 강화할 수 있다.

결론적으로, 데이터 필러의 성공적인 구현은 단순히 개별 기술을 도입하는 것을 넘어, 데이터 거버넌스를 중심으로 조직 전체의 협업과 프로세스 변화를 요구한다. 비록 구현 과정에 많은 어려움이 따르겠지만, AI 와 같은 최신 기술의 발전과 함께 데이터 중심의 제로트러스트는 점차 현실화되고 있다. 조직은 데이터 필러에 대한 지속적인 투자와 노력을 통해, 끊임없이 변화하는 위협 환경 속에서도 가장 중요한 자산을 안전하게 보호하는 견고한 보안 체계를 완성할 수 있을 것이다.

■ 참고 문헌

[1] KISA, “제로트러스트가이드라인 V2.0”, 2024.12

[2] NIST, “Data Security | NCCoE”

[3] NIST SP 1800-35 Final,“Implementing a Zero Trust Architecture:High-Level Document”, 2025.06

[4] DGI, “Data Governance Institute 2014 Data Governance Framework”, 2014

[5] CISA, “CISA Zero Trust Maturity Model V2”, 2023.11

[6] DoD, “Zero Trust Overlays”, 2024.06

[7] 국가사이버안보센터, “국가 망 보안체계 보안 가이드라인(Draft)”, 2025.01

[8] 국가사이버안보센터, “국가 망 보안체계 보안 가이드라인 1.0”, 2025.09

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] Gartner, “Data Security Posture Management Reviews and Ratings”

[3] CLOUDIAN, “8 Data Security Best Practices You Must Know”

[4] Broadcom, “Symantec Data Loss Prevention Product Brief”

[5] 펜타시큐리티, “Database (DB) Encryption - Everything You Need to Know”