SK 쉴더스

Threat Intelligence Report

EQST INSIGHT

EQST(이큐스트)는 'Experts, Qualified Security Team' 이라는 뜻으로
사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

2025
11

SK 쉴더스

Contents

Headline

생성형 AI 콘텐츠 진위 검증을 위한 워터마크 기술의 현황

혁신사업본부 사이버보안 AI 랩스 김기남 책임

■ 1. 대규모 언어 모델(LLM) 발전과 Vertical AI 의 부상

1.1 LLM 발전 동향

대규모 언어 모델(Large Language Model, LLM)은 방대한 텍스트 데이터를 학습하여 인간의 언어를 이해하고 생성하는 능력을 갖춘 인공지능(AI) 모델이다. LLM 은 트랜스포머(Transformer)라는 혁신적인 신경망 아키텍처를 기반으로 문장의 문맥과 단어 간의 복잡한 관계를 파악한다. 이는 단순 텍스트 생성을 넘어 번역, 요약, 질의응답, 코드 생성 등 다양한 자연어 처리(NLP) 작업을 높은 정확도로 수행하도록 한다.

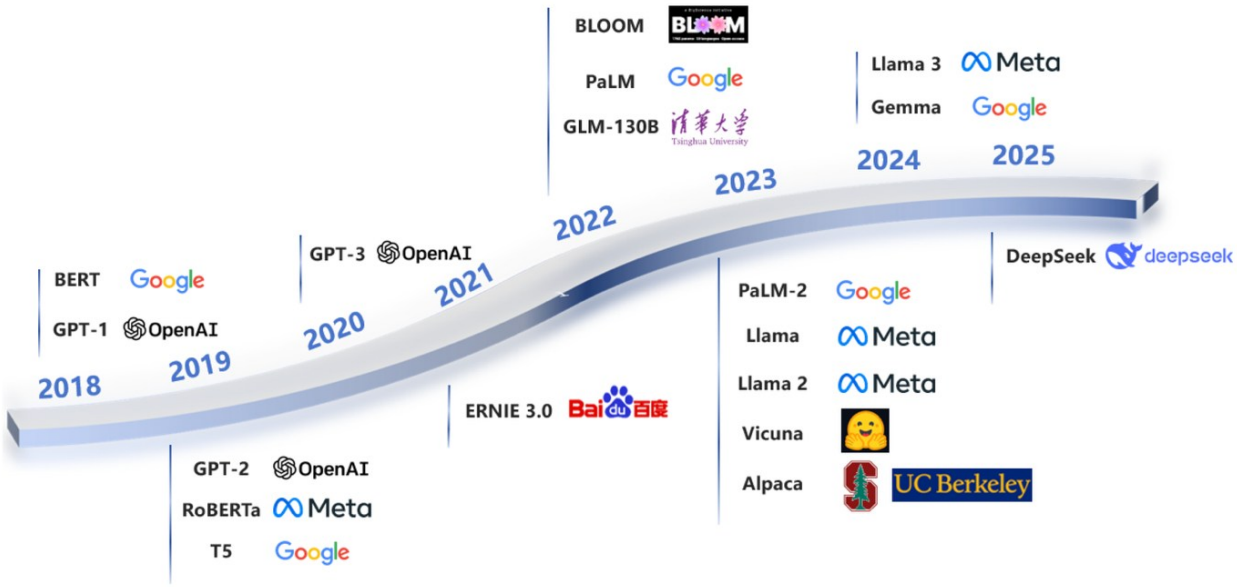


그림 1. 연도별 LLM 주요 모델

지금까지 수많은 LLM 이 개발되었다. 각 LLM 은 '스케일링 법칙(Scaling Law)'에 따라 데이터의 크기가 커질수록 성능이 비약적으로 향상된다는 점이 입증되었다. 이는 초기 LLM 이 모델 크기와 학습 데이터 양을 늘리는 '규모의 경쟁'에 집중했던 이유가 결과로 이어졌다.

지금까지 수많은 LLM 이 개발되었다. 초기에는 주로 모델 파라미터 수와 학습 데이터 규모를 확장하는데 초점을 두었다. 이는 모델의 규모와 학습 데이터 양이 커질수록 성능이 비약적으로 향상된다는 '스케일링 법칙(Scaling Law)'에 근거한 것으로, 이러한 방향성은 오랫동안 LLM 발전의 핵심 기조로 자리해왔다.

그러나 최근에는 단순히 크기를 키우는 경쟁을 넘어, 성능과 효율성을 동시에 강화하는 방향으로 빠르게 발전하고 있다. 이러한 변화의 핵심 동향은 모델 아키텍처 혁신, 컨텍스트 윈도우 확장, 그리고 추론 능력 고도화 세 가지로 요약할 수 있다.

- 모델 아키텍처 혁신

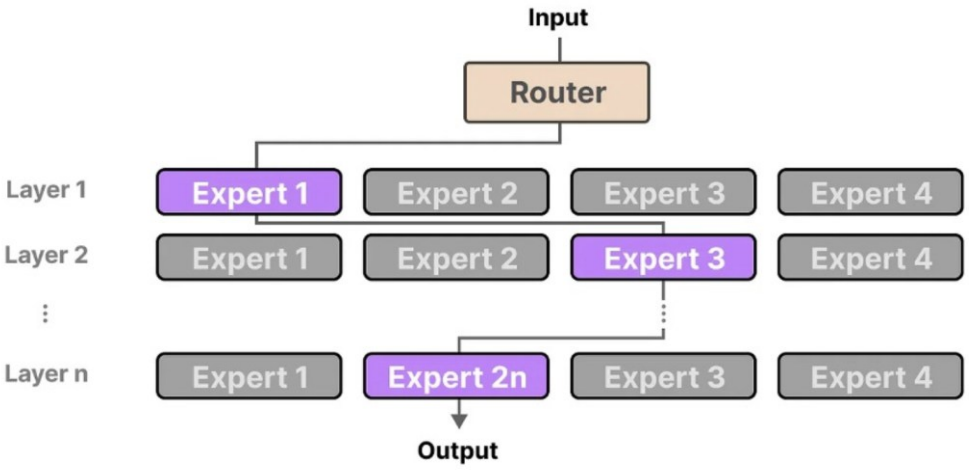


그림 2. 전문가 혼합(Mixture-of-Experts, MoE) 구조

전문가 혼합(Mixture-of-Experts, MoE) 구조는 특정 과업에 최적화된 일부 전문가 네트워크만 선택적으로 활용하여 연산 효율을 극대화한다. 최신 모델들은 MoE 구조를 채택하여, 하나의 대형 모델로 다양한 서비스와 도메인에 효율적으로 대응하고 클라우드 비용과 GPU 자원 소모를 최소화하고 있다.

- 컨텍스트 윈도우 확장

초기 LLM 은 수천 토큰 수준의 텍스트만 처리할 수 있었다. 하지만, 최근 Gemini 1.5 Pro, Llama 4 Scout 등의 모델은 수십만에서 백만 토큰 이상을 한 번에 처리한다. 이를 통해 수천 페이지에 달하는 연구 논문, 기술 문서, 법률 자료 등 방대한 문서를 단번에 분석하고 전체 맥락 속에서 핵심 정보를 정확히 찾아낼 수 있어, 전문가의 지식 활용과 비즈니스 환경의 데이터 처리 효율을 크게 향상시킬 수 있다.

- 추론 능력 고도화

최신 모델은 단계별 사고(Chain-of-Thought, CoT) 기법과 강화학습을 통해 문제 해결 과정을 논리적으로 설명하는 능력을 내재화하고 있다. GPT-4o 나 DeepSeek-R1 과 같은 모델들은 수학, 코딩, 논리 문제에서 높은 정확도를 보이며 결과와 이유를 함께 제시하여 신뢰도를 높였다. 이는 장기적으로 다단계 의사결정이 가능한 자율 AI 에이전트로의 발전 가능성을 시사한다.

1.2 LLM 의 한계와 Vertical AI 의 발전

LLM 의 급격하게 발전했음에도 불구하고 금융, 제조, 보안 등 전문 산업 분야에 AI 를 도입하는 데에는 여전히 어려움이 있다. LLM 은 방대한 지식을 바탕으로 다양한 주제에 대해 폭넓게 답할 수 있지만, 특정 산업이나 도메인에 그대로 적용하기에는 다음과 같은 한계점이 있다.

- 정확성과 신뢰성 부족

LLM 은 사실과 다른 정보를 그럴듯하게 생성하는 '환각(Hallucination)' 현상에서 자유롭지 않다. 또한 학습하지 않은 최신 데이터가 있을 시 정확성이 떨어진다. 예를 들어, 최신 제로 데이 취약점 관련 질문에 부정확한 답변을 하거나, 존재하지 않는 IP 를 공격자로 지목하는 등 잘못된 공격 패턴을 제시할 수 있는 위험성이 있다.

- 전문 지식 및 맥락 이해의 한계

분야마다 사용하는 고유 용어 등 LLM 이 이해하지 못하는 깊이 있는 전문 지식이 존재하기 마련이다. 사이버보안의 경우, 대응 시 공격 기법(TTPs), 복잡한 로그 데이터 등 깊이 있는 전문 지식이 필요하다. LLM 은 용어의 미묘한 차이나 특정 공격 벡터의 맥락을 완벽하게 이해하지 못해 위협에 효과적인 대응이 불가하다.

- 데이터 유출 및 보안 위험

LLM 은 주로 외부 API 통신을 통해 사용된다. 내부 시스템 로그, 악성코드 샘플 등 민감한 데이터를 전송하는 것은 그 자체로 심각한 데이터 유출 사고로 이어질 수 있다.

최근 이러한 한계로 특정 산업과 도메인에 최적화된 Vertical AI 의 필요성이 커지고 있다. Vertical AI 는 특정 내부 데이터와 전문 지식을 직접 학습하거나 실시간으로 참조하여 보다 정확하고 신뢰성 있는 답변을 지원한다. 또한, 통제된 내부 인프라에서 모델을 운영함으로써 데이터의 외부 유출을 차단할 수 있다.

Vertical AI 를 구현하기 위해 각 도메인에 특화된 LLM 을 체계적으로 설계하고 구축하는 것이 핵심 경쟁력으로 꼽힌다. 도메인 특화 LLM 은 단순한 기술적 구현을 넘어 산업별 문제 해결과 혁신을 가속화하는 Vertical AI 의 중심 엔진으로 자리잡고 있다.

■ 2. 사이버보안 특화 LLM 구축 방안

사이버보안 특화 LLM 은 내부 데이터와 보안 전문 지식을 기반으로 정확한 답변을 생성할 수 있는 LLM 과 그 외 시스템 구축을 목표로 한다. 구축을 위한 세 단계는 1. 기반 모델 선정 2. RAG 구축 3. LLM 파인튜닝 순이며, 이는 신입 수준의 모델을 전문가 수준으로 성장시키는 과정을 거쳐야 한다.

그림 3. 사이버보안 특화 LLM 구축 프로세스

2.1 목적에 맞는 기반 모델 선정

사이버보안 도메인 특화 LLM 을 구축하기 위해서는 우선 목적에 부합하는 기반 모델(Base Model)을 선정하는 과정이 필요하다. 단순히 최신 성능의 LLM 을 선택하는 것이 아니라, 실제 보안 환경에서 요구되는 정확성, 확장성, 보안 내재화 요소 등을 종합적으로 고려해야 한다.

기반 모델 선정 시 고려해야 할 주요 기준은 다음과 같다.

- 모델 크기와 성능의 균형

크기가 큰 모델일수록 정확도가 높지만 학습과 추론에는 많은 자원이 필요하다. 또한, 실시간성이 중요한 사이버 위협 대응 환경에서는 응답 지연(latency)은 문제가 발생할 수 있다. 따라서 업무 목적과 리소스 제약에 따라 모델 규모를 조절하는 것이 중요하다.

- 보안 특화 데이터와의 적합성

사이버보안 데이터는 일반 텍스트와 달리 로그, 코드, 스크립트, 취약점 데이터(CVE) 등 다양한 비정형 텍스트로 구성된다. 이러한 보안 특화 데이터를 효율적으로 이해하고 처리할 수 있는 모델을 선택해야 한다. SecBench, SecEval 등 사이버보안 벤치마크 데이터셋을 통해 모델을 사전에 검증한다.

- 보안 내제화

개인정보 비식별화, 민감 데이터 필터링 등 보안 기능을 제공하거나 연계가 용이한 모델인지 고려한다. 또한, 모델이 입력 데이터나 학습 데이터에 포함된 민감 정보를 외부로 유출하지 않고 안전하게 처리할 수 있는지 확인해야 한다.

기반 모델은 최대 성능만 고려하는 것이 아니라, 한정된 자원 내에서 성능, 비용, 보안 등 다양한 지표 간의 트레이드 오프 관계를 이해한 후 전략적으로 선정해야 한다. 최신 정보 반영, 부족한 도메인 전문성과 같은 문제는 이후 설명할 RAG 와 파인튜닝을 통해 보완할 필요가 있다.

2.2 최신성과 신뢰성 강화를 위한 RAG 구축

LLM 은 방대한 지식을 가지고 있지만, 학습 시점이 고정되어 있어 최신 정보를 반영하지 못하거나 사실이 아닌 정보를 그럴듯하게 만들어내는 환각 현상을 보인다. 또한, 명확한 답변의 근거를 제시하지 못하면 신뢰도에 문제가 생기기도 한다.

이러한 문제를 해결하기 위해 등장한 기술이 검색 증강 검색(Retrieval-Augmented Generation, RAG)이다. RAG 는 LLM 이 더 정확하고 신뢰할 수 있는 답변을 생성하도록 돕는 기술로, LLM 이 치르는 오픈북 시험에 비유할 수 있다. LLM 이 자체적으로 학습한 지식에 의존하는 것이 아니라, 질문을 받으면 관련된 정보를 검색하여 참고한 뒤 그 내용을 바탕으로 답변을 생성하는 방식이다.

RAG 를 통해 LLM 은 답변의 근거가 되는 최신 위협 정보나 내부 데이터 소스를 제시할 수 있어, AI 판단의 신뢰성과 설명 근간을 확보할 수 있다. 또한, 기존에 파편화되어 있던 각종 위협 정보, 시스템 로그 등을 하나의 지식 베이스로 연결하여 자연어 질문 하나로 모든 정보를 탐색할 수 있게 한다.

RAG 구축 및 활용 프로세스는 다음과 같다.

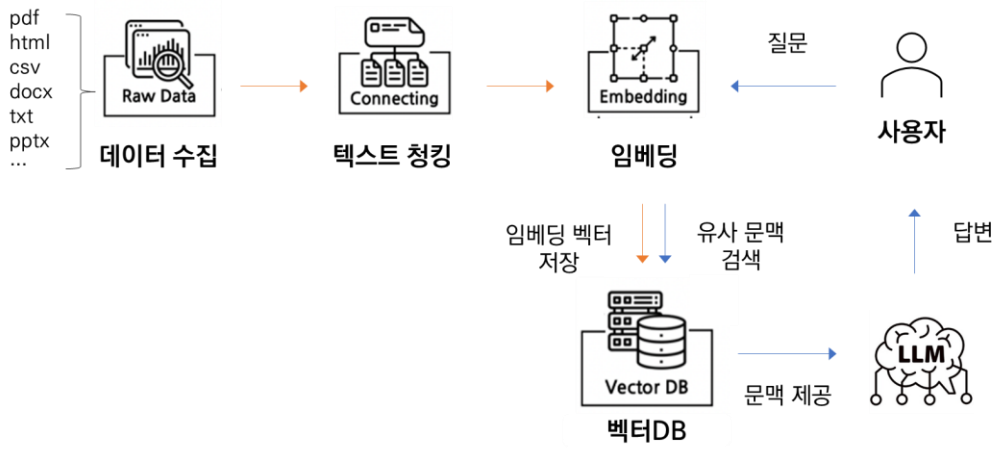


그림 4. RAG 구축 및 활용 프로세스

① 데이터 수집

답변의 근거로 삼을 수 있는 내 · 외부 데이터(pdf, docx, pptx 등)를 우선적으로 수집해야 한다. 데이터의 품질은 RAG 시스템의 성능에 직접적인 영향을 미치므로, 정확하고 최신 정보를 포함하도록 관리해야 한다.

② 텍스트 청킹

LLM 이 처리하기에 적합한 크기의 텍스트 청크(chunk) 단위로 데이터를 분할한다. 청크 크기는 LLM 의 성능, 데이터의 특성, 검색 효율성 등을 고려하여 결정한다. 너무 작은 청크는 문맥 정보를 잃을 수 있으며, 너무 큰 청크는 LLM 처리에 부담을 가중시킬 수 있다.

③ 임베딩

임베딩 모델(Embedding Model)을 사용해 텍스트 청크를 숫자로 이루어진 벡터로 변환한다. 임베딩 모델은 텍스트의 의미를 보존하면서 벡터 공간에 표현하는 역할을 한다. 고품질의 임베딩 모델을 선택하는 것이 RAG 시스템의 성능 향상에 중요하다.

④ 벡터 DB 구축

변환된 벡터는 벡터 DB(Vector Database)에 저장한다. 벡터 DB 는 유사한 벡터를 효율적으로 검색할 수 있도록 설계된 특수한 데이터베이스로 Milvus, Chroma, Weaviate 등의 벡터 DB 를 활용할 수 있다.

⑤ 검색 및 생성

사용자 질문과 유사한 문맥을 가진 데이터를 벡터 검색을 통해 추출한다. 검색된 데이터를 기반으로 LLM 이 응답을 생성한다. 이 과정에서 LLM 이 원본 데이터의 문맥을 반영하므로 정확도와 신뢰도가 높아진다.

2.3 도메인 지식 내재화를 위한 LLM 파인튜닝

RAG 를 통해 최신 데이터를 반영할 수 있으나, 특정 보안 영역에서 요구되는 심층적인 지식과 맥락 이해는 부족할 수 있다. 이를 보완하는 방법이 파인튜닝(Fine-Tuning)이다. 다만, 파인튜닝은 필수적인 것은 아니며 업무 목적과 환경에 따라 선택적으로 적용해야 한다.

파인튜닝을 통해 조직의 고유한 보고서 스타일을 따르거나 특정 공격 유형에 민감하게 반응하는 AI 를 만들 수 있다. 사이버보안 분야의 전문성을 내재화하여 보안 분석 보고서 작성, 위협 탐지 패턴 해석, 사고 대응 절차 제안 등의 업무에서 보다 정교한 답변을 제공받을 수 있다.

파인튜닝 과정은 다음과 같이 세 단계로 나타낼 수 있다.

① 데이터셋 구축

모델 학습용 데이터셋을 구축한다. 도메인 전문 데이터를 기반으로 질의응답(Question-Answer) 형식의 데이터 쌍을 여러 개 생성한다. 데이터셋의 품질은 파인튜닝 결과에 직접적인 영향을 미치므로 고품질의 데이터셋을 구축하는 것이 중요하다.

② 모델 학습

준비된 데이터셋을 사용하여 사전 학습된 기반 모델을 추가로 학습하는 단계이다. 구축된 질의응답 데이터셋을 따라 하도록 모델을 학습시키고 파인튜닝(Supervised Fine-Tuning)을 수행한다. 이 때, 모델 전체를 재학습 시키는 방식은 상당한 컴퓨팅 자원을 소모하므로 일부 파라미터만 수정하는 PEFT(Parameter-Efficient Fine-Tuning)와 같은 효율적인 기법을 사용한다.

③ 평가 및 배포

파인튜닝이 완료된 모델이 태스크에 대한 성능 향상을 달성했는지 평가한다. 또한 모델이 새로운 전문 지식을 학습하면서 기존에 가지고 있던 방대한 일반 지식을 유지하는지 검증해야 한다. 검증을 통과한 모델은 실제 운영 환경에 배포해 활용한다.

기반 모델 선정, RAG 구축, 그리고 LLM 파인튜닝의 3 단계 접근법을 통해 내부 데이터와 최신 위협 정보를 효과적으로 활용하여 정확하고 신뢰성 높은 답변을 생성하는 LLM 시스템 구축 방법을 알아보았다. 그러나 성공적인 LLM 시스템 구축만큼 중요한 것은 시스템을 안전하게 운영하고 잠재적인 위협으로부터 보호하는 것이다. 3 장에서는 LLM 시스템의 보안 취약점과 그에 대한 효과적인 대응 방안을 구체적으로 살펴본다.

■ 3. LLM 시스템 보안 취약점 및 대응 방안

LLM 이라는 최신 기술의 성장으로 기존 웹 애플리케이션과는 새로운 보안 위협들이 등장하고 있다. 금융, 의료, 보안 등 특정 산업들은 개인정보보호 및 데이터 보안에 엄격한 규제를 받고 있다. 민감한 정보가 많아 보안에 특히 주의해야 한다. 구축한 LLM 시스템에서 발생할 수 있는 보안 취약점을 사전에 파악하고 그에 대한 대응 방안을 마련하는 것이 중요해지고 있다.

3.1 LLM 시스템 보안 취약점

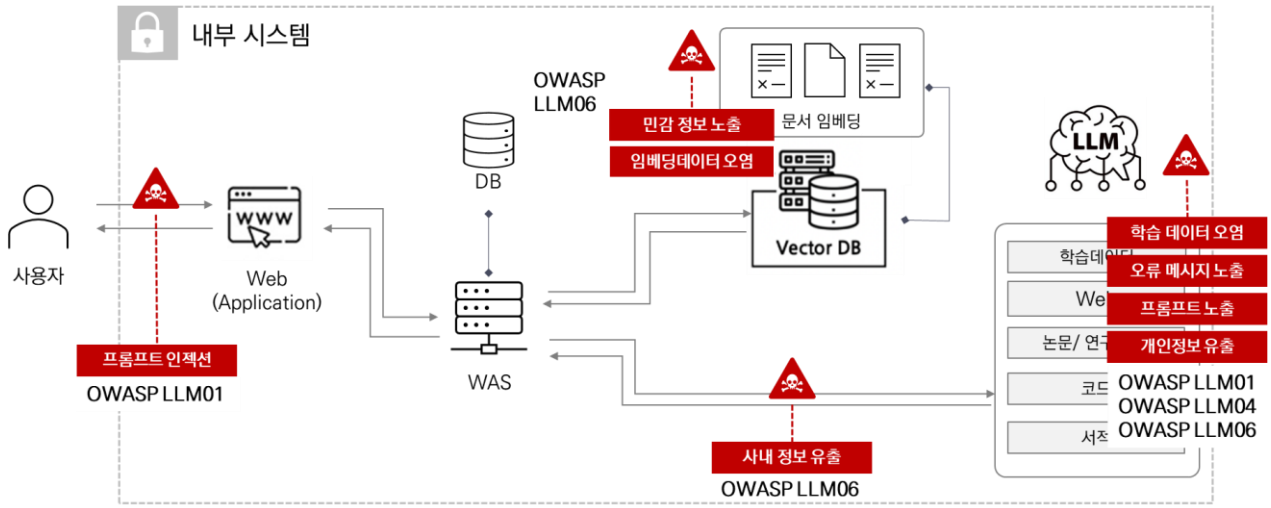


그림 5. LLM 보안 취약점

LLM 시스템에서 발생할 수 있는 취약점은 LLM 모델의 내재적 취약점과 시스템 인프라 및 운영 환경의 외재적 취약점으로 구분할 수 있다. 이 두 가지는 서로 다른 공격 경로와 방어 전략이 필요하므로 이를 분리하여 이해하는 것이 중요하다.

① LLM 자체 취약점

LLM 자체 취약점은 모델의 작동 방식과 데이터 처리 과정에서 발생하는 문제이다. 주로 모델의 예측을 조작하거나 의도하지 않은 동작을 유도하는 방식으로 나타난다. 대표적인 취약점은 프롬프트 인젝션, 민감 정보 유출, 학습 데이터 오염 등이 있다.

- 프롬프트 인젝션(Prompt Injection)

공격자가 모델에 입력하는 프롬프트를 조작하여 모델의 예측을 조작하거나 의도하지 않은 동작을 유도하는 공격이다.

- 민감 정보 유출(Sensitive Information Disclosure)

모델이 출력하는 정보 중 민감한 정보가 포함되어 있는 경우, 이를 제대로 처리하지 않아 정보가 유출되는 취약점이다.

- 학습 데이터 오염(Data and Model Poisoning)

공격자가 모델의 사전학습 또는 미세조정 과정에 사용되는 데이터셋에 악의적인 데이터를 주입하는 공격을 의미한다.

② 시스템 인프라 및 운영 취약점

LLM을 구동하고 서비스로 제공하는 전체 시스템 환경에서 발생하는 보안 문제이다. 모델 자체보다는 모델을 둘러싼 인프라가 공격 대상이 된다. 대표적인 취약점은 공급망 공격, 인증 및 권한 관리 취약점, 임베딩 데이터 오염 등이 있다.

- 공급망 공격(Supply Chain Vulnerabilities)

LLM, 파인튜닝에 사용되는 데이터셋, 외부 라이브러리 등 LLM 시스템을 구성하는 외부 요소에서 발생하는 취약점을 통해 시스템 전체가 위험에 노출되는 취약점이다.

- 인증 및 권한 관리 취약점(Authentication & Authorization Vulnerabilities)

LLM 시스템을 사용하는 사용자의 부적절한 인증 및 권한 관리를 이용해 공격자가 시스템에 접근하거나 데이터를 조작하는 취약점이다.

- 임베딩 데이터 오염(Embedding Data Poisoning)

RAG 시스템에서 발생하는 취약점으로, 공격자가 벡터 DB 에 저장된 임베딩 데이터를 조작하는 것을 의미한다.

3.2 최신성과 신뢰성 강화를 위한 RAG 구축

LLM 시스템에서 발생할 수 있는 다양한 보안 취약점들은 시스템 설계 단계부터 체계적인 보안 아키텍처를 적용해야 효과적으로 대응할 수 있다. 사용자 인증부터 데이터 처리, 모델 응답에 이르는 전 과정에 걸쳐 보안을 내재화해야 한다.

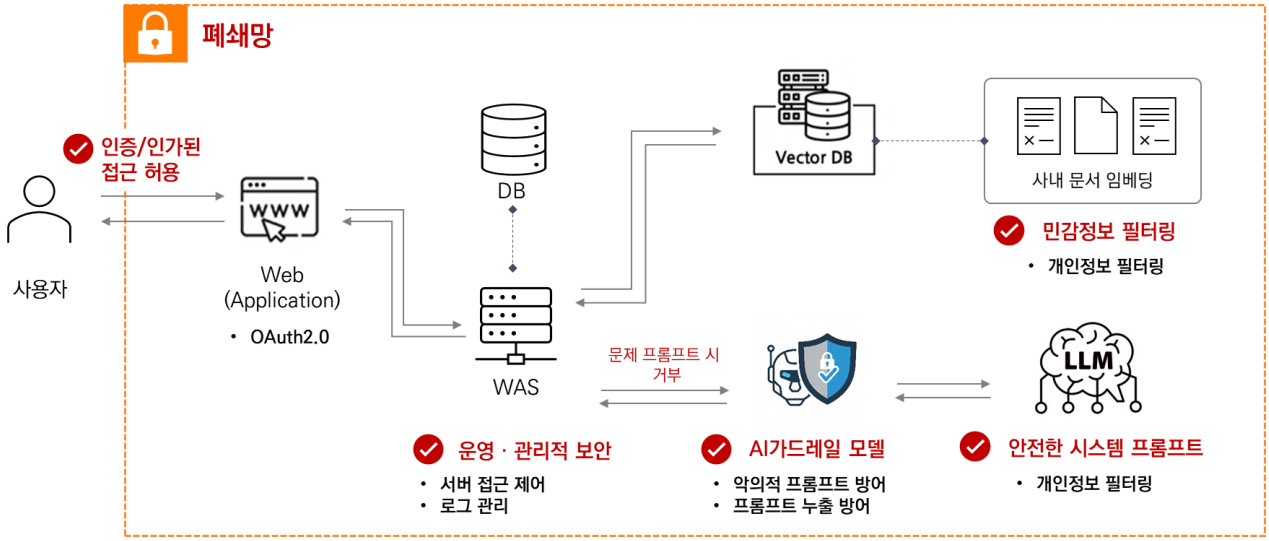


그림 6. 안전한 LLM 시스템 아키텍처

[그림 6]은 보안 취약점에 대응하기 위해 AI Guardrail 을 적용하여 입출력을 제어하였으며, 폐쇄망과 다층적 보안 구조를 통해 구축된 안전한 LLM 시스템 아키텍처 예시를 보여준다.

① AI Guardrail 을 적용한 입출력 제어

프롬프트 인젝션(Prompt Injection), 민감 정보 유출와 같이 LLM 입출력과 관련된 취약점을 대응하기 위해 입출력 내용을 필터링하는 AI 가드레일을 사용할 수 있다. 단순히 특정 키워드를 차단하는 것을 넘어, 문맥을 이해하고 정책 기반으로 잠재적 위협을 방어하는 역할을 수행한다.

- 입력 데이터 필터링

사용자의 질의는 메인 LLM 에 전달되기 전 AI 가드레일을 통해 먼저 검증된다. 이 과정에서 악의적인 공격 패턴이나 민감 정보 유출 시도가 감지되면 해당 요청을 즉시 차단하고 관리자에게 알림을 전송한다.

- 출력 데이터 제어

LLM 이 생성한 응답에 외부 유출이 금지된 민감 정보나 기밀 데이터가 포함된 경우, 이를 최종 사용자에게 전달하기 전에 차단하여 정보 유출을 방지한다.

② 폐쇄망 구성과 다층적 보안 구조

LLM 시스템은 외부와 완벽히 차단된 폐쇄망(내부망) 환경에서만 운영되도록 설계하여, 외부로의 정보 유출 경로를 원천적으로 차단한다. 또한, 모델 학습에 사용된 데이터와 실제 서비스 운영에서 처리되는 데이터를 명확히 분리하여 관리해야 한다.

- 신뢰할 수 있는 모델 공급망 확보

공급망 공격을 예방하기 위해 공신력 있는 기업이나 연구 기관이 제공하는 LLM 모델만을 채택해야 한다. 모델 배포 시에는 해시 값 검증을 통해 무결성을 확보하고, 모든 업데이트는 중앙 관리 서버를 통해서만 안전하게 수행한다.

- 강화된 사용자 접근 통제

SSO(Single Sign-On) 기반의 표준화된 인증 절차를 적용하고 역할 기반 접근 제어(RBAC, Role-Based Access Control)를 통해 사용자의 권한을 세분화하여 시스템 접근을 엄격하게 통제한다.

■ 맺음말

성공적인 사이버보안 LLM 도입을 위해서는 범용 LLM 한계를 보완한 보안에 특화된 LLM 구축에 있다. 이 과정에서 RAG, 파인튜닝과 같은 기술 구현은 물론, 프롬프트 인젝션 등의 새로운 위협에 대응할 LLM 보안 체계도 반드시 병행돼야 한다. 기술과 보안의 균형을 갖춘 특화 LLM 은 지능화되는 위협 환경에 선제적으로 대응하고, 미래 보안 경쟁력을 확보하는 핵심 동력이 될 것이다.

SK 쉴더스 사이버보안 AI 랩스에서는 AI 발전 트랜드에 따라 대규모 언어 모델(LLM)을 기반으로 한 생성형 AI 연구 과제를 진행하고 있다. 최근 자체 기술력으로 사내 내부망에서 안전하게 활용할 수 있는 '생성형 AI Shieldi(쉴디)' 서비스를 개발하여 고도화하였다. 이를 통해 사내 정책/가이드라인에 대한 맞춤형 상담과 보고서 생성 · 번역 · 요약 등 AI 기반의 업무 생산성을 높이고 Shadow AI 와 같은 잠재적 보안 위협을 최소화할 것으로 기대하고 있다.

■ 참고문헌

[1] DeepSeek-AI, DeepSeek-V3 Technical Report, 24.12

[2] DeepSeek-AI, DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning, 2501

[3] Llama Team, AI @ Meta, The Llama 3 Herd of Models, 24.07

■ 참고 자료

[1] Meta, The Llama 4 herd: The beginning of a new era of natively multimodal AI innovation

[2] SK쉴더스 EQST 그룹, LLM Application 취약점 진단 가이드

Keep up with Ransomware

기존 랜섬웨어 코드를 재활용한 BlackField 랜섬웨어

■ 개요

2025 년 10 월 랜섬웨어 피해 사례 수는 지난 9 월(583 건) 대비 약 37% 증가한 799 건으로 집계됐다. 기존 주요 그룹인 Qilin·Sinobi 등의 지속적인 공격 활동에 더해, 10 월 새롭게 등장한 여러 신규 랜섬웨어 조직이 공격에 가세하면서 전체 피해 규모가 확대된 것으로 보인다.

Clop 그룹은 Oracle E-Business Suite 의 신규 취약점(CVE-2025-61882)을 악용해 침투한 것이 확인되었다. 해당 취약점은 인증 없이 페이로드[1] 가 포함된 POST 요청만으로 서버 내부 기능 호출이 가능하며, 이를 통해 공격자는 원격에서 코드를 실행할 수 있다. Clop 은 과거에도 취약점을 악용한 대규모 공격을 반복해왔다. 2023 년도에는 MOVEit Transfer 의 SQL Injection 취약점(CVE-2023-34362, CVE-2023-35036, CVE-2023-35708)을 악용했으며, 2024 년도에는 Cleo 사의 파일 전송 솔루션 제품군에서 발견된 인증 우회 취약점(CVE-2024-55956)을 악용해 대규모 침해를 발생시켰다.

한편, 취약점을 악용한 침투 사례는 Clop 그룹 이외에도 타 랜섬웨어 그룹에서 지속적으로 확인되고 있다. Medusa 그룹은 Fortra GoAnywhere MFT 에서 발생한 취약점(CVE-2025-10035)을 악용한 사례가 보고됐다. 이 취약점은 사용자 인증 없이 특정 요청을 전달할 경우, 서버가 이를 오처리 하도록 유도해 공격자의 명령을 실행할 수 있게 되는 취약점이다. 공격자는 이를 악용해 악성 스크립트 실행과 내부 데이터 탈취를 수행했으며, 최종적으로 랜섬웨어까지 실행했다.

[1] 페이로드(payload): 공격자가 악의적인 실행을 유도하기 위해 첨부하는 데이터/명령

SLSH 그룹은 2025 년 8 월 처음 등장했다. 외부적으로는 Lapsus$와 Scattered Spider 그룹이 ShinyHunters 와 합류해 구성된 연합체인 것처럼 홍보하고 있다. 그러나 실제로는 ShinyHunters 를 중심으로 두 그룹의 일부 구성원만 참여한 형태로, 운영자가 다중 닉네임을 활용해 연합체처럼 보이도록 위장한 것으로 확인된다. 이들은 자체 구축한 다크웹 데이터 유출 사이트와 운영 인프라 등을 EaaS(Extortion-as-a-Service)[2] 형태로 외부 공격자에게 대여하고 있다. 이는 널리 알려진 RaaS(Ransomware-as-a-Service)[3] 모델과 유사하지만, 데이터 탈취와 협박에 중점을 둔다는 점에서 EaaS 와는 차이가 있다. SLSH 는 10 월 초 데이터 유출 사이트를 개설해 탈취한 정보를 게시하였으나, 10 월 11 일 법 집행기관의 압박이 강화되었다는 이유로 2026 년까지 활동을 중단하겠다고 발표했다. 이에 따라 해당 그룹이 운영하던 다크웹 유출 사이트는 현재 비활성화된 상태다.

한편 SLSH 의 운영진 중 하나인 ShinyHunters 는 과거 BreachForums 의 관리자 역할을 수행했던 인물로 유명하다. BreachForums 는 2022 년부터 2024 년까지 법집행기관의 압박으로 여러 차례 폐쇄되었다가, 부활이라는 명목으로 반복 등장한 바 있다. 2025 년 하반기에 다시 모습을 드러낸 BreachForums 는 복구된 것처럼 보였으나, ShinyHunters 는 SLSH 텔레그램 채널을 통해 10 월 이후 해당 포럼은 더 이상 운영되지 않으며 이후 새롭게 개설되는 사이트는 법집행기관이 운영하는 허니팟일 확률이 높다고 주장하였다.

[2] EaaS(Extortion-as-a-Service): 데이터 탈취·협박을 서비스 형태로 제공하는 비즈니스 모델

[3] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 공격할 수 있도록 하는 비즈니스 모델

■ 랜섬웨어 뉴스

Clop, Oracle E-Business Suite의 신규 취약점을 악용해 침투

- Oracle E-Business Suite의 신규 취약점(CVE-2025-61882)을 악용해 인증 없이 서버 내부 기능 호출 및 코드 실행을 수행
- 해당 취약점은 인증 없이 원격 코드 실행이 가능
- Clop은 2023년 MOVEit, 2024년 Cleo 파일 전송 솔루션 등 과거에도 제로데이 취약점을 통한 대규모 침해 사례가 확인됨

Medusa의 GoAnywhere MFT 취약점(CVE-2025-10035) 악용 공격

- Medusa 그룹은 Fortra GoAnywhere MFT의 취약점(CVE-2025-10035)을 악용한 것으로 확인됨
- 해당 취약점은 인증 없이 서버에 악의적 요청 가능
- 요청 처리 오류로 인해 공격자의 악의적인 명령 실행이 가능

SLSH, EaaS 기반으로 활동하는 신규 위협 그룹 등장

- Lapsus$, Scattered Spider, ShinyHunters의 연합체를 주장하지만 실제로는 소수 운영자가 다중 닉네임으로 운영함
- 이들은 RaaS 모델이 아닌 데이터 탈취·협박 중심의 EaaS 모델을 사용함
- 10월 초 데이터 유출 사이트 개설 후 활동 시작 이후 법 집행기관의 단속 압박 등으로 현재는 사이트가 비활성화된 상태

BreachForums 재등장에 대해 ShinyHunters는 법집행기관이 운영하는 허니팟이라 주장

- BreachForums은 2022년부터 2024년까지 여러 차례 법집행기관 압박으로 폐쇄되었으나 이후 반복적으로 재등장함
- 2025년 하반기에 다시 등장한 BreachForums은 정상 복구된 것처럼 보였지만 진위에 대한 의혹이 제기됨
- ShinyHunters는 SLSH 텔레그램을 통해 해당 사이트가 법집행기관 운영 허니팟일 가능성이 높다고 주장함

10월, 신생 그룹 9개 등장

- 전체 신규 그룹중 NasirSecurity, BrotherHood, FulcrumSec, Genesis 는 암호화가 아닌 데이터 갈취 중심
- 산업 구분 없이 무차별적 표적 공격이 증가

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

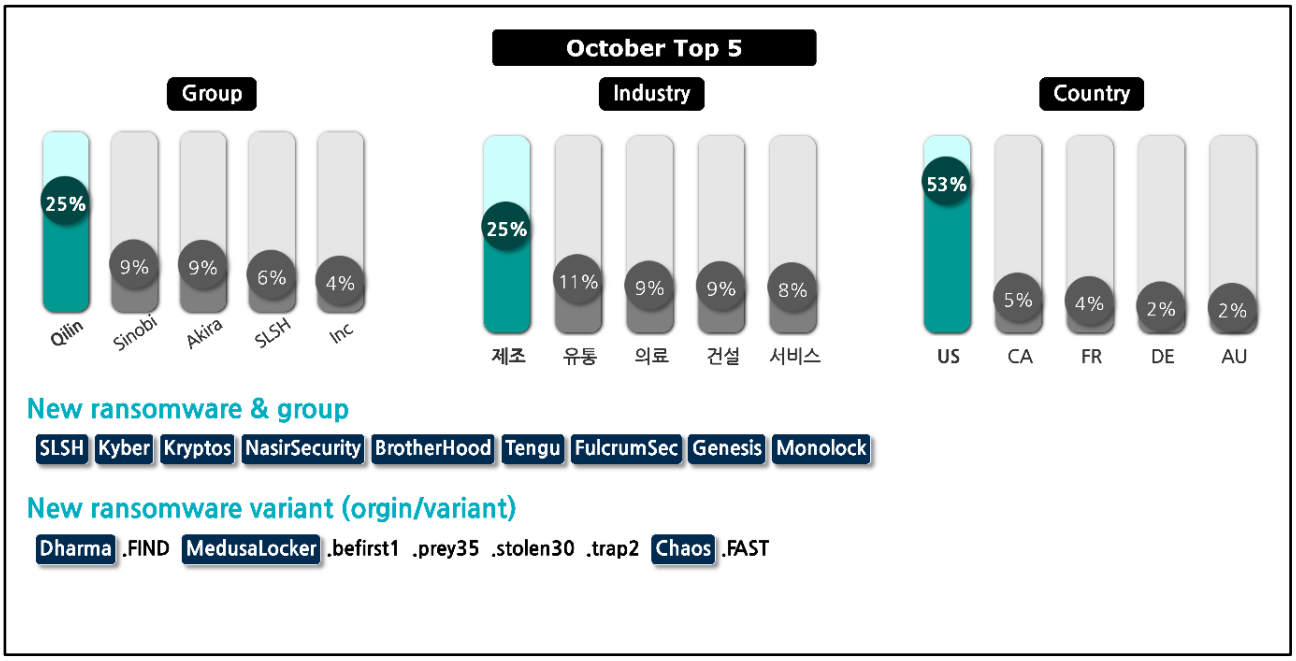


그림 2. 2025 년 10 월 랜섬웨어 위협 현황

새로운 위협

10 월에는 총 9 개의 신규 랜섬웨어 그룹이 등장했다. 이들 중 SLSH, Kyber, Kryptos, Tengu, BrotherHood, FulcrumSec, Genesis 는 자체 다크웹 유출 사이트를 운영하고 있다. 현재 Tengu 와 FulcrumSec 의 다크웹 유출 사이트는 비활성화된 상태로 확인된다.

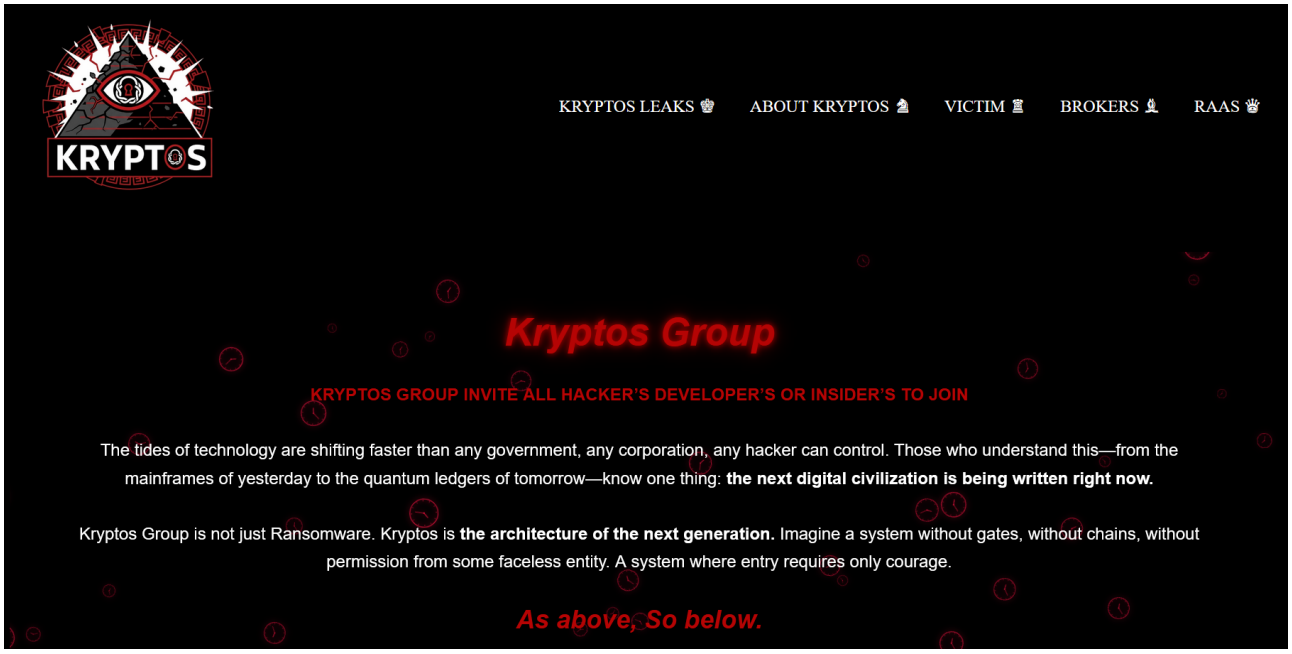


그림 3. Kryptos 의 RaaS 모집글

2025 년 10 월에 발견된 Kryptos 랜섬웨어는 현재까지 총 5 건의 피해 정보를 게시했다. 해당 그룹이 공개한 RaaS 계열사 모집 글에 따르면, 참여자는 매달 50 달러(한화 약 7 만원)의 유지비를 내야 하며 공격 성공 시 수익의 10%를 지불해야 한다고 명시되어 있다. 또한 단순히 가입 의사를 밝히는 것만으로는 계열사로 활동할 수 없으며, 가입 전 반드시 'Attack Phase'라는 테스트 절차를 통과해야 한다. 내부자·브로커·개발자 유형에 따라 서로 다른 검증 기준을 적용하는 등, 엄격한 선발 체계를 통해 운영하고 있는 것으로 분석된다.

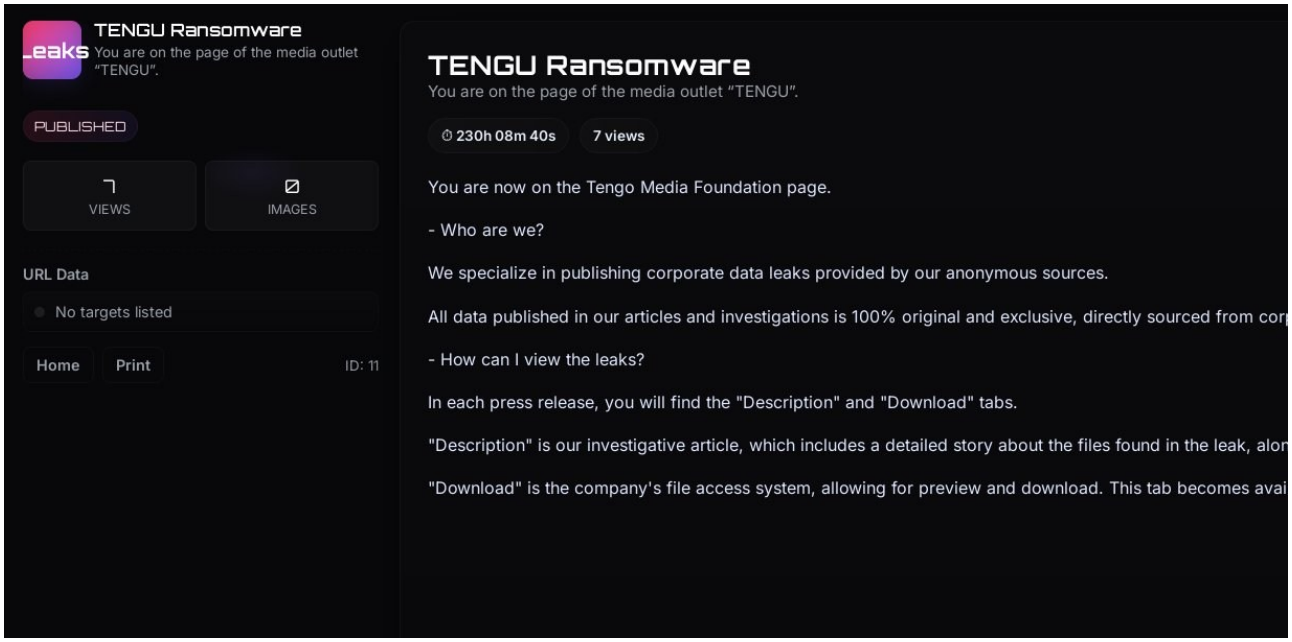


그림 4. Tengu 의 다크웹 유출 사이트

2025 년 10 월에 발견되어 현재까지 총 6 건의 피해 사례가 확인된 Tengu 랜섬웨어는, 등장 초기부터 다크웹 유출 사이트뿐만 아니라 X 에서도 활동을 홍보하며 존재감을 드러냈다. 그러나 현재 Tengu 가 운영하던 다크웹 유출 사이트는 접근이 불가능한 상태다. 이후 추가적인 공격 징후도 확인되지 않고 있다.

Top5 랜섬웨어

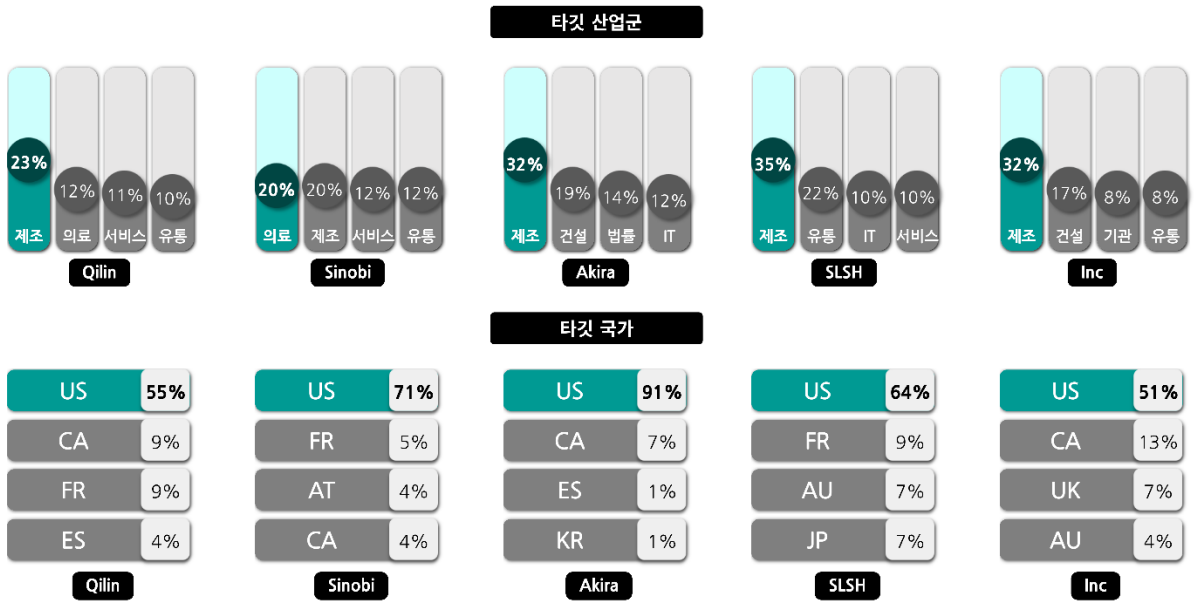


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

일본의 음료 제조사 아사히는 Qilin 그룹의 공격을 받아 생산 라인이 일시 중단되었다. 내부 재무 문서·공급망 자료·계약 문서 등이 포함된 약 27GB 규모의 데이터가 탈취됐다. 해당 데이터는 이후 Qilin 그룹의 다크웹 유출 사이트에 공개되었다.

Sinobi 그룹은 10 월 13 일 미국 뉴저지주의 의료 센터인 Central Jersey Medical Center 를 공격해 약 930GB 규모의 환자 개인정보를 포함한 데이터를 탈취했다. 이 자료는 다크웹 유출 사이트를 통해 공개됐다. 이어 10 월 28 일 미국 플로리다주의 환경분석 기업인 Florida-Spectrum Environmental Services 를 공격해 기업의 재무제표 및 계약서 등을 포함한 약 500GB 의 데이터를 탈취했다.

Akira 그룹은 10 월 2 일 미국의 컴퓨터 저장장치 제조사 Apricorn 을 공격해 직원 의료기록, 재무 정보, 계약서 등을 포함한 데이터를 다크웹 유출 사이트에 공개하겠다고 협박했다. 같은 날 미국의 디스플레이 제조사인 DisplayIt 도 공격 대상이 되어 기밀 파일과 프로젝트 자료가 유출됐다.

SLSH 그룹은 10 월 초 토요타, FedEx, UPS, Disney/Hulu 등 약 39 개 기업의 정보를 유출 사이트에 게시하며, 10 월 10 일까지 응답이 없을 경우 모든 자료를 공개하겠다고 협박했다. 또한, 같은 시기 Red Hat Consulting 의 내부 GitLab[4] 저장소에서 약 570GB 규모의 소스코드와 고객 리포트를 탈취했다고 주장하며, 이를 다크웹에 게시했다.

[4] GitLab: 기업 내부 개발 소스코드와 CI/CD 설정 등 핵심 개발 자산이 저장된 플랫폼

INC 그룹은 미국의 골프 의류 제조사 Summit Golf Brands 를 공격해 약 47GB 의 데이터를 탈취했다. 회계 자료, 디자인 파일, 인사 자료 등이 포함된 유출 자료는 다크웹 사이트에 공개되었다. 또한, 이들은 프랑스의 IT 기업인 Partitio 를 공격해 약 437GB 규모의 데이터를 유출했다.

SafePay 그룹은 미국 오하이오주 Liberty Township 교육청을 공격해 일부 내부 재무자료, 운영 문서, 교직원 관련 문서가 포함한 48GB 의 데이터를 탈취했다. 또한 독일의 IT 서비스업체 MCSL GmbH 도 공격을 받아 고객 보고서, 프로젝트 문서, 내부 커뮤니케이션 파일이 유출됐다. 미국의 차고 문 제조업체 The Overhead Door Company 역시 공격을 당했다. 해당 기업은 기술 문서, 회계 기록, 고용 계약서 등이 포함된 내부 자료가 노출된 것으로 확인됐다.

한편, Inc 그룹은 독일의 통신기기 제조업체 funktel GmbH 의 3.5TB 가량의 데이터를 탈취했다고 주장했다. 이들은 주요 제품의 설계도, 내부 메일, 급여 명세서, 운영 계획서 등 다양한 문서를 샘플로 공개됐다. 또한 미국의 의료 업체 Medical Center of Marin 도 공격해 환자 개인정보가 포함된 설문지나 의료 소견서, 환자의 신분증 등 환자의 민감 정보가 유출됐다.

■ 랜섬웨어 집중 포커스

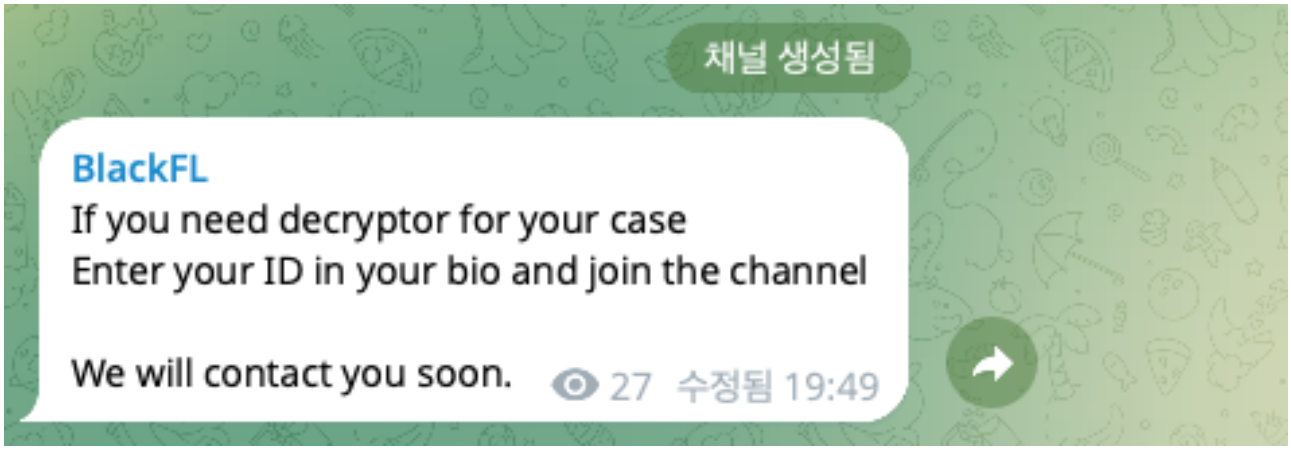


그림 6. BlackField 랜섬웨어 텔레그램 채널

BlackField 랜섬웨어는 2025 년 9 월 악성코드 샘플 공유/분석 플랫폼인 VirusTotal 을 통해 처음 발견되었다. 공개된 2 개의 샘플은 과거 유포된 Cylance 랜섬웨어의 소스코드를 기반으로 개발되었다. 현재 실제 공격 사례는 확인되지 않았으나, 향후 피해 발생이나 데이터 유출 사이트에 활동이 본격화될 가능성이 있다.

```
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp             ; hCrypto
mov     ebp, esp
and     esp, 0FFFFFFF8h
call    HideWindow_407200
call    GetProcessHeap_407290
call    PrivEsc_4055B0
call    ParseCmdLine_401000
call    CreateMutex_4050A0
call    AddScheduleTask_405110
call    CreateLogFile_404CB0
call    CopyRansomNote_405660
call    SetProcessPriv_4051E0
call    DeleteRecycle_405200
call    DeleteShadowCopy_405210
call    VolumeMountAtoZ_4059B0
call    Encrypt_407060
call    DeleteRecycle_405200
call    DeleteShadowCopy_405210
call    RestartDropPE_405450
call    CloseLogFile_404E90
call    DeleteService_4051C0
call    CloseMutex_4050E0
call    SelfDelete_405540
push    0               ; uExitCode
call    ds:ExitProcess
_main endp
```

```
; int __fastcall main(int argc, const char **argv, const char **envp)
main proc near
sub     rsp, 28h
call    HideWindow_140007FB0
call    GetProcessHeap_140008050
call    PrivEsc_140005CB0
call    ParseCmdLine_140001000
call    CreateMutex_140005580
call    AddScheduleTask_140005610
call    CreateLogFile_140005030
call    CopyRansomNote_140005DE0
call    SetProcessPriv_140005740
call    DeleteRecycle_140005770
call    DeleteShadowCopy_140005780
call    VolumeMountAtoZ_140006260
call    Encrypt_140007D50
call    DeleteRecycle_140005770
call    DeleteShadowCopy_140005780
call    Restart_dorpPE_140005AC0
call    CloseLogFile_1400052E0
call    DeleteService_140005700
call    CloseMutex_1400055D0
call    SelfDelete_140005C10
xor     ecx, ecx        ; uExitCode
call    cs:ExitProcess
```

그림 7. Cylance(좌), BlackField(우)

BlackField 랜섬웨어는 Cylance 랜섬웨어와 비교하였을 때 main 함수 내 악성 수행 구조가 완전히 동일하며, PDB[5] 경로에도 'Cylance Ransomware'라는 이름이 명시되어 있다. 이러한 정황으로 볼 때 자체적인 개발 역량을 보유한 그룹이라기보다는 외부에서 소스코드를 구매했거나 공개된 소스를 일부 수정해 활동하는 것으로 판단된다. 또한 BlackField 그룹은 자체 데이터 유출 사이트를 운영하지 않고, 텔레그램 채널·TOX[6] ·이메일 등을 통해 피해자와 접촉하는 것으로 확인되어 실제 활동 및 피해 사례를 직접적으로 확인하기는 어렵다.

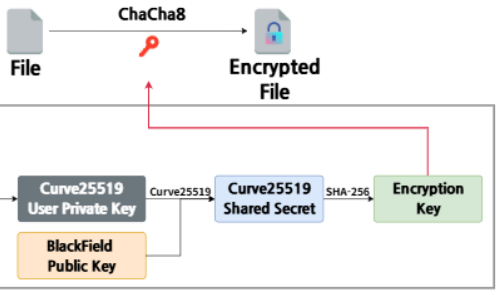
본 보고서는 Cylance 랜섬웨어 기반의 BlackField 랜섬웨어 분석을 진행하여 랜섬웨어 위협에 효과적으로 대비할 수 있도록 하고자 한다.

[5] PDB(Path Database): 프로그램 개발 과정에서 사용된 프로젝트 이름·디렉터리 구조 등이 노출되는 정보

[6] TOX: 중앙 서버 없이 P2P 기반으로 동작하는 익명 메신저

암호화 키

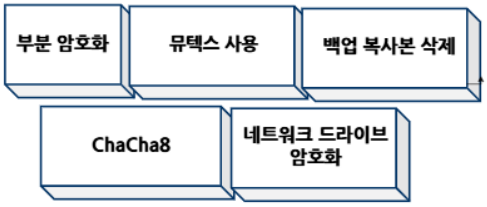
Curve25519 알고리즘으로 암호화 키를 생성하며 ChaCha8 알고리즘으로 암호화



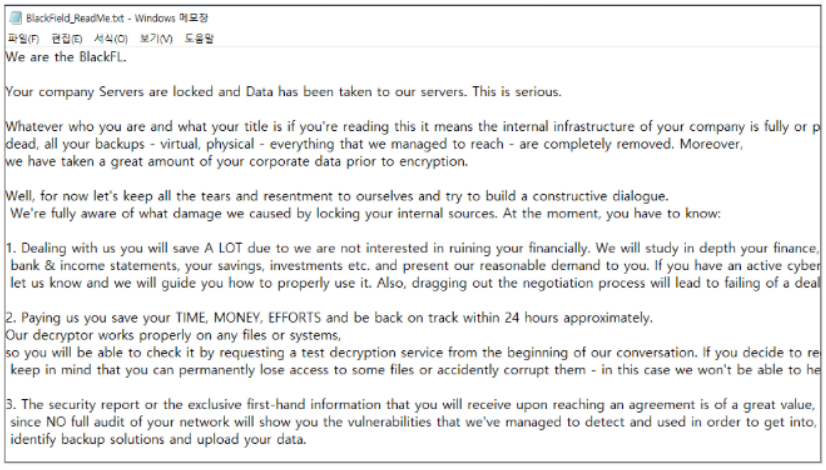
암호화 방식

* Full Mode.
  파일 전체 암호화
* Split Mode.
  -Skip 인자로 전달받은 암호화 간격만큼 스킵하며 1MB 암호화
* Custom Mode.
  파일 크기 ≤ 16MB: 파일 전체 암호화
  파일 크기 16MB ~ 512MB: 256KB 간격마다 1MB 암호화
  파일 크기 512MB ~ 8GB: 4MB 간격마다 1MB암호화
  파일 크기 8GB ~ 128GB: 64MB 간격마다 1MB 암호화
  파일 크기 128GB ~ 2TB: 1GB 간격마다 1MB 암호화
  파일 크기 > 2TB: 16GB 간격 마다 1MB 암호화

특징



랜섬노트


BlackField_ReadMe.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
We are the BlackFL.

Your company Servers are locked and Data has been taken to our servers. This is serious.

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or p
dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover,
we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue.
We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance,
bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber
let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately.
Our decryptor works properly on any files or systems,
so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to re
keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to he

3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value,
since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into,
identify backup solutions and upload your data.

BlackField_ReadMe.txt

변경 확장자

.BlackFL

제작 언어

C/C++

그림 8. 랜섬웨어 개요

DireWolf 랜섬웨어 전략

그림 9. 랜섬웨어 공격 전략

BlackField 랜섬웨어는 다양한 실행 인자를 통해 암호화 동작을 정밀하게 제어할 수 있도록 설계되어 있다. 이러한 구조는 공격자가 목표 타겟, 암호화 방식, 뮤텍스 생성 여부를 유연하게 설정할 수 있다. BlackField 의 실행 인자와 기능은 아래 표와 같다.

옵션	보조 옵션	서비스
-path	-	암호화 대상 경로 지정, 옵션이 존재하지 않으면 전체 암호화
-mode	full	파일 전체 암호화
	fast	파일 부분 암호화
	split	특정 크기 간격으로 암호화
	Custom	랜섬웨어 내 정의된 파일 크기에 따라 부분 암호화
-priority	off	프로세스 우선 순위 설정
-skip	-	-split 암호화에서 skip 크기 지정
-power	restart	파일 시스템 덮어쓰기 이후 재시작
	shutdown	파일 시스템 덮어쓰기 이후 시스템 종료
-console	-	암호화 진행 과정 창 활성화 여부 확인
-nomutex	-	중복 실행 방지를 위한 뮤텍스 생성 여부 확인
-nonetdrive	-	네트워크 드라이브 암호화 여부 확인
-nodel	-	암호화 이후 자기자신 삭제 여부 확인

표 1. 랜섬웨어 실행인자

랜섬웨어 실행 시 path 인자와 함께 암호화 대상 경로가 지정되면 시스템 전체 암호화를 하지 않고 지정된 경로에만 암호화된다. 다른 랜섬웨어들이 옵션에 따라 분기해 부분 암호화하는 것과 달리, BlackField 는 path 옵션이 활성화되면 작업 스케줄러에 관리자 권한으로 실행되도록 스스로 등록한 후 즉시 실행한다. 또한 nomutex 옵션이 활성화되지 않은 경우, 랜섬웨어의 중복 실행을 방지하기 위해 "Global\\BlackFLMutex" 문자열로 뮤텍스 [7] 를 생성한다. 이후 랜섬웨어 동작을 기록할 로그 파일을 생성하고, 복호화를 방해하기 위해 휴지통을 비우며 WMI[8] 를 통해 볼륨 섀도 복사본을 삭제한다. 이후 감염 PC 에 연결된 모든 네트워크 드라이브를 시스템에 마운트하여 목록을 로그에 남기고, 이들을 대상으로 암호화하기 위한 초기 절차를 완료한다.

이후 시스템 전체 드라이브를 순차적으로 탐색해 모든 디렉토리를 확인한 뒤, 해당 위치에 랜섬노트를 생성하고, 암호화 대상을 판별한다. 이때 특정 경로와 확장자 및 파일명은 암호화 대상에서 제외한다. 확인된 예외 대상은 아래 표와 같다.

암호화 제외 경로	확장자 및 파일명
Windows, $Windows.~bt, $windows.~ws, windows.old, windows nt, All Users, Public, Boot, Intel, PerfLogs, System Volume Information, MSOCache, $RECYCLE.BIN, Default, Config.Msi, tor browser, microsoft, google, yandex, DropBox	dll, exe, sys, drv, efi, msi, lnk, BlackFL, ntldr, ntuser.dat, bootsect.bak, ntuser.dat.log, autorun.inf, thumbs.db, iconcache.db, bootfont.bin, boot.ini, desktop.ini, ntuser.ini, bootmgr, BOOTNXT, BlackField_ReadMe.txt, LPW5.tmp, MSVC150.dll, LLKFTP.bmp

표 2. 암호화 예외 대상

[7] 뮤텍스(Mutex): 하나의 자원에 여러 스레드 혹은 프로세스가 동시에 접근하지 못하도록 하는 동기화 매커니즘으로, 랜섬웨어에서는 흔히 중복 실행 방지를 위해 사용한다.

[8] WMI(Windows Management Instrumentation): 윈도우 운영체제의 구성 요소, 상태, 동작 정보를 표준화된 방식으로 조회·관리할 수 있도록 하는 관리 인터페이스

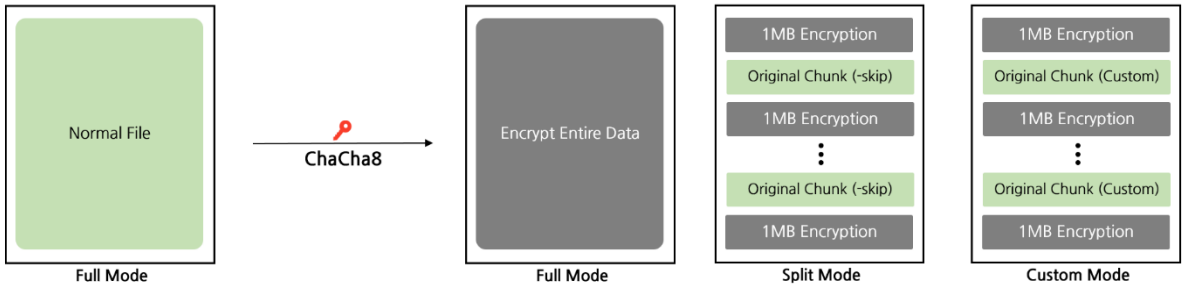


그림 10. BlackField 랜섬웨어 암호화 방식

BlackField 랜섬웨어는 파일 암호화를 수행하기 위해 먼저 키 생성 단계를 진행한다. 난수 생성 함수를 통해 32 바이트 키와 8 바이트 nonce 값을 생성하고, 생성된 32 바이트 키를 기반으로 Curve25519 알고리즘을 이용해 공개키를 만든다. 이후 공격자의 공개키와 연산하여 공유 비밀을 도출하고, 이를 SHA-256 으로 해시해 32 바이트 파생키를 생성한다. 최종적으로 이 파생키를 사용해 ChaCha8 알고리즘으로 파일 암호화를 수행한다.

파일 암호화 방식은 전달받은 -mode 인자에 따라 달라진다. 파일 전체를 암호화하는 full 모드, 일부 구간만 암호화하는 fast 모드, -skip 옵션에 설정된 값만큼 일정 바이트를 주기적으로 건너뛰며 암호화하는 split 모드 그리고 파일 확장자·크기에 따라 암호화 범위가 결정되는 Custom 모드가 존재한다. mode 옵션이 지정되지 않은 경우 기본적으로 Custom 모드가 사용되며, 이 모드에서는 파일 확장자와 크기에 따라 특정 범위만 선택적으로 암호화한다. 각 조건별 암호화 범위는 아래 표와 같다.

파일 크기	암호화 모드	암호화 간격
≤ 16MB	전체 암호화	-
16MB ~ 512MB	부분 암호화	0x40000 (256KB)
512MB ~ 8GB	부분 암호화	0x400000 (4MB)
8GB ~ 128GB	부분 암호화	0x4000000 (64MB)
128GB ~ 2TB	부분 암호화	0x40000000 (1GB)
> 2TB	부분 암호화	0x400000000 (16GB)

표 3. Custom 모드 암호화 범위

파일 크기에 따라 부분 암호화를 수행하는 대상 확장자는 다음과 같다.

암호화 대상 확장자
mdf, ndf, edb, mdb, accdb, db, db2, db3, sql, sqlite, sqlite3, sqlitedb, database, zip, rar, 7z, tar, whim, gz, xld, xls, xlsx, csv, bak, back, backup,

표 4. Custom 모드 적용 대상 확장자

랜섬웨어 대응방안

그림 11. 랜섬웨어 대응방안

BlackField 랜섬웨어는 2025 년 9 월 새롭게 등장했으나, 랜섬노트를 제외한 Cylance 랜섬웨어와 동일한 재활용 코드로 구성되어 있다. 기존에 유출된 소스코드를 기반으로 하거나, 포럼 등에서 코드를 구매해 일부만 변형한 뒤 사용하는 것이다. 이와 같은 사례는 최근 랜섬웨어 생태계에서 매우 흔하게 확인된다. 공개된 랜섬웨어를 재활용한 공격은 보안 솔루션에서 탐지 가능성이 높고 대응 또한 상대적으로 용이하다는 점에서 기술적 위협 수준은 낮아 보일 수 있다. 그러나 최근 공격 경향을 고려했을 때, 공격자는 이미 내부망에 침투해 시스템 구조를 충분히 파악한 후 최종 단계에서 랜섬웨어를 실행하는 경우가 많아 단순한 코드 재사용이라고 해더 위협을 과소평가해서는 안 된다.

또한 BlackField 그룹은 자체 다크웹 데이터 유출 사이트를 운영하지 않으며, 감염 후 텔레그램 채널이나 TOX 를 통해 피해자와 직접 접촉하는 방식을 사용한다. 때문에 실제 피해 사례의 파악이 어렵고, 공격 전술 또한 충분히 공개되지 않았다.

따라서 이미 알려진 변종 기반의 랜섬웨어라 하더라도, EDR 솔루션을 도입하고 최신 보안 패치를 적용하여, 알려진 취약점을 통한 침투나 비정상적인 동작을 신속히 식별·차단할 수 있도록 해야 한다. 이로써 파일 암호화 과정에서 발생하는 행위 기반 패턴을 실시간으로 탐지하고, 악성 프로세스의 실행을 중단시킬 수 있다.

IoCs

Hash(SHA-256)
41c9cd08fff67539525aa413b9199be6e0a4f1a8fc58610a183d77d179d3f282
9f66af5c1e09535d43de5713a3c1d8130e12f8981d1066777f025cf24d963bdc

■ 참고 사이트

• Emsisoft (https://www.emsisoft.com/en/blog/44123/)

• Vulncheck (https://www.vulncheck.com/blog/cve-2025-10035-fortra-go-anywhere-mft)

• Trustwave (https://www.trustwave com/en-us/resources/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand/)

• Cybersecuritynews (https://cybersecuritynews.com/breachforums-back-again)

Special Report

제로트러스트 보안전략 : 데이터 (Data)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

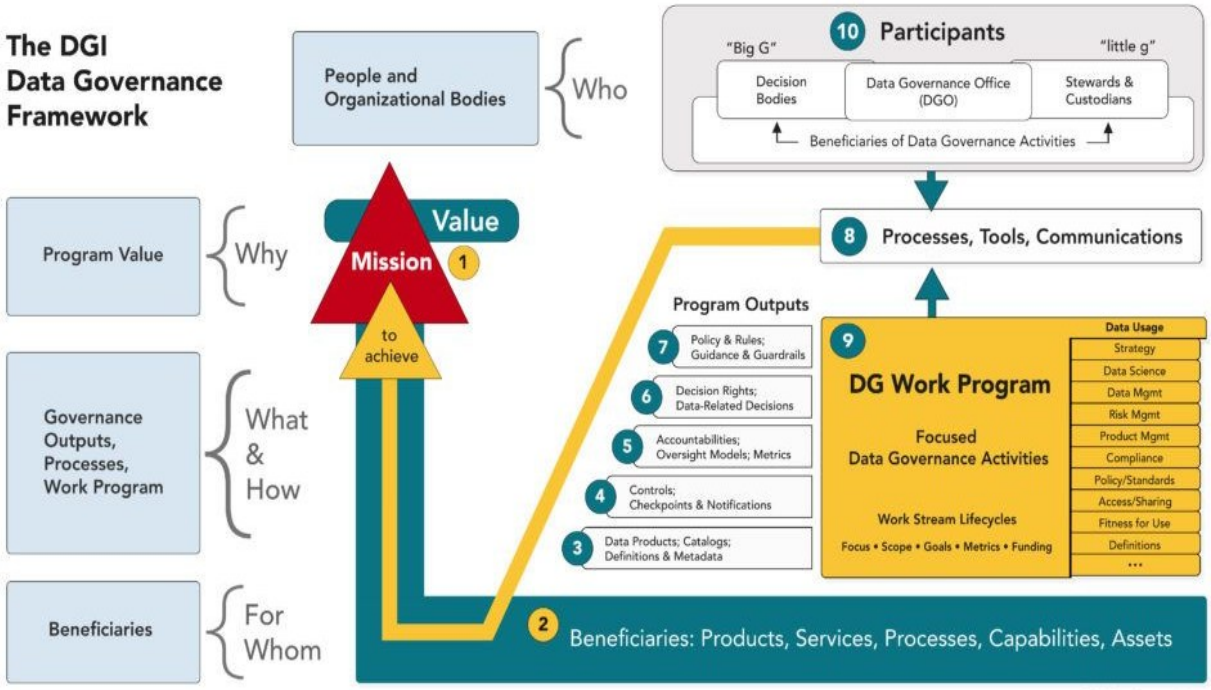
■ 데이터 (Data) 필러 개요

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.

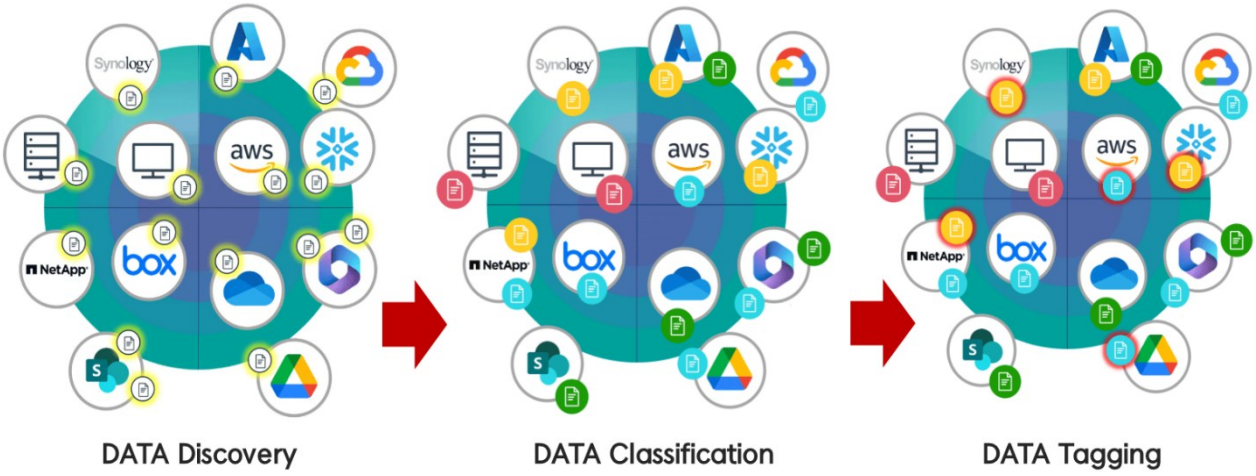
출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

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.

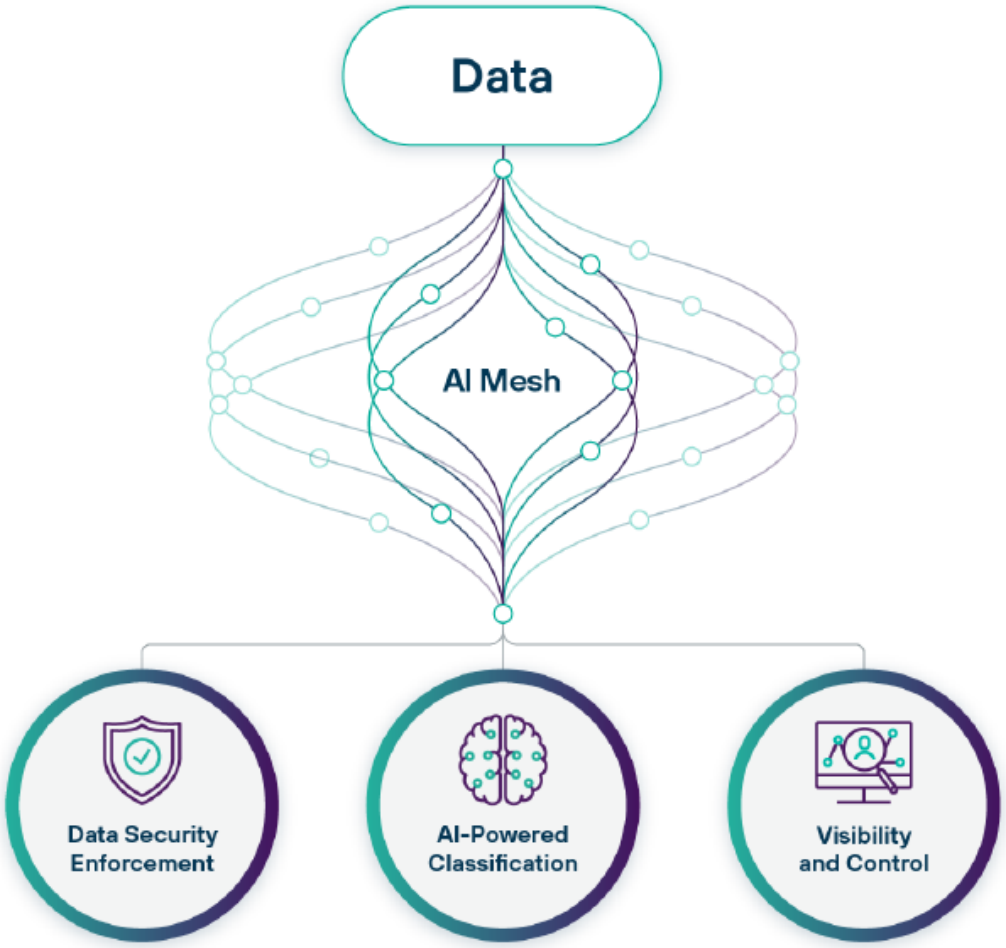
(2) 데이터 식별 (Data Classification)

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"

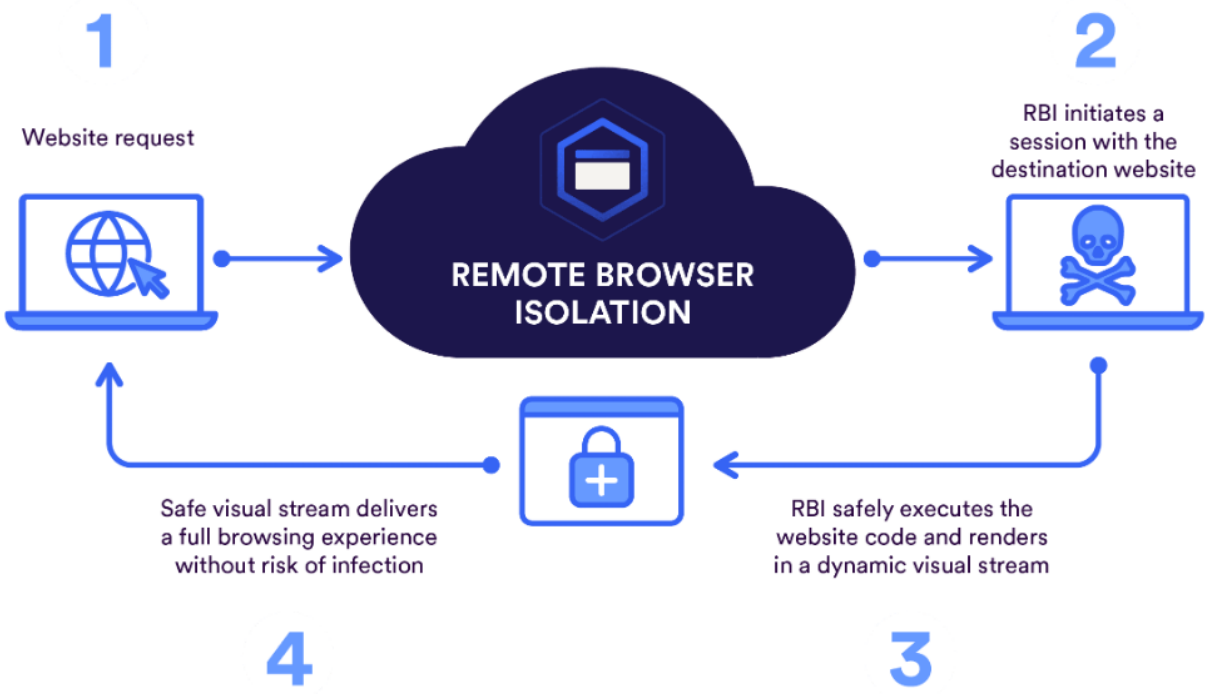
그림 5. AI Mesh For DSPM

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.

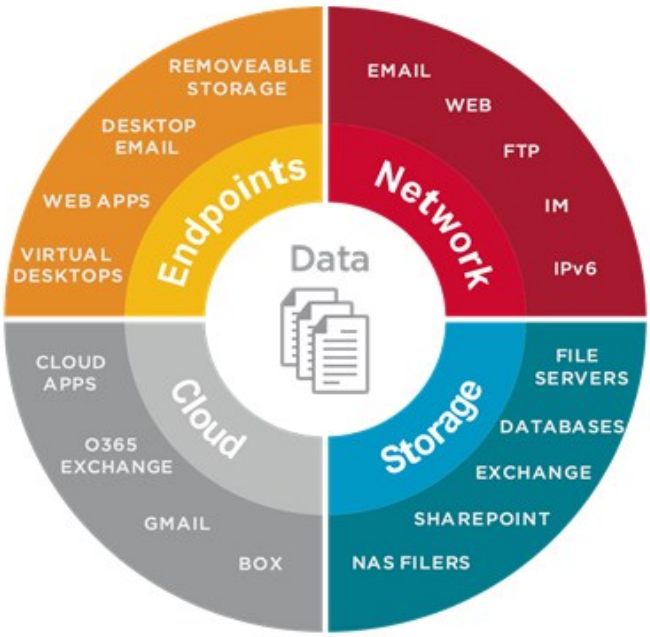
RBI 를 도입하면 일반적으로 기존 브라우저의 직접 사용을 제한하고, 격리된 브라우저를 통해서만 웹 접속이 이루어진다. RBI 는 브라우저 환경에서 발생 가능한 모든 보안 위협에 대한 통합 대응 기능을 제한다.

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”

EQST INSIGHT

2025.11

SK쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹