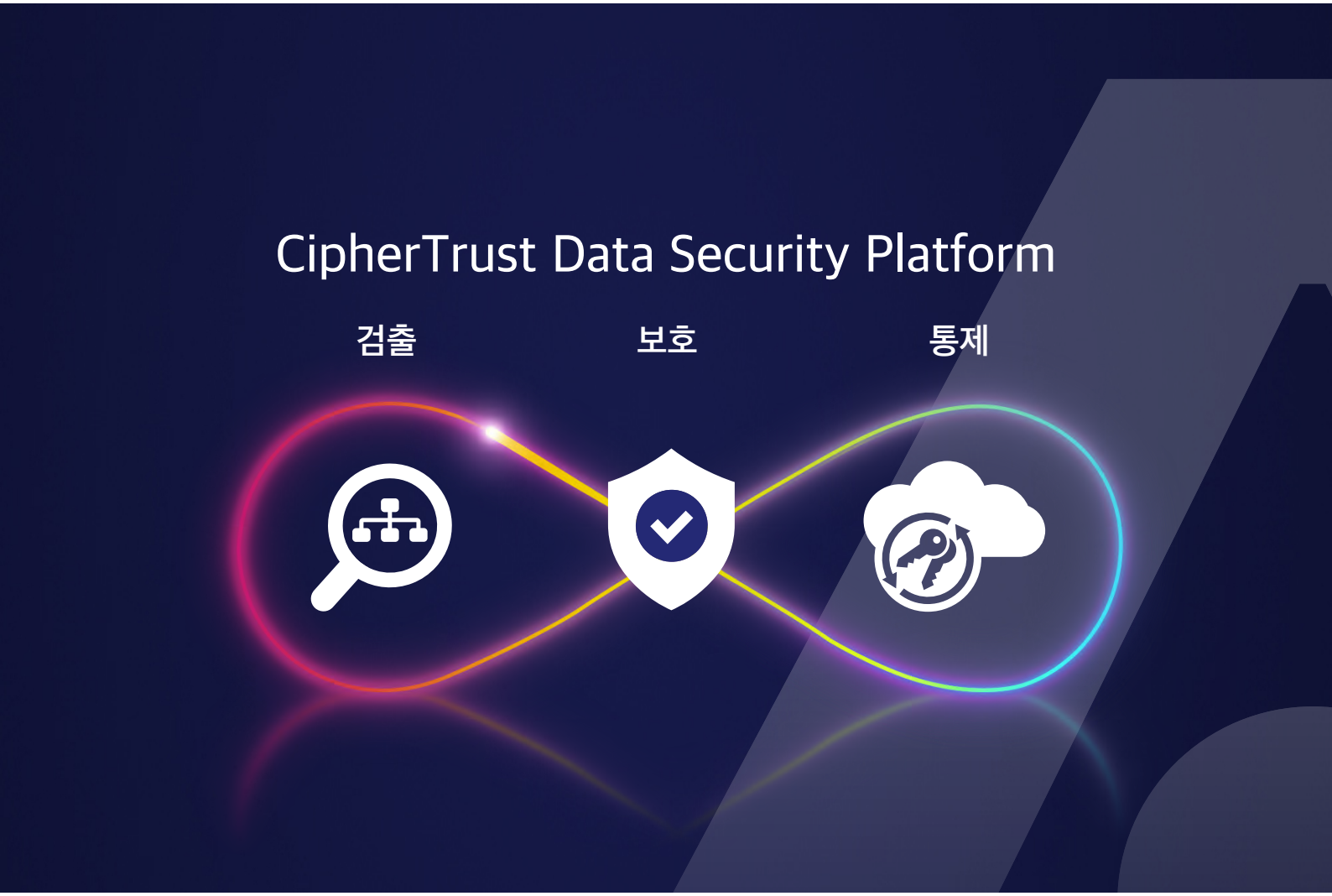
cpl.thalesgroup.com

THALES

모든 조직의 민감 데이터 보호를 위한 핵심 요소



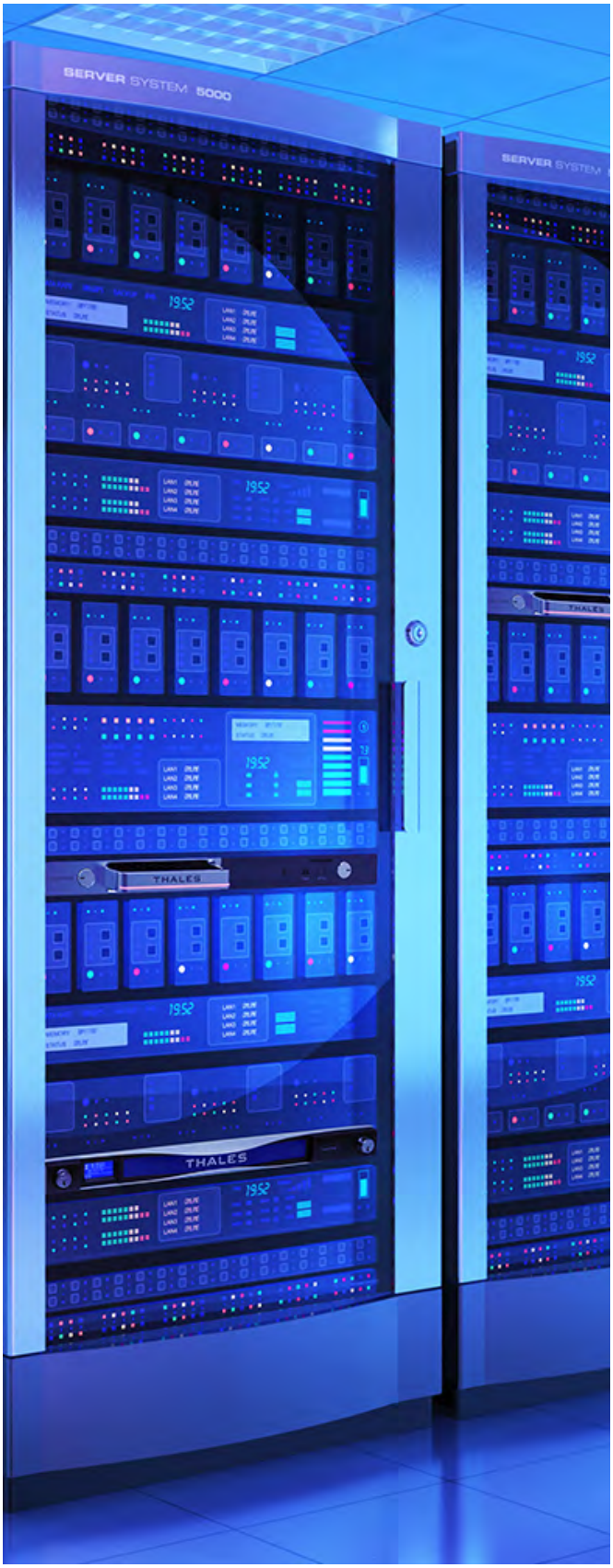
백서

목차

개요

전통적으로 조직은 주로 경계 방어에 IT 보안을 집중했기 때문에 벽을 세워 외부 위협이 네트워크에 진입하는 것을 차단했습니다. 경계 방어는 여전히 중요하지만 충분하지는 않습니다. 사이버 범죄는 주기적으로 경계 방어를 뚫고 있으며 데이터는 클라우드 방어 경계 외부 어딘가에 있는 경우가 많으므로, 조직은 데이터가 어디에 있든 데이터를 보호하는 데이터 중심 보안 전략을 적용해야 합니다. 오늘날 급증하는데이터, 진화하는 글로벌 및 지역 개인정보 보호 규제, 클라우드 채택의 증가, 지속적인 지능형 위협으로 인해 조직은 데이터 중심 보안을 활용해 위치에 관계없이데이터를 통제하게 된 동시에 데이터를 절도한 범죄자가 읽을 수 없게 만들 수 있게 되었습니다. 그러나 효과적인 보안은 사용자 개입 없이 자동으로 동작해야 합니다.

이 백서에서는 급증하는 데이터 시대의 데이터 보안 문제에 대해 간략하게 설명합니다. 또한, 중요한 데이터를 검색 및 분류하고 여기에 데이터 중심 보안을 적용하는 전략을 제공합니다.



데이터 급증, 규제 증가, 발전하는 사이버 범죄

많은 레거시 데이터 보안 아키텍처는 데이터가 데이터 센터에 상주하고 온프레미스에서 사용된다는 가정하에 구축되었습니다. 전통적인 IT 환경은 끝에서 끝까지 IT에서 제어하는 환경이었습니다. IT는 인프라, 보안 및 애플리케이션을 소유하고 운영했으며 결과적으로 데이터와 사용자 모두에 대한 막대한 가시성과 통제력을 가졌습니다. 데이터 및 애플리케이션에 대한 모든 액세스는 방화벽 또는 차세대 방화벽, VPN, 안티 바이러스, 침입 방지 시스템 등과 같은 경계 보안 계층을 거쳐갔습니다.

보안을 경계 너머까지 확장하여 중요한 데이터 보호

레거시 데이터 보안 아키텍처

신뢰가 없는 영역

신뢰 경계에 기반한 보안

데이터 중심 보안 아키텍처

보안은 어디서나 데이터를 보호합니다

그러나 현대 조직에서는 이러한 검문 포인트가 더 이상 존재하지 않습니다. 데이터 센터 주변의 경계가 아무리 강력하더라도, 제공되는 보안은 개념적일 뿐입니다. 그 이유는 다음과 같습니다.

1. 데이터 이동과 급증에 따라 확장할 수 없는 경계 보안

클라우드 서비스, 빅 데이터 환경 및 IoT 기술이 널리 채택됨에 따라 조직은 막대한 양의 데이터를 매우 빠르게, 종종 타사 인프라나 파트너사로 움직이고 있습니다. 이는 다음과 같이 많은 과제를 제시합니다.

- 정형, 반정형, 비정형 데이터를 포함한 다양한 데이터 형식
- SLA(서비스 수준 계약)를 위반하는 대기 시간 및 성능적인 병목 현상을 가중하는 경계 보안 관문 때문에 사용자가 종종 클라우드 서비스에 직접 액세스하게 되는 현상
- 모든 곳에 존재하는 내부자: 더 이상 직원은 경계 내에 있는 내부자가 아닙니다. 귀사의 데이터는 이제 계약자, 서비스 제공업체, 기타 제삼자의 손안에 있습니다. 이러한 '내부자'는 귀사가 심사하지 않았고모니터링할 수 없으며 통제할 수 없는 개인입니다.

2. 운영 복잡성 및 규정

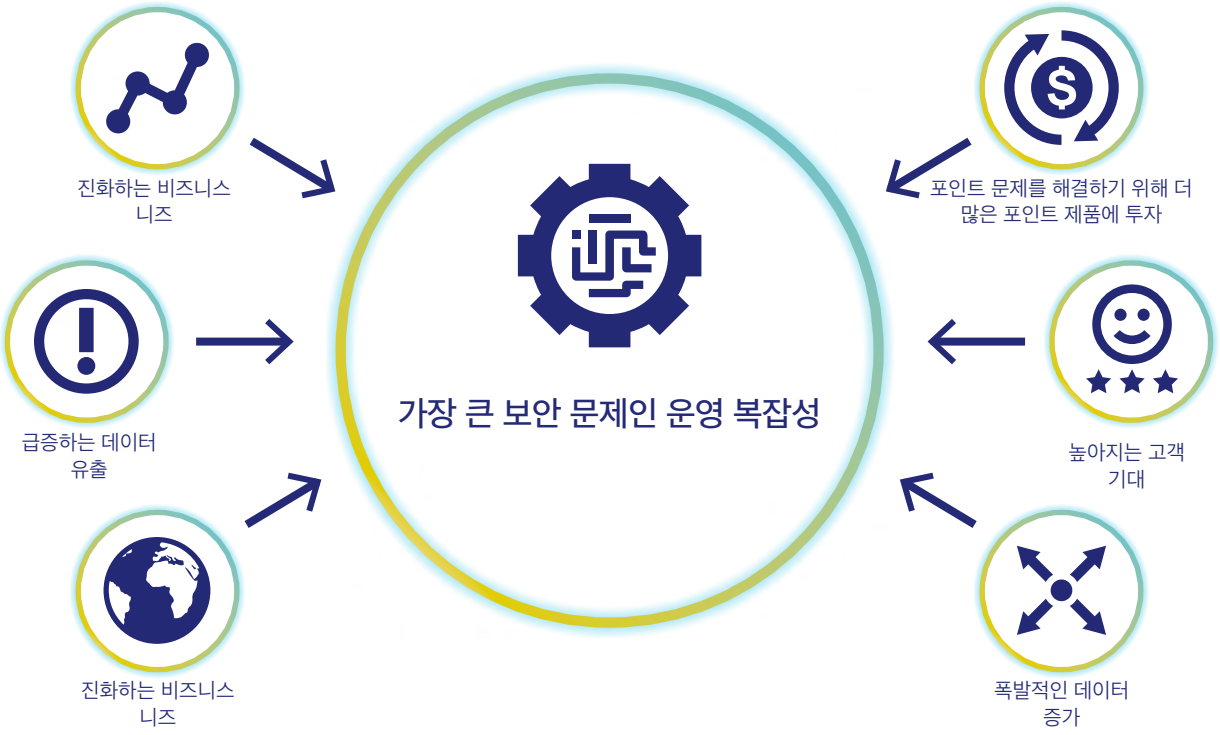
클라우드, 컨테이너, 빅 데이터 기술 및 여러 공급업체의 서로 다른 도구로 데이터를 움직이면 복잡성이 가중됩니다. 보안 경계가 점점 희미해짐에 따라, 조직은 분산된 IT 리소스에 대한 일관된 통합 정책을 제공, 구현 및 관리해야 합니다. 모든 조직에는 기존 플랫폼과 새로운 플랫폼이 혼합되어 있습니다.

규제 준수 요건이 서로 다른 글로벌 및 지역별 개인정보 보호 규제가 증가함에 따라 폭발적인 데이터 증가 상황이 더욱 복잡해집니다. 효과적인 규제 준수를 위해, 조직은 더 이상 데이터 보안을 사일로·레거시 접근 방식에만 의존할 수 없게 되었습니다.

이 모든 것이 점점 더 복잡해지는 오늘날의 데이터 환경에 더해집니다. 따라서 조직이 운영 복잡성을 데이터 보안 배포의 가장 큰 장벽으로 인식하는 것은 놀라운 일이 아닙니다. CISO(최고 정보보안 책임자) 및 CDO(최고 데이터 책임자)는 저장 또는 사용 위치에 관계없이 민감 데이터를 강력하게 보호하는 포괄적이고 통합된 데이터 보안 솔루션의 필요성을 점점 더 크게 인식하고 있습니다.

레거시 데이터 보안 아키텍처는 현대 데이터 중심 환경의 다양한 특성에 대응하지 못하기 때문에 점점 더 집요해지는 공격자로 인한 정교한 데이터 유출로부터 조직을 보호할 수 없습니다. 오늘날의 CISO와 CDO가 조치와 대응 조치를 이용해 반응하는 반복 주기를 끊으려면 완전히 새로운 보안 접근 방식을 취해야 합니다.

데이터 보안 배포의 가장 높은 장벽, 운영 복잡성



조직의 민감 데이터를 보호하기 위한 3요소 전략

레거시 보안 아키텍처는 조직이 데이터와 상호 작용하는 방식에 대한 오래된 관점을 반영하기 때문에 자주 심각한 실패를 일으켰습니다. 오늘날의 데이터 보안을 위해서는 조직의 가장 가치있는 자산이 데이터이며 이 자산이 기하급수적으로 증가하고 있음을 인식하는 것이 필요합니다.

데이터 중심 보안은 데이터가 이동하는 엔드포인트나 네트워크, 애플리케이션이 아닌 데이터 자체를 보호합니다. 결과적으로는 데이터 자체가 안전하기 때문에 증가된 위험 없이 조직이 필요로 하는 만큼 데이터를 움직일 수 있습니다. 진보 속도를 늦추고 데이터 급증을 억제하는 대신, 조직은 데이터 저장 위치나 사용 위치와 관계없이 데이터 중심 보안을 통해 데이터를 최대한 활용할 수 있습니다.

아래 차트는 데이터 중심 보안의 세 가지 핵심 요소를 보여줍니다.

데이터 보안의 세 가지 핵심 요소

#1
민감 데이터의 검출 및 분류
- 민감 데이터의 효과적인 검출 및 분류
- 데이터와 데이터 리스크에 대한 명확한 이해

#2
민감 데이터의 보호
- 암호화, 액세스 제어 및 토큰화를 통한 민감 데이터의 보호
- 도난이나 유출시 데이터를 읽을 수 없고 쓸모 없게 만드는 작업

#3
암호키의 통제
- 중앙 집중식 키 관리
- 키 수명주기 관리
- 통합 키 관리 및 암호화 정책

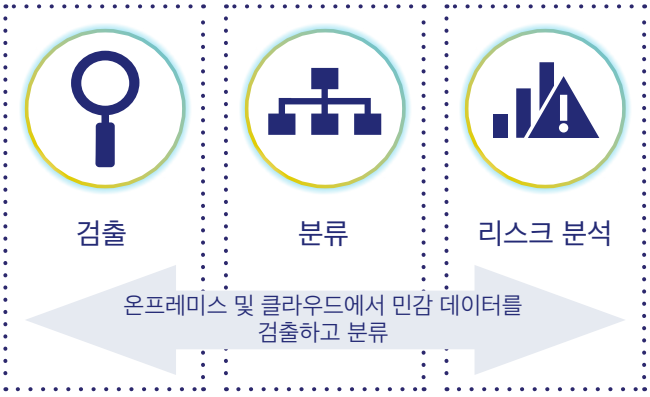
데이터 중심 보안 접근 방식은 조직의 DNA여야 합니다. 이 전체론적 접근 방식은 데이터 보안 및 보호의 최전선에서 수백 명의 엔터프라이즈 CISO, CDO, CIO 및 설계자와 협력한 탈레스의 경험과 수많은 규정, 업계 표준에서 요구하는 모범 사례를 기반으로 합니다. 데이터 보안에 이 접근 방식을 채택하려면 조직은 다음과 같은 작업을 수행해야 합니다.

1. 민감 데이터의 검출 및 분류

민감 데이터는 기업과 클라우드, 그 너머에까지 퍼져 있습니다. 일반적으로 IT 보안은 데이터가 저장되는 위치와 액세스 권한이 있는 사람에 관해 제한적인 가시성을 가지고 있습니다. 분산 데이터가 내포한 위험은 데이터 유출에서 규제 준수 위반에 이르기까지 다양합니다. 온프레미스 데이터 센터에서 가장 민감한 데이터 자산이 있는 위치를 식별하는 것으로 시작해, 클라우드와 호스팅 서비스와 같은 확장 환경으로 이동하십시오. 또, 스토리지 및 파일 서버, 애플리케이션, 데이터베이스 및 가상 기계를 검색하는 것으로 시작하십시오. 데이터 저장 위치와 상관없이 전사적으로 데이터를 찾아낸 뒤, 내부 정책과 외부 규정에 따라 민감도와 중요성을 분류합니다.

민감 데이터를 검출, 식별 및 분류하는 것은 이 프로세스의 중요한 첫 번째 단계이지만 반복할 수 있어야 하고 기술이나 지역에 구애받지 않아야 합니다. 오늘날의 데이터 검출 및 분류 솔루션은 보유하고 있는 민감 데이터의 종류, 위치 및 위험도 점수를 명확하게 이해할 수 있도록 시각화된 대시보드와 깊이 있는 검출 방법을 제공합니다. 위험도 점수는 보호 수준, 발견된 구성 요소의 수, 위치, 민감 데이터의 양 등과 같은 다양한 매개 변수를 집계하고 조직이 파일 및 데이터베이스와 같은 데이터 개체의 민감도를 식별할 수 있도록 해줍니다. 이후 비즈니스는 문제 해결의 우선 순위를 정하거나 타사 데이터 공유 또는 클라우드 마이그레이션에 대해 더 많은 정보에 기반해 결정을 내리는 등의 방식으로 데이터를 보호하고 리스크를 완화할 수 있습니다.

효과적인 데이터 보안의 첫 단계, 데이터 검출 및 분류



2. 민감 데이터 보호

민감 데이터 자체를 보호하는 이상적인 방법은 조직 전반적으로 기본 암호화 전략을 설정하여 데이터 누출과 유출 사고 공개 위험을 완화하는 것입니다.

데이터를 검색하고 분류하면, 데이터 세트별로 비즈니스에 더할 수 있는 리스크를 파악할 수 있고 액세스 컨트롤과 난독화 보안 메커니즘을 구현하는 방법과 위치 예: 세분화된 액세스 제어를 통한 파일 수준 암호화 및 동적 데이터 마스킹을 통한 토큰화에 우선 순위를 정할 수 있습니다. 즉, 권한이 없는 사용자가 액세스하기 어렵게 만들고 도난 또는 유출시 데이터를 읽을 수 없고 쓸모 없게 만들어 데이터를 보호하는 것입니다.

현재 암호화는 조직에서 가장 널리 이용하는 효과적인 데이터 보안 방법 중 하나입니다. 데이터 암호화는 데이터를 다른 형식인 암호 데이터로 변환하므로 권한이 있는 사용자만 평문 데이터에 액세스할 수 있습니다. 특정 알고리즘을 사용하여 데이터를 변환하는 것이 암호화라면, 토큰화는 민감 데이터를 민감하지 않은 데이터로 대체함으로써 보호합니다. 토큰화는 인식할 수 없는 토큰화 데이터 형식을 생성하는데, 이는 소스 데이터의 형식을 유지합니다. 토큰화된 데이터는 원본 데이터와 동일한 크기 및 형식으로 저장할 수도 있습니다. 따라서 토큰화된 데이터를 저장하기 위해 데이터베이스 스키마나 프로세스를 변경할 필요가 없습니다.저장되는 데이터 유형에 이러한 종류의 구조가 없는 경우(예: 텍스트 파일, PDF, MP3 등)라면, 토큰화는 적절한 난독화 형식이 아닙니다. 대신 파일 시스템 수준의 암호화가 적합합니다. 이 암호화 방식은 원래의 데이터 블록을 암호화된 데이터 버전으로 변경합니다.

기업 요건에 가장 적합한 데이터 암호화 솔루션 유형을 결정할 때 몇 가지 고려할 사항이 있습니다. 이해하기 쉽게 표현하자면, 데이터 암호화 유형은 기술 스택 내에서의 이용 위치에 따라 구분할 수 있습니다. 데이터 암호화를 일반적으로 이용하는 기술 스택에는 디스크, 파일 시스템, 데이터베이스 및 애플리케이션이라는 네 가지 스택 수준이 있습니다. 일반적으로 암호화를 이용하는 스택 수준이 낮을수록 더욱 간단하고 침해 정도가 적은 구현을 실행할 수 있습니다. 그러나 이러한 데이터 암호화 방식으로 해결할 수 있는 위협의 수와 유형도 줄어듭니다. 반면에 더 높은 스택 수준에서 암호화를 사용하면 일반적으로 더 높은 수준의 보안을 실현하고 더 많은 리스크를 완화할 수 있습니다.

스택 상위 수준에 구현하면 보안 수준이 높아지지만 개발 복잡성도 증가함

3. 암호키의 통제

암호화 프로세스의 보안은 데이터를 암호화하는 데 사용되는 암호키의 보안에 따라 달라집니다. 데이터를 암호화·토큰화하는 데 사용하는 키가 암호화·토큰화된 데이터와 함께 도난당하면 데이터를 해독하고 일반 텍스트로 읽는 것이 가능하므로 안전하지 않습니다. 중요한 데이터를 암호화 및 토큰화를 통해 성공적으로 보호하려면 암호키 자체를 타사나 클라우드 제공업체가 아닌 귀사에서 직접 보호, 관리하고 제어해야 합니다.

점점 더 많은 사일로 암호화 솔루션을 배포하면서 조직들은 일관성 없는 정책, 각기 다양한 수준의 보호, 비용 증가의 문제를 겪고 있습니다. 이 미로를 통과하는 가장 간단한 경로는 중앙 집중식 키 관리 모델로 전환하는 것입니다. 암호키 관리에는 암호키의 전체 수명주기를 관리하고 손실이나 오용으로부터 보호하는 것이 포함됩니다. 키에는 수명주기가 있습니다. 생성되고 유용하게 이용되다가 폐기됩니다. 키 수명주기 관리에는 키 생성, 사용, 저장, 배포, 보관 및 삭제가 포함됩니다. 중앙 집중식 키 관리의 이점은 다음과 같습니다.

- 통합 키 관리 및 암호화 정책
- 시스템 전반적인 키 폐기
- 사용자 및 관리 권한 설정시 인적 오류 위험 감소
- 높은 가용성 및 확장성
- 안전한 FIPS 140-2 인증
- 자동화로 비용 절감
- 통합된 감사 정보
- 단순화된 백업 및 복구
- 포괄적인 직무 분리로 보안 강화

중앙에서 암호키 관리

효과적인 데이터 중심 보안의 이점

효과적인 데이터 중심 보안 솔루션을 사용하면 데이터 급증과 글로벌 및 지역 개인정보 보호 규제의 출현으로 인해 발생하는 보안 문제를 해결하고 더 안전한 미래를 준비할 수 있습니다.

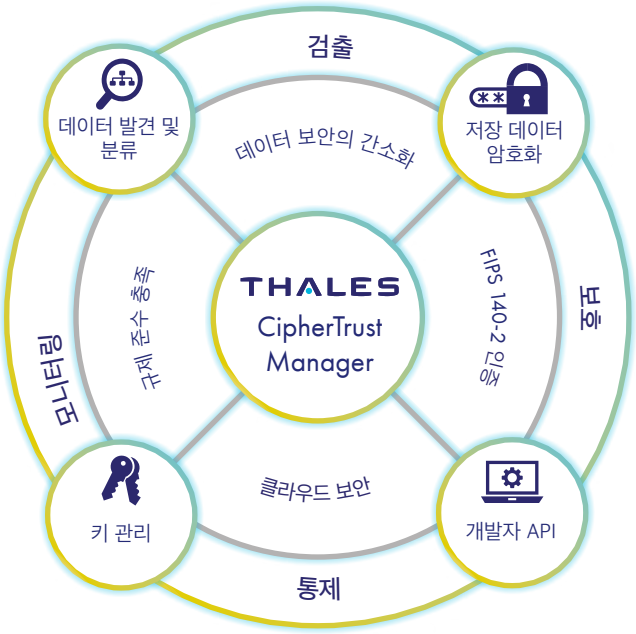
올바르게 구축된 데이터 중심 보안 솔루션:

- 조직이 위험을 완화하고 비용을 절감하도록 지원합니다. 조직은 기존 보안 인프라를 글로벌 규모로 운영하고, 노동 집약적이고 반복적이며 오류가 발생하기 쉬운 수동 작업 프로세스를 줄이고 새로운 기술을 활성화하며 미래에도 사용할 수 있는 투자로 비용을 절감할 수 있습니다.
- 모든 데이터 자산에 대해 지속적으로 포괄적인 시각을 제공하고 보안 정책과 제어의 거버넌스를 용이하게 합니다.
- 조직이 데이터와 데이터의 리스크를 이해하고 해결 우선 순위를 지정할 수 있도록 지원합니다.
- 데이터를 보호하므로 보호 프로파일을 유지하면서 여러 온프레미스 및 클라우드 환경에서 안전하게 이동할 수 있습니다.
- 민감한 정보를 훔치려는 악의적인 사용자 및 지능형 지속 공격(APTs)으로부터 데이터를 보호합니다.
- 벌금을 줄이고 조직이 정부, 기관 및 산업 규정을 준수하도록 지원합니다. 조직은 자동화된 보고서를 작성하고 보안 절차를 감사하면서 위반을 모니터링하고 보안 정책 및 규칙을 시행할 수 있습니다.
- 데이터 유출이나 감사 문제에 대응하여 방어 가능한 법적 위치를 확보합니다.

탈레스가 3요소 보안 전략 구현을 지원하는 방법

탈레스는 데이터 보호 부문의 세계적인 선도 기업입니다. 당사는 데이터 검출 및 분류, 암호화, 고급 키 관리, 토큰화, 인증 및 접근 관리를 통해 기업이 데이터와 신원, 지적재산을 보호하고 이를 관리하는 데 필요한 모든 것을 제공합니다.탈레스의 CipherTrust Data Security Platform은 중앙 집중식 키 관리 방식을 이용하여 데이터 검출과 분류, 데이터 보호, 전례 없는 수준의 접근 통제 세분화를 단일 플랫폼에서 처리합니다. 그 결과, 데이터 보안 작업에 필요한 자원을 감축할 수 있고 어디서나 규제 준수를 통제할 수 있으며 비즈니스 전반에서 위험 부담을 크게 경감할 수 있습니다.

CipherTrust Data Security Platform



CipherTrust Data Security Platform

- 데이터 검출 및 분류
  - 데이터 시각화를 통한 리스크 분석
- 데이터 보호 기술
  - 파일, 데이터베이스, 빅 데이터, 컨테이너에 투명한 암호화 적용
  - 애플리케이션 데이터 보호
  - 동적 데이터 마스킹 이용 토큰화
  - 형식 보존 암호화(FPE)
  - 정적 데이터 마스킹
  - 관리자 액세스 컨트롤
- 중앙 집중식 키 관리
  - FIPS 140-2 준수
  - 멀티 클라우드 키 관리
  - KMIP 통합을 위한 최고의 파트너 생태계
  - 데이터베이스 암호화 키 관리(Oracle TDE, 빅 데이터, MS SQL, 상시 암호화되는 SQL 서버 등)
- 모니터링 및 리포팅
- 중앙 집중형 관리 콘솔

CipherTrust Data Security Platform의 이점

데이터 보안의 간소화

차세대 통합 데이터 보안 기능으로 어디서나 민감 데이터를 검출 및 보호하고 통제합니다.CipherTrust Data Security Platform은 민감한 데이터를 검색 및 분류하고 외부 위협에 대처하며 내부자 남용을 방지할 뿐만 아니라 데이터가 클라우드나 외부 공급업체의인프라에 저장되어 있는 경우에도 지속적인 제어를 구현하는 강력한 도구를 조직에 제공하는 '단일 창' 중앙 집중식 관리 콘솔로 데이터 보안 관리를 간소화합니다. 조직은 디지털 혁신을 구현하기 전에 프라이버시 격차를 쉽게 발견·해결하고 보호 우선 순위를 지정하며 정보에 입각하여 프라이버시 및 보안 의무에 대한 의사 결정을 내릴 수 있습니다.

규제 준수 시간 단축

규제 기관과 감사자는 규제 받는 민감 데이터를 통제하고 이를 증명할 보고 자료를 보유할 것을 조직에 요구합니다. 데이터 검출 및 분류, 암호화, 액세스 제어, 감사 로그, 토큰화 및 키 관리와 같은 CipherTrust Data Security Platform 기능은 어디에서나 데이터 보안과 개인정보 보호 조건을 지원합니다. 이러한 통제 기능은 새로운 배포 솔루션이나 변화하는 규제 준수 조건에 맞춰 빠르게 추가할 수 있습니다.이 플랫폼의 중앙 집중식 특성과 확장성을 통해 새로운 데이터 보호 요건에 대응하여 필요한 커넥터의 스크립트를 배포하고 라이선스를 추가함으로써 새로운 통제 기능을 신속하게 더할 수 있습니다.

안전한 클라우드 마이그레이션

CipherTrust Data Security Platform은 조직이 민감 데이터를 클라우드에 안전하게 저장할 수 있도록 고급 암호화 및 중앙 집중식 키 관리 솔루션을 제공합니다. 이 플랫폼은 고급 멀티 클라우드 BYOE(Bring Your Own Encryption) 솔루션을 제공하여 클라우드 벤더 암호화 의존성 문제를 방지하고 중앙 집중식, 독립 암호키 관리를 통해 데이터 이동성을 보장하며 여러 클라우드 벤더에서 데이터를 효율적으로 보호합니다. 자체 암호화를 이용할 수 없는 조직은 CipherTrust Cloud Key Manager를 사용하여 외부에서 키를 관리함으로써 업계 모범 사례를 따를 수 있습니다. CipherTrust Cloud Key Manager는 여러 클라우드 인프라 및 SaaS 애플리케이션에서 BYOK(Bring Your Own Key) 사용 사례를 지원합니다. CipherTrust Data Security Platform을 사용하면 가장 강력한 보호 장치가 클라우드에서 기업의 민감한 데이터와 애플리케이션을 보호하여 조직이 규제 준수 조건을 충족하고 데이터가 생성, 사용 또는 저장되는 위치에 상관없이 데이터를 보다 효과적으로 통제할 수 있도록 지원합니다.

총 소유 비용 절감

CipherTrust Data Security Platform은 데이터 보안을 단순화하고 규제 준수 시간을 단축하며 멀티 클라우드 보안 및 제어 기능을 제공하여 조직 규모에 관계없이 어디에서나 TCO를 줄일 수 있습니다. 확장 가능한 인프라를 기반으로 구축된 이 플랫폼은 IT 및 보안 조직이 일관되고 반복 가능한 방식으로 전사적으로 미사용 데이터를 검색, 분류 및 보호할 수 있도록 합니다. 레거시 접근 방식을 사용하려면 종종 값비싼 전용 포인트 제품이 필요할 수 있는데, 이는 추가 통합 및 관리 업무에 추가 업무 시간을 요구할 수 있어 잠재적인 비용 절감 효과가 없습니다. CipherTrust Data Security Platform에서 사용할 수 있는 많은 제품은 개별 배포나 조합 배포가 가능하며 가장 낮은 TCO로 다음 보안 과제나 규제 준수 조건에 대비할 수 있습니다. CipherTrust 솔루션은 데이터 검색, 분류, 위험 분석, 데이터 보호 및 보고를 단일 플랫폼으로 통합함으로써 IT 직원과 예산을 보다 전략적인 작업에 사용할 수 있도록 해주며 보안을 희생하지 않고도 현대 조직이 필요로 하는 협업의 개방성과 자유를 강화합니다.

요약

데이터의 가치가 높아지면서 데이터에 대한 공격이 더욱 정교해지고 있습니다. 조직은 가장 민감한 정보와 평판을 보호해야 합니다. 데이터 중심 보안은 오늘날의 사이버 보안 위협에 대항하여 규제 준수와 유의미한 보호를 모두 제공하는 유일한 접근 방식입니다. 데이터 발견 및 분류, 데이터 보호, 중앙 집중식 암호키 관리의 세 가지 핵심 요소를 토대로 하는 효과적인 데이터 중심 보안 전략을 통해, 조직은 민감 데이터에서 안전하게 가치를 창출하고 디지털 트랜스포메이션 기술을 자신있게 도입할 수 있습니다.

탈레스의 데이터 중심 솔루션을 사용하면 비용 효율적이고 효과적으로 조직 전체의 민감한 정형 데이터와 비정형 데이터를 보호할 수 있습니다.

THALES

연락처

모든 지사 위치 및 연락처 정보:
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <