

솔루션 개요

THALES
Building a future we can all trust

CYBERSECURITY

Thales 데이터 암호화 + 지속적 모니터링

암호화와 관찰성으로
데이터 보호 강화하기

cpl.thalesgroup.com

Thales CipherTrust Data Security Platform (CDSP) 와 Data Security Fabric (DSF) 은 고급 데이터 보호와 실시간 관찰성, 위협 탐지를 결합해 데이터 인프라 전반에 강력한 방어 체계를 만듭니다. 암호화된 데이터베이스는 물론 암호화되지 않은 데이터베이스, 숨겨진 데이터베이스까지 접근 내역을 추적하면서 규제 요구사항도 충족할 수 있습니다. 실제로 데이터 침해의 약 3분의 2는 사람과 관련된 문제에서 발생합니다.

과제: 심각한 보안 공백

데이터베이스의 민감 데이터를 보호하는 방법은 많지만, 보안·성능·가용성이라는 IT 요구사항이 서로 충돌하기도 합니다. 기존 데이터베이스부터 데이터 웨어하우스, 빅데이터 플랫폼, 멀티클라우드 환경까지 복잡하게 얽힌 환경에서 중요 데이터를 보호하고 관리하려면 적절한 균형점을 찾아야 합니다.

암호화나 모니터링 중 하나만으로는 포괄적인 데이터베이스 보호를 입증할 수 없습니다. HIPAA, PCI DSS, SOX, GDPR 같은 규제는 강력한 데이터 보호와 상세한 접근 모니터링을 모두 요구하는데, 기존 방식으로는 위험한 공백이 생깁니다.

많은 기업이 데이터 보안의 첫 걸음으로 암호화 솔루션 배포를 선택했습니다.

반면 데이터베이스 접근을 모니터링하고 무단·의심 활동을 탐지하는 기존 Database Activity Monitoring(DAM) 툴 구축을 먼저 한 조직도 있습니다.

하지만 모니터링 없는 암호화는 복호화 권한이 있는 내부 사용자의 위협이나 정책 위반을 전혀 감지하지 못합니다.

암호화 없는 모니터링은 보안 통제가 우회되면 민감 데이터가 무단 접근에 그대로 노출됩니다.

또한 개별 솔루션들은 운영 복잡도를 높이고, 벤더가 늘어나며, 통합 부담을 가중시키면서도 대규모 성능 문제는 제대로 해결하지 못합니다. 이런 툴들은 숨은 비용을 발생시키고 모든 데이터 자산에 일관된 컴플라이언스 기준을 적용하지 못합니다.

지금 당장 대응해야 하는 이유

- **다중 환경 리스크:** 침해 사고의 40%가 여러 환경에 걸쳐 발생하며, 평균 비용은 517만 달러, 탐지까지 283일 소요
- **새도우 데이터 문제:** 침해의 35%가 관리되지 않는 데이터에서 시작되며, 평균보다 16% 더 많은 비용 발생
- **인적 요소:** 침해의 60%가 사회공학, 실수, 계정 탈취, 내부자 위협 등 사람 관련 요인
- **내부자 위협의 현실:** 정당한 데이터베이스 접근 권한을 가진 사용자도 권한을 남용하거나 계정이 탈취될 수 있어 보안 사각지대 발생
- **디지털 전환:** 클라우드 이전은 완전한 보안 전략 수립의 기회

솔루션: 통합 데이터베이스 보안

데이터베이스 침해는 조직의 핵심 자산인 고객 정보, 재무 데이터, 비즈니스 가치를 만드는 지적자산을 위협합니다. 모든 위협의 중심에는 "데이터"가 있고, 민감 데이터는 비즈니스 크리티컬 애플리케이션, 데이터베이스, 클라우드 저장소에서 사용자·시스템·AI가 접근하는데, 적절한 정책과 통제가 없으면 유출될 수 있습니다.

데이터베이스 암호화를 추가해야 하는 이유

기존 Database Activity Monitoring(DAM)을 쓰는 조직이라면, CipherTrust Database Protection 암호화를 추가해 기존 모니터링을 보완하면서 민감 데이터 보호·모니터링·탐지를 모두 요구하는 규제 공백을 메울 수 있습니다. 기존 투자는 살리면서 컴플라이언스 범위를 강화하는 방법입니다.

CipherTrust Database Protection(CDP)은 성능이 중요한 환경에서 구조화 데이터를 보호하면서도 조인과 분석에 필요한 포맷과 활용성은 그대로 유지합니다. CDP의 고성능 컬럼 단위 암호화는 모든 데이터베이스 쓰기·읽기가 암호화하지 않은 데이터베이스와 거의 같은 속도로 이뤄지게 합니다.

CDP의 강점은 애플리케이션 다운타임이나 재작성 없이 암호화 키를 교체할 수 있다는 점입니다. 데이터 보호 모범 사례에서는 시간이 지나면 암호화 키를 바꿔야 합니다. 키 교체나 데이터 재암호화는 보통 1~2년마다 실행하는데, CDP는 라이브 키 교체 기능이 있는 AES 암호화를 제공해 교체 중단 시간을 없애고 수작업도 필요 없게 만듭니다.

CipherTrust Transparent Encryption(CTE)은 비구조화 데이터를 파일 단위로 암호화해 사용자와 프로세스의 무단 접근을 지속적으로 차단합니다. CTE는 애플리케이션, 인프라, 시스템 관리나 업무 방식을 바꾸지 않고도 모든 활동의 상세한 접근 감사 로그를 만듭니다.

FIPS 140-3 L1 인증을 받은 CipherTrust Transparent Encryption 에이전트는 운영체제의 파일시스템이나 장치 계층에 위치하며, 암호화·복호화가 그 위에서 실행되는 모든 애플리케이션에 투명하게 적용됩니다. 온프레미스든 여러 클라우드든 빅데이터나 컨테이너 환경이든 데이터가 어디 있든 보호합니다.

CipherTrust Database Protection 장점

민감 데이터 규제 대응: PCI DSS, HIPAA, GDPR, CCPA 같은 규정은 저장·전송 중인 민감 데이터 암호화를 명시적으로 요구합니다. 암호화는 데이터 기밀성을 보장하는 확실한 기술 통제 수단입니다.

데이터 노출 리스크 감소: 침해가 발생해도 암호화된 데이터는 키 없이 읽을 수 없어 잠재적 과징금과 피해를 줄입니다.

데이터 무결성 강화: 컴플라이언스 감사자들은 암호화를 민감 정보를 보호하고 리스크 관리 규정 준수를 강화하는 강력한 사전 예방 조치로 봅니다.

컴플라이언스 감사 범위 축소: 데이터를 암호화하면 엄격한 컴플라이언스 통제 대상이 되는 시스템과 환경 수를 줄일 수 있습니다.

가시성과 통제를 추가해야 하는 이유

데이터베이스 암호화를 이미 쓰는 조직이라면, 포괄적 관찰성 플랫폼인 Data Security Fabric(DSF)을 추가해 온프레미스·하이브리드·멀티클라우드 환경 전반에서 실시간 데이터 활동 모니터링, 행동 분석, 이상 탐지, 정책 시행 기능을 확보할 수 있습니다.

기존 데이터 보호 통제가 누가 민감 데이터에 접근할 수 있는지를 정한다면, DSF는 정당한 복호화 권한을 가진 승인 사용자와 애플리케이션이 그 데이터를 실제로 어떻게 쓰는지 보여줍니다.

데이터 보호의 실효성은 암호화 알고리즘 강도, 키 관리 방식, 업계 표준과 규제 준수 여부 등 여러 요소에 달려 있습니다.

DSF로 암호화 운영을 감사하면 암호화 구현이 적절한지 평가하고, 취약점을 찾아내고, 잠재적 보안 공백을 메울 수 있습니다.

보안 관리자는 암호화된 데이터 사용 현황을 완전히 파악할 수 있습니다. 시스템이 승인 사용자가 보호된 데이터를 어떻게 다루는지 관찰하고, 접근 권한이 정당해도 오용을 빠르게 탐지합니다.

담당자는 정책 위반에 즉시 대응하고, 감사 추적과 보고서로 모든 규제 프레임워크의 컴플라이언스 준비 상태를 입증할 수 있습니다.

Data Security Fabric 장점

모든 데이터 접근 현황 파악: Data Security Fabric(DSF)으로 위치와 무관하게 모든 데이터 저장소를 확인하고, 시스템 이벤트·알림·위반·차단된 출처·경고·데이터베이스 감사·파일서버 감사·아카이빙 정보 등을 중앙 통합 대시보드에서 볼 수 있습니다. 지속 모니터링은 애플리케이션 계정과 권한 있는 사용자 계정의 모든 데이터 저장소 활동을 수집·분석해 누가 언제 어떤 데이터에 접근해 무엇을 했는지 보여주는 상세 감사 추적을 제공합니다.

감사 관리 강화: 자동화된 컴플라이언스 보고서는 상세한 접근 추적과 암호화 상태를 포함해 관계형 데이터베이스, NoSQL 데이터베이스, 메인프레임, 빅데이터 플랫폼, 데이터 웨어하우스 등 다양한 온프레미스 플랫폼의 감사를 통합합니다. Azure SQL, Amazon Relational Database Services(RDS) 같은 PaaS 서비스를 포함해 Microsoft Azure와 Amazon Web Services(AWS)에 호스팅된 데이터베이스도 지원합니다. 상세한 데이터 활동이 자동으로 수집되어 감사 요청 대응이 훨씬 쉬워집니다.

모든 곳에서 컴플라이언스 확장: GDPR, PCI, NYDFS, HIPAA, CPRA 같은 규정에 대한 통합 정책 모니터링, 시행 워크플로, 보고서로 규제 준수 활동을 간소화합니다. 감사 대상 모든 데이터 자산의 정보를 통합하고 완전히 색인화해 효율적으로 저장하며, 수년치 정보에 실시간으로 접근할 수 있어 사고 조사나 감사 문의 대응 시간이 크게 줄어듭니다.

데이터베이스 보호 + 데이터 가시성·통제

단일 벤더에서 데이터베이스 보호와 모니터링을 함께 구현하면 운영 복잡도는 낮추면서 우수한 보안 성과를 내고 포괄적인 규제 준수를 입증할 수 있습니다.

데이터 가시성·통제 기능을 갖춘 데이터베이스 보호는 강력한 암호화·키 관리와 세밀한 접근 모니터링·행동 분석을 결합한 시너지 접근법으로, 엔드투엔드 데이터 보안과 거버넌스를 제공합니다. 더 강력한 보호, 더 나은 컴플라이언스, 운영 효율성을 동시에 달성할 수 있습니다.

보안 공백 해소: 비교 불가 커버리지

CipherTrust Data Security Platform(CDSP)은 데이터베이스 암호화, 중앙 집중식 키 관리, 토큰화, 데이터 마스킹으로 강력한 데이터 검색·통제·보호 기능을 제공합니다. 이 기능들이 함께 보안 공백을 메우고 운영을 단순화합니다.

DSF(Data Security Fabric)는 실시간 데이터 활동 모니터링, 위협 탐지, 사용자 행동 분석, 컴플라이언스 보고 등 포괄적인 데이터 모니터링 기능을 제공합니다. 데이터베이스 접근 패턴과 정책 위반을 지속적으로 파악할 수 있습니다.

CipherTrust Data Security Platform (CDSP)	Data Security Fabric (DSF)
<ul style="list-style-type: none"> 저장 데이터 보호: 온프레미스, 클라우드, 백업에 저장된 데이터 보호 	<ul style="list-style-type: none"> 포괄적인 데이터 활동 모니터링: 모든 데이터 저장소와 데이터 유형의 완전한 가시성 확보
<ul style="list-style-type: none"> 투명한 암호화: 애플리케이션이나 워크플로 변경 없이 데이터 암호화 	<ul style="list-style-type: none"> 민감 데이터 실시간 분석: 모든 데이터 저장소에서 비준수·위험·악의적 데이터 접근을 탐지하고 보고
<ul style="list-style-type: none"> 중앙 집중식 키 관리: 암호화 키를 안전하게 생성·저장·관리 	<ul style="list-style-type: none"> 자동화된 데이터 분류·검색: 거버넌스되지 않은 데이터를 찾아내고, 모든 데이터를 분류하며, 취약점 평가
<ul style="list-style-type: none"> 토큰화: 민감 데이터를 비민감 토큰으로 바꿔 무단 접근과 오용을 어렵게 함 	<ul style="list-style-type: none"> 엔터프라이즈 규모 리스크 우선순위 지정: 핵심 데이터 리스크 지표를 통합 뷰로 확인해 리스크 프로필을 파악하고 공백 완화
<ul style="list-style-type: none"> 동적 데이터 마스킹: 민감 데이터를 실시간으로 마스킹·삭제해 사용 중에도 무단 접근 차단 	<ul style="list-style-type: none"> AI/ML 기반 행동 이상·위협 탐지: 비정상적인 사용자 행동을 식별하고 복잡한 기술 이벤트를 IT 운영팀과 보안 담당자가 즉시 조치할 수 있는 쉬운 용어로 전환

CipherTrust Data Security Platform 장점

벤더 통합으로 비용 절감: 조달, 계약 관리, 교육 부담을 줄이고 기존 인프라와 전문성을 활용하는 빠른 데이터 보호 경로 확보합니다.

리스크 감소: 외부 공격과 내부자 위협을 모두 다루는 다층 방어로 잠재적 침해 비용을 낮추고, 방지한 사고 비용과 운영 효율성 개선으로 측정 가능한 ROI를 창출합니다.

전방위 컴플라이언스 커버리지: 모든 주요 규정이 데이터 보호와 접근 모니터링을 함께 요구해 두 기능이 자연스럽게 시너지를 냅니다.

<p>HIPAA</p> <p>PHI 암호화 + 접근 감사 추적</p>	<p>PCI DSS</p> <p>카드 소비자 데이터 보호 + 사용자 접근 로깅</p>
<p>SOX, GLBA, DORA</p> <p>금융 데이터 통제 + 접근 모니터링</p>	<p>GDPR, CCPA</p> <p>개인 데이터 암호화 + 처리 기록</p>
<p>FISMA</p> <p>연방 보안 표준 + 감사 기능</p>	<p>NERC CIP, NIS2</p> <p>핵심 인프라 데이터 보호 + 접근 추적</p>

Thales의 강점: 비교 불가 혁신과 전문성

예방 + 탐지 통제: 암호화는 무단 접근을 막고 모니터링은 오용을 탐지

감사 대응력: 상세한 접근 추적과 암호화 상태를 담은 자동화 컴플라이언스 보고

운영 효율성: 통합 접근법으로 벤더 확산과 통합 부담 감소

신속 대응: 중앙 집중식 정책 관리로 몇 분 만에 보안 공백 해소

입증된 비즈니스 성과

단일 벤더 전략으로 첫날부터 포괄적인 데이터베이스 보안을 배포할 수 있어 운영 복잡도는 낮추면서 일관된 정책과 간소화된 운영으로 데이터 계층 보안을 제공합니다.

데이터베이스 암호화는 확실한 ROI를 냅니다. Forrester의 Total Economic Impact 연구에서 3년간 221% 투자 수익률과 910만 달러 정량화 효과를 확인했습니다. 구축 후 6개월 이내에 투자를 회수하고, 자동화와 중앙 집중화로 키 관리 업무를 70% 줄입니다.

업계 평가

KuppingerCole이 탈레스를 2025년 Data Security Platforms 부문 "Overall Leader"로 선정했고, Forrester는 평가 대상 벤더 중 두 번째로 높은 전략 점수를 받은 "Strong Performer"로 평가했습니다. Gartner Peer Insights는 Imperva를 190개 이상 고객 리뷰에서 4.5점으로 평가했으며, 여러 FIPS 140-2 Level 3 인증이 엔터프라이즈 보안 아키텍처를 검증합니다.

보안 전문가 상담

데이터베이스 보안 공백을 해결할 준비가 되셨나요? 지금 Thales 담당자에게 연락하여 [CipherTrust Database Encryption](#) 솔루션과 [Data Security Fabric](#) 플랫폼이 어떻게 협력해 포괄적인 데이터 보호, 빠른 컴플라이언스 대응, 측정 가능한 비즈니스 가치를 제공하는지 알아보십시오.

탈레스 소개

탈레스는 글로벌 사이버보안 리더로서 기업, 정부, 세계에서 가장 신뢰받는 조직들이 최고의 ROI로 어디서나 대규모로 핵심 애플리케이션, 민감 데이터, 신원, 소프트웨어를 보호하도록 돕습니다. Fortune Global 500대 기업의 58%를 포함해 30,000개 이상 고객을 보유하고 있으며, 솔루션은 전 세계 148개국에 배포되어 있습니다. 혁신적인 서비스와 통합 플랫폼으로 탈레스는 고객이 리스크를 더 잘 파악하고, 사이버 위협으로부터 방어하며, 컴플라이언스 공백을 메우고, 매일 수십억 사용자에게 신뢰할 수 있는 디지털 경험을 제공하도록 지원합니다.