솔루션 개요

THALES
CYBERSECURITY

CipherTrust 데이터 보안 태세 관리

꼭 필요한 5가지 핵심 질문

cpl.thalesgroup.com

THALES

CYBERSECURITY

DSPM의 중요성이 커지는 배경에는 데이터 보안 패러다임이 네트워크 경계 기반 방어에서 데이터 중심 접근 방식으로 전환되고 있다는 점이 있습니다. 데이터가 하이브리드 멀티클라우드 환경 전반에 걸쳐 계속 증가하고 분산됨에 따라, 민감한 정보를 보호하고 신뢰를 유지하고자 하는 조직에게 데이터 보안 태세를 동적으로 관리하는 것이 점점 더 중요해지고 있습니다.

데이터 보안 태세 관리(DSPM)란 무엇인가?

데이터 보안 태세 관리(DSPM)는 민감한 데이터가 어디에 있는지, 누가 해당 데이터에 접근할 수 있는지, 데이터가 어떻게 사용되었는지, 그리고 데이터 저장소 또는 애플리케이션의 보안 상태가 어떠한지에 대한 가시성을 제공합니다.

Source: https://www.gartner.com/reviews/market/data-security-posture-management

데이터 보안 태세 관리(DSPM)는 조직이 인프라 전반에 걸쳐 민감한 데이터를 보호하는 데 도움이 되는 솔루션과 프로세스를 말합니다. DSPM 솔루션은 데이터 검색, 분류, 보호, 위험 평가를 자동화하여 민감한 데이터가 어디에 있고 누가 접근할 수 있는지에 대한 가시성을 제공합니다. 이러한 도구는 취약점을 식별하고, 경보를 생성하며, 데이터 보안 위험을 해결하기 위한 대응 방안을 제공합니다. 다른 보안 시스템과의 통합 및 컴플라이언스 보고 기능을 통해 DSPM은 조직이 강력한 데이터 보안 태세를 유지하고 규제 요구사항을 충족하도록 지원합니다.

Gartner에 따르면, DSPM 솔루션은 온프레미스, 클라우드, 멀티클라우드, 하이브리드 클라우드 환경에 걸쳐 저장된 비정형 및 정형 데이터에 대한 검색, 분류, 위험 분석을 자동화합니다. 이를 통해 민감한 데이터의 위치, 접근 가능성, 현재 적용된 보호 조치를 지속적으로 파악합니다. DSPM 솔루션은 식별된 위험을 해결하기 위한 권고사항이나 자동화 기능을 제공하는 경우가 많으며, 데이터 보안 전략을 규제 요구사항에 맞춰 거버넌스와 컴플라이언스를 보장합니다.

오늘날 데이터 환경에서 DSPM의 중요성

최근 데이터 보안 환경은 기술적, 사회적 변화로 인해 급격히 변화하고 있으며, 이에 따라 통합적이고 포괄적인 데이터 보안 태세 관리(DSPM) 전략이 필수가 되었습니다.

DSPM이 중요해진 배경에는 데이터 보안 패러다임이 **경계 기반 방어에서 데이터 중심 접근 방식으로 전환**되고 있다는 점이 있습니다. 데이터가 하이브리드 멀티클라우드 환경 전반에 걸쳐 지속적으로 증가하고 분산되면서, 민감 정보를 보호하고 신뢰를 유지해야 하는 조직에게 데이터 보안 태세의 동적 관리는 더욱 필수적인 요소가 되고 있습니다.

통합된 DSPM 전략은 정형 데이터와 비정형 데이터를 모두 아우르며, 클라우드 환경 전반에 분산된 데이터를 관리할 수 있어야 합니다. 데이터 저장 방식이 더욱 다양해지고 복잡해짐에 따라 강력한 DSPM 솔루션의 필요성이 커지고 있습니다. DSPM 솔루션은 운영 무결성과 규제 준수를 지원하는 동시에, 끊임없이 진화하는 위협으로부터 민감 정보를 보호하는 현대 사이버 방어 전략의 핵심 기반입니다. 이제 DSPM은 새롭게 등장하는 위협에 효과적으로 대응하여 데이터를 보호해야 합니다.

데이터 보안 라이프사이클 가시성 부족:

오늘날의 복잡한 데이터 환경에서 정형 및 비정형 데이터의 위치와 상호작용을 이해하는 것은 매우 중요합니다. 그러나 데이터가 클라우드, 데이터 레이크, 온프레미스 시스템에 분산되면서 데이터를 정확하게 식별하고 분류하는 작업이 어려워졌습니다. "Cloud Security Alliance: Understanding Data Security Risk 2025" 보고서에 따르면, 응답자의 80%가 고위험 데이터 소스를 식별하는 데 확신이 없다고 답했습니다. 설상가상으로 데이터는 쉽게 이동하고 공유할 수 있어 위치에 대한 통제가 약화됩니다. 사용자가 적절한 보안 절차 없이 데이터를 공유할 경우, 민감 정보가 관리 범위 밖의 알 수 없는 장소나 외부로 이동하여 데이터 유출 공격에 노출될 위험이 커집니다.

자격 증명 무분별 확산:

클라우드 컴퓨팅의 급속한 확장으로 인해 많은 조직이 점점 더 민감한 데이터를 온라인에 저장하고 있습니다. 이러한 전환으로 인해 기존 보안 조치로는 충분히 대응할 수 없는 새로운 취약점과 복잡한 구성에 노출되었습니다. 클라우드 서비스, 컨테이너, DevOps의 신속한 도입으로 인해 키와 시크릿이 플랫폼, 리포지토리, 코드베이스 전반에 흩어져 있습니다. 이처럼 통제되지 않은 자격 증명의 확산은 공격 표면을 넓히고, 많은 보안 침해 사고가 유출되거나 잘못 관리된 자격 증명에서 비롯되고 있습니다. 2024 Verizon 데이터 침해 조사 보고서에 따르면 데이터 침해의 80%가 도난당한 자격 증명과 관련이 있습니다. 민감한 자격 증명을 보호하고 무단 접근을 방지하기 위해서는 강력한 감독과 일관된 보안 조치가 필수적입니다.

AI 기반 자격 증명 보안 위협:

AI를 활용한 피싱 캠페인과 같은 공격은 기존 방식보다 훨씬 정교하고 대규모로 실행 가능하며 탐지가 어려워, 자격 증명 탈취 위험을 크게 증가시키고 있습니다. 다중 인증(MFA)은 필수적이지만 그것만으로는 부족합니다. 비정상적인 접속 시간, 로그인 위치, 예기치 않은 데이터 다운로드 등을 추적하는 행위 기반 모니터링을 추가해야 정교한 AI 기반 위협에 효과적으로 대응할 수 있는 다층 방어 체계를 구축할 수 있습니다. **Sapios 연구와 Deep Instinct 보고서**에 따르면, 보안 전문가의 75%가 지난 1년간 사이버 공격이 증가했다고 답했으며, 85%는 생성형 AI를 활용한 공격자들이 그 주요 원인이라고 지적했습니다. 이처럼 빠르게 진화하는 위협 환경은 전체 IT 인프라에서 조직 데이터를 보호하기 위한 효과적인 DSPM 전략의 중요성을 더욱 부각시키고 있습니다.

양자 컴퓨팅 암호화 위험:

Microsoft의 Majorana 1 칩과 같은 최근 개발 성과는 양자 컴퓨팅이 머지않아 RSA, ECC 등 비대칭 암호화 알고리즘을 무력화할 수 있는 수준에 도달할 가능성을 보여줍니다.

Shor 알고리즘을 구현한 양자 컴퓨터가 등장하면 현재 사용 중인 암호화 체계가 무너지고 민감 데이터가 대규모로 노출될 위험이 있습니다. 2025 Thales 데이터 위협 보고서는 "지금 수집하고 나중에 복호화(Harvest now, decrypt later)" 공격이 70%로, 양자 컴퓨팅 관련 최대 위협으로 조사되었으며, 공격자들이 양자 컴퓨터가 상용화 되는 시점에 복호화할 목적으로 현재 암호화된 데이터를 수집하고 있다고 밝혔습니다. 이러한 위협에 대응하기 위해 조직은 지금부터 양자 내성 알고리즘을 도입하고 암호화 민첩성(crypto agility)을 확보해야 합니다.

위험 사전 탐지:

정보 유출과 데이터 파괴 등 내부자 위협은 갈수록 정교해지고 탐지가 어려워지고 있습니다. 2025 Thales 데이터 위협 보고서에 따르면, 보안 담당자들은 내부 직원에 의한 데이터 노출을 외부 해킹만큼이나 심각한 위협으로 인식하고 있습니다. 침해 사고를 사전에 차단하기 위해서는 강력한 모니터링 체계를 통한 선제적 위험 관리가 필수이며, 전통적인 경계 기반 보안만으로는 더 이상 충분하지 않습니다.

데이터 보안 태세 관리의 5가지 핵심 질문에 대한 답변

민감한 데이터가 어디에 있는가?

민감한 데이터의 위치를 파악하는 것이 데이터 보안의 출발점입니다. 여기에는 정형 데이터(데이터베이스, 스프레드 시트 등)와 비정형 데이터(이메일, 문서, 멀티미디어 파일 등)를 모두 식별하는 작업이 포함됩니다. 이러한 데이터는 온프레미스 서버는 물론 AWS, Azure, Google Cloud 등 다양한 클라우드 플랫폼에 분산되어 있는 경우가 대부분입니다.

중요성

- **적절한 보안 통제 구현:** 데이터 유형에 따라 규제 요구 사항이나 비즈니스 정책에 부합하는 차별화된 보안 조치를 적용해야 합니다.
- **데이터 확산 관리:** 데이터 볼륨이 증가하고 하이브리드 및 멀티클라우드 환경으로 분산되면서, 민감 데이터의 위치를 지속적으로 추적하고 관리하는 것이 더욱 어렵지만 동시에 더욱 중요해지고 있습니다.
- **규정 준수:** 데이터 보호법(GDPR, CCPA, HIPAA 등) 준수는 종종 특정 유형의 데이터가 저장된 위치에 대한 상세한 정보를 요구합니다.

데이터 거버넌스:

글로벌 데이터 보호 규정은 미준수 시 막대한 과징금을 부과하기 때문에, 민감 데이터가 침해되기 전에 위협을 조기에 발견하기 위한 행위 변화 탐지가 매우 중요합니다. 이에 따라 보안 전략은 DSPM과 같은 데이터 중심 접근법을 통합하여 새로운 취약점과 공격 경로에 대응할 수 있도록 진화해야 합니다. 많은 조직이 민감 데이터가 정확히 어디에 있는지, 무방비 상태로 노출되어 있지는 않은지 파악하지 못하고 있습니다. 이러한 가시성 부족은 실수로 이어지거나 공격자에게 침투 기회를 제공하며, 조직이 인지하지 못하는 숨겨진 취약점이나 잘못 설정된 데이터베이스를 통해 발생하는 경우가 많습니다.

오늘날 기업은 온프레미스 서버, 퍼블릭/프라이빗 클라우드, SaaS 플랫폼 등 다양한 스토리지 환경을 동시에 운영하고 있습니다. 이처럼 데이터 저장소가 다변화되면서 민감 데이터가 여러 위치에 분산되어 전체 현황을 파악하고 관리하는 작업이 복잡해지고 있습니다.

현대 조직은 정형 데이터(데이터베이스 등)와 비정형 데이터(이메일, 문서 등)를 포함하여 방대한 양의 데이터를 빠르게 생성하고 처리합니다. 이 모든 데이터의 위치를 실시간으로 지속 모니터링하는 것은 상당히 어려운 과제입니다.

또한 조직 내 데이터는 유동적이어서 다양한 애플리케이션과 사용자에 의해 끊임없이 이동하고, 처리되고, 액세스됩니다. 이처럼 데이터가 지속적으로 이동하기 때문에 고도화된 모니터링 도구 없이는 특정 시점의 정확한 데이터 위치를 파악하기 어렵습니다.

따라서 온프레미스, 클라우드, 멀티클라우드, 하이브리드 환경 전반에 분산된 정형 및 비정형 데이터 저장소를 자동으로 검색하고 분류하는 것이 매우 중요합니다. 자동화된 검색 및 분류 체계만이 신규 또는 변경된 데이터 저장소를 정기적이고 일관성 있게 발견하고 분류할 수 있는 유일한 방법입니다.

누가 내 민감한 데이터에 접근할 수 있는가?

민감한 데이터에 대한 접근 권한을 통제하고 모니터링하는 것은 무단 사용 및 데이터 침해를 방지하는 데 필수적입니다. 여기에는 내부 직원과 외부 파트너 모두에 대한 권한 관리가 포함됩니다.

중요성

- **데이터 침해 방지:** 민감 데이터에 대한 접근 권한을 업무상 필요한 인원으로만 제한함으로써 내부자 위협과 외부 공격 위험을 최소화할 수 있습니다.
- **컴플라이언스 지원:** 대부분의 규제 프레임워크는 데이터 접근에 대한 엄격한 통제를 요구합니다. 접근 권한 보유 현황을 파악하면 관련 규정을 효과적으로 준수할 수 있습니다.
- **데이터 거버넌스 강화:** 데이터 접근 활동을 모니터링하면 감사 추적 및 사용 패턴 분석이 가능하며, 이는 보안 및 운영 효율성 향상에 핵심적인 역할을 합니다.

많은 조직은 통합 관리 도구의 부재로 인해 데이터 접근에 대한 가시성과 통제력이 제한적입니다. 다양한 시스템과 플랫폼에 분산된 접근 정보를 효과적으로 수집하고 분석할 수단이 없으면, 현재 누가 민감 데이터에 접근할 수 있는지 파악하기 어렵습니다.

현대 기업은 대부분 역할 기반 접근 제어(RBAC), 속성 기반 접근 제어(ABAC) 등 복잡하고 다층적인 접근 통제 체계를 운영합니다. 이러한 복잡한 구조로 인해 누가, 어떤 데이터에, 어떤 조건에서 접근할 수 있는지를 정확히 파악하기 어렵습니다.

또한 대규모 조직에서는 부서나 사업부별로 IT 리소스를 독자적 으로 관리하는 경우가 많아, 접근 통제 정책이 일관되지 않게 적용됩니다. 이러한 분산 관리 체계는 전사 차원의 데이터 접근 현황 추적을 어렵게 만들고, 민감 정보에 대한 접근 권한 가시성을 더욱 저하시킵니다.

따라서 데이터 저장소를 스캔하여 부여된 사용자 권한을 확인하고, 모든 데이터베이스 객체에 대한 사용자와 권한을 매핑함으로써 전체 접근 권한 현황을 파악하는 것이 데이터 보안 태세 관리의 핵심입니다.

자격 증명은 얼마나 안전하게 보호되고 있는가?

암호화된 데이터를 복호화할 수 있는 암호화 키와 시크릿 같은 자격 증명 및 메타데이터에 대한 보호 체계를 구축하는 것이 매우 중요합니다. 특히 양자 컴퓨팅 시대가 도래하여 악의적인 복호화 공격이 현실화될 때를 대비한 암호화 전략이 필수적입니다.

중요성

- **메타데이터 보안 강화:** 암호화 키와 시크릿을 암호화된 데이터와 물리적으로 분리하여 중앙에서 관리함으로써 민감 데이터 보호를 위한 추가 보안 계층을 확보할 수 있습니다.
- **양자 컴퓨팅 위협 대응:** 암호화 민첩성(Crypto Agility)을 지원하는 솔루션을 도입하면 양자 내성 암호화(PQC) 알고리즘과 키를 즉시 적용할 수 있어 미래 위협에 선제적으로 대비할 수 있습니다.
- **자격 증명 확산 통제:** 키와 시크릿의 무분별한 확산을 차단하고 자격 증명을 체계적으로 관리하는 것은 공격 표면을 최소화하고 무단 데이터 접근을 원천 차단하는 데 필수적입니다.

많은 조직이 암호화를 데이터 보호의 핵심 수단으로 활용하지만, 암호화된 데이터를 복호화할 수 있는 키와 시크릿의 보호는 간과하는 경우가 많습니다. 이는 마치 현관 매트 아래 집 열쇠를 두는 것과 같습니다. 암호화 키와 시크릿을 암호화된 데이터 근처에 저장하면 보안이 무력화됩니다. 조직은 데이터를 여러 클라우드 서비스 제공업체(CSP)에 분산 저장하는 경우가 많은데, 이로 인해 키 생성, 관리, 순환 프로세스가 CSP마다 상이하게 운영됩니다.

암호화 솔루션을 추가로 도입할수록 비일관적인 정책 관리, 제각각인 보호 수준, 그리고 비용 증가라는 문제에 직면하게 됩니다. 이러한 복잡성을 해소하는 가장 효과적인 방법은 중앙 집중식 암호화 키 관리 시스템으로 전환하는 것입니다.

키와 시크릿의 전체 생명주기(생성, 저장, 순환, 백업, 복구, 폐기, 종료)를 중앙에서 통합 관리하면 직무 분리 원칙을 효과적으로 구현할 수 있습니다. 이를 통해 키를 생성·관리하는 담당자가 보호된 데이터에 직접 접근할 수 없도록 통제하고, 중요 작업에 대한 책임을 분산함으로써 보안 위험을 최소화할 수 있습니다.

내 민감한 데이터는 어떻게 사용되었는가?

시간 경과에 따라 데이터가 어떻게 접근되고 사용되는지 추적하는 것은 보안 및 규제 준수를 위해 필수적입니다. 여기에는 데이터 접근 및 수정의 컨텍스트를 이해하고 보안 위협을 나타낼 수 있는 비정상적인 패턴을 탐지하는 것이 포함됩니다.

중요성

- **이상 징후 탐지:** 비정상적인 접근 패턴이나 예상치 못한 데이터 수정은 데이터 침해의 조기 경보 신호가 될 수 있습니다.
- **감사 및 포렌식 분석:** 데이터 사용에 대한 상세한 로그는 정기 감사뿐만 아니라 보안 사고 발생 시 포렌식 조사에서 결정적인 증거 자료로 활용됩니다.
- **데이터 접근 통제 최적화:** 데이터 사용 패턴을 분석하면 실제 업무 요구사항과 보안 정책에 부합하도록 접근 통제 체계를 지속적으로 개선할 수 있습니다.

효과적인 데이터 사용 추적을 위해서는 모든 데이터 접근 활동을 상세하고 정확하게 기록하는 고도화된 모니터링 및 로깅 솔루션이 필요합니다. 그러나 많은 기업이 이러한 솔루션을 갖추지 못했거나 전체 시스템에 완전히 통합하지 못해 데이터 사용 현황에 대한 가시성 공백이 발생하고 있습니다.

오늘날 기업은 온프레미스 시스템, 다수의 클라우드 플랫폼, 다양한 엔드포인트 장치가 혼재된 매우 복잡한 데이터 환경에서 운영되고 있습니다. 각 환경마다 데이터 처리 및 저장 방식이 상이하기 때문에 전사 차원에서 데이터 접근과 사용 이력을 일관되게 추적하기가 매우 어렵습니다.

GDPR, HIPAA 등 다양한 규제는 데이터 접근 및 사용에 대한 상세한 로깅을 의무화하고 있습니다. 여러 국가와 지역의 서로 다른 규제 요구사항을 동시에 충족하는 것은 민감 데이터의 사용 추적을 더욱 복잡하게 만듭니다.

강력한 규제 준수 및 보안 체계는 데이터 보호의 근간이며, 사용 현황, 취약점, 접근 권한에 대한 완전한 가시성을 확보하는 것이 핵심입니다. 디지털 경제가 데이터의 폭발적 증가를 가속화함에 따라, 조직은 규제 위반과 보안 침해 위험을 최소화하기 위해 데이터 중심의 컴플라이언스 및 보안 솔루션을 도입해야 합니다. 자동화된 워크플로우와 권장 조치를 활용하면 보안팀이 데이터 위험을 조기에 식별하고 신속하 게 대응할 수 있습니다.

데이터 저장소의 보안 태세(현재 데이터 보안 상태)는 어떠한가?

데이터 저장소의 보안 태세를 평가한다는 것은 현재 적용된 보안 조치의 실효성을 검증하고, 존재하는 취약점을 식별하며, 잠재적 위협이 미칠 수 있는 영향을 파악하는 것을 의미합니다.

중요성

- **방어 체계 강화:** 데이터 보안의 취약점과 보안 격차를 식별하여 선제적으로 개선함으로써 침해 사고를 사전에 차단할 수 있습니다.
- **보안 자원의 효율적 배분:** 보안 취약 영역을 정확히 파악하면 제한된 보안 자원을 우선순위가 높은 곳에 집중 배치할 수 있습니다.
- **보안 복원력 확보:** 보안 태세를 정기적으로 평가함으로써 진화하는 위협과 변화하는 비즈니스 환경에 신속하게 대응할 수 있는 방어 체계를 유지할 수 있습니다.

효과적인 보안 태세 관리를 위해서는 지속적으로 업데이트되는 최신 취약점 정의가 필요하며, 이를 기반으로 자산을 평가하고 취약점을 스캔하여 위험도를 판정합니다. CIS 및 DISA STIG 벤치마크 기반의 사전 정의된 취약점 테스트를 통해 데이터베이스를 스캔하면, 최신 위협에 노출된 데이 터베이스를 즉시 파악할 수 있습니다. 이러한 스캔은 CVSS(Common Vulnerability Scoring System)를 활용하여 네트워 크와 데이터에서 발견된 취약점의 위험도를 평가하고 점수를 부여합니다. CVSS는 “IT 취약점의 특성과 영향을 표준화하여 전달하기 위한 개방형 프레임워크”로, 미국 국립표준 기술연구소(NIST)가 관리하는 SCAP(Security Content Automation Protocol) 프레임워크의 핵심 구성 요소입니다. CVSS 점수 체계를 활용하면 발견된 취약점의 내재 위험을 정량적으로 측정하고 완화 작업의 우선순위를 과학적으로 결정할 수 있습니다.

모니터링은 데이터 관리 생명주기에서 핵심적인 단계로, 시스템 이벤트, 경보, 정책 위반, 차단된 접근 시도, 게이트웨이 및 에이전트 상태, 시스템 경고, 데이터베이스 감사 로그, 파일 서버 감사 로그, 아카이빙 정보 등을 실시간으로 제공합니다.

이벤트, 경보, 정책 위반에 대한 모니터링은 다양한 관점에서 이루어질 수 있습니다. 구현 환경에 따라 서로 다른 역할 과 보안 정책을 가진 여러 유형의 사용자가 존재할 수 있습니다. 사전 정의된 심각도 등급을 적용하거나 정책을 맞춤 설정하여 이벤트 해석 기준을 세밀하게 조정함으로써, 경보가 오탐(False Positive)인지, 실제 공격인지, 또는 다른 유형 의 이벤트인지를 정확히 판별할 수 있습니다.

위험을 넘어 데이터를 안전하게 보호하는 통합 플랫폼

데이터는 조직의 가장 가치 있는 자산이며 규모의 경제를 실현하는 핵심 동력입니다. AI를 비롯한 혁신 기술의 도입으로 조직은 그 어느 때보다 방대한 양의 데이터를 생성하게 될 것입니다. 이러한 데이터와 데이터 저장소의 폭발적 증가는 더 많은 보안 사각지대와 데이터 노출 취약점을 야기합니다. 데이터를 안전하게 보호하는 동시에 그 잠재력을 최대한 활용하기 위해서는 민감 데이터를 정확하게 식별하고 보안, 거버넌스, 컴플라이언스 체계를 강화하는 것이 필수적입니다.

데이터 자산 현황 파악

CipherTrust DSPM은 온프레미스, 클라우드, 멀티클라우드 및 하이브리드 클라우드 환경을 포함한 광범위한 데이터 저장소 전반에 걸쳐 정형 및 비정형 데이터의 검색 및 분류를 자동화합니다.

- **데이터 스캔 및 식별:** CipherTrust DSPM은 온프레미스와 클라우드 환경을 체계적으로 스캔하여 데이터 저장소를 자동 검색합니다. 데이터베이스, 빅데이터 플랫폼, 클라우드 스토리지, 파일 시스템 등이 모두 포함됩니다.
- **데이터 분류:** 검색이 완료되면 CipherTrust DSPM은 데이터 유형 및 민감도에 따라 자동으로 분류합니다. 이를 통해 조직은 보유 데이터 현황을 정확히 파악하고 보안 우선순위를 효과적으로 수립할 수 있습니다.
- **사용자 접근 권한 관리:** CipherTrust DSPM은 사용자 권한을 체계적으로 관리하고, 데이터 접근 활동을 모니터링하며, 특히 특권 사용자의 활동을 집중 감시하여 과도하거나 부적절하거나 미사용 권한을 식별합니다. 보안 및 IT 팀에 데이터가 조직 내에서 어떻게 접근되고, 사용되며, 이동하는지에 대한 완전한 가시성을 제공합니다.

데이터 보안 태세 강화

체계적인 데이터 보호 전략은 데이터 보안 태세 관리 (DSPM)의 핵심 요소이지만 종종 간과되곤 합니다. 암호화와 효과적인 자격 증명 관리를 통한 견고한 데이터 보호 기반 구축은 강력한 보안 태세를 유지하는 데 필수적입니다. CipherTrust DSPM은 민감 데이터를 식별하고 업계 최고 수준의 보안 기술로 보호합니다. 자격 증명과 메타데이터를 안전하게 관리함으로써 사용자와 애플리케이션의 무단 접근을 원천 차단하고, 조직의 데이터 보안 및 컴플라이언스 체계를 전반적으로 강화합니다.

- **민감 데이터 보호:** 암호화, 데이터 마스킹, 토큰화 등 핵심 데이터 보호 기술을 구현하여 신용카드 정보, 지적 재산권, 개인 식별 정보(PII) 등 민감 정보를 보호하고, 오직 인가된 애플리케이션과 담당자만 이를 사용할 수 있도록 통제합니다.
- **암호화 키 및 메타데이터 보안:** 암호화와 데이터 마스킹은 데이터 보호의 첫 번째 단계입니다. 그러나 보호된 데이터를 복호화할 수 있는 키와 시크릿을 중앙 집중식 키 관리 체계로 안전하게 보호하는 것이 동등하게 중요합니다. 이를 위해서는 하이브리드 클라우드 환경 전반에 분산된 키와 시크릿을 탐지하고 관리 대상으로 등록해야 합니다.
- **양자 컴퓨팅 위협 대응:** 양자 컴퓨터는 현재 널리 사용되는 암호화 방식을 무력화할 수 있어 심각한 사이버보안 위협이 되고 있습니다. 이로 인해 데이터 침해, 통신 보안 손상, 블록체인 및 인증 프로토콜 취약점 등이 발생할 수 있습니다. 조직은 이러한 위협에 선제적으로 대응하기 위해 양자 내성 암호화로 전환하고 사전 예방적 보안 대책을 수립해야 합니다.
- **자격 증명 확산 통제:** 암호화, 토큰화, 데이터 마스킹 기술은 자격 증명이 인가된 대상 범위를 벗어나 유출되지 않도록 보호합니다. 이러한 기술을 통해 데이터를 판독 불가능하거나 사용 불가능한 상태로 유지함으로써 민감 데이터를 포함하는 무단 데이터 저장소의 생성을 원천 차단합니다.

강력한 데이터 보호 기반이 마련되면, CipherTrust DSPM은 조직이 선제적 위험 분석을 통해 관리 중인 데이터의 위험 요소를 효과적으로 식별하고 우선순위를 설정할 수 있도록 지원합니다. 지능형 위험 분석 기능은 조직이 취약점의 위치와 심각도를 신속하게 파악할 수 있는 핵심 인사이트 를 제공합니다. 이를 기반으로 위험 완화를 위한 전략적 대응 계획을 수립하고 실행함으로써, 데이터 보안 태세를 대폭 강화하고 조직의 가장 중요한 자산인 데이터를 안전하게 보호할 수 있습니다.

- **위험 평가:** 데이터가 어떻게 저장, 접근, 공유되는지 평가함으로써 CipherTrust DSPM은 데이터 침해로 이어질 수 있는 취약점, 위험한 구성 설정, 부적절한 접근 통제를 식별합니다. CipherTrust DSPM은 모든 환경의 데이터 보안 위험에 대한 통합 뷰를 제공하여 조직이 민감 데이터의 위치, 적용된 보호 수준, 보호 방식을 한눈에 파악하고, 내부자 위협을 시사하는 키 또는 시크릿 오용 사례를 탐지할 수 있습니다.

- **행위 변화 탐지:** 사용자 및 엔터티의 행위 변화는 위험과 잠재적 환경 위협의 핵심 지표입니다. AI 기반 위협이 등장 하면서 행위 분석은 정교한 피싱 전술이나 은밀한 공격의 미묘한 징후를 포착하는 데 매우 효과적인 도구로 입증되었습니다.
- **AI 관련 위험 식별:** 업무 효율성 향상을 위한 AI 활용이 증가하면서 조직은 새로운 유형의 보안 위험에 직면하고 있습니다. 섀도우 AI 서비스를 식별하고, AI를 통한 민감 데이터 유출을 방지하며, 비정상적인 AI 활동을 탐지하고 신속히 대응하는 것이 필수적입니다.
- **인시던트 상관관계 분석:** AI 기반 분석을 활용하여 사용자 행위를 애플리케이션 및 데이터 컨텍스트와 결합함으로써 외부 위협과 내부자 위협을 정확히 파악하고 "저속 은밀형 (Low and Slow)" 공격에 효과적으로 대응합니다.
- **우선순위 기반 대응:** 맞춤형 위험 점수 체계를 통해 조직은 단순히 위험을 식별하는 수준을 넘어 심각도와 영향도를 기반으로 우선 대응이 필요한 영역을 결정할 수 있습니다. 이를 통해 보안 투자 효과가 가장 큰 영역에 자원을 집중 배치할 수 있습니다.

데이터 보안 운영 지속적 개선

위험이 식별되면 신속하고 효과적으로 대응하는 것이 핵심입니다. CipherTrust DSPM은 위험을 식별하는 데 그치지 않고 이를 완화하기 위한 구체적인 권장사항을 함께 제공합니다. 플레이북 기능을 활용하면 조직은 위험한 행위를 보이는 사용자를 자동으로 격리하거나 위협 조사를 위한 티켓을 생성하는 등 데이터 보안을 위한 자동화된 대응 조치를 설정할 수 있습니다.

- **보안 강화 권고:** 위험 평가 결과를 바탕으로 CipherTrust DSPM은 보안 취약 영역에 대한 실행 가능한 인사이트와 구체적인 보안 강화 방안을 제공합니다.
- **보안 정책 자동 적용**: CipherTrust DSPM은 다양한 플랫폼 전반에 걸쳐 보안 정책을 자동으로 적용하여 데이터 자산 보호에 필요한 수작업을 대폭 줄일 수 있습니다.
- **인시던트 우선순위 관리:** CipherTrust DSPM은 영향받은 시스템과 정책 위반의 심각도를 신속히 파악하여 효율적인 인시던트 관리 및 신속한 문제 해결을 지원합니다.

데이터 거버넌스 및 컴플라이언스 이니셔티브는 데이터 생명주기 전반에 걸쳐 조직 데이터의 품질, 보안, 가용성을 보장하기 위한 정책과 프로세스를 수립합니다. CipherTrust DSPM은 데이터 접근, 사용, 전송에 대한 완전한 가시성을 제공하여 조직의 데이터 보안 전략이 거버넌스 및 컴플라이언스 요구사항과 일치하도록 지원합니다.

- **규제 준수 지원:** 민감 데이터가 적절히 보호되고 접근 통 제가 올바르게 구현되도록 보장하여 GDPR, HIPAA, CCPA 등의 규제 요구사항을 충족합니다. 특히 새로운 규제 요구사항을 만족하기 위해서는 키와 시크릿의 사용 이력을 감사할 수 있는 기능이 필수적입니다.
- **컴플라이언스 보고서 생성:** CipherTrust DSPM은 감사자 및 이해관계자에게 규제 준수 상태를 입증할 수 있는 상세한 보고서를 자동으로 생성합니다.

DSPM 솔루션은 민감 데이터를 체계적으로 보호하려는 조직에 필수적입니다. 이러한 솔루션은 효과적인 데이터 보안 전략의 토대가 되는 5가지 핵심 질문에 명확한 답변을 제공합니다.

CipherTrust DSPM: DSPM에 필수적인 핵심 기술 통합

데이터 검색

CipherTrust DSPM은 온프레미스부터 클라우드까지 다양한 환경에서 민감 데이터를 자동으로 검색하고, 중요 정보를 식별 및 매핑합니다. 이를 통해 컴플라이언스 관리를 강화하고 침해 사고를 예방할 수 있습니다.

데이터 분류

CipherTrust DSPM은 데이터를 민감도 및 규제 요구사항에 따라 세밀하게 분류하여 적절한 보안 조치를 정확히 적용하고 데이터 보호 우선순위를 명확히 설정할 수 있도록 지원합니다.

데이터 암호화, 마스킹, 토큰화

CipherTrust DSPM은 IT 에코시스템 전반에서 저장 및 전송 중인 데이터를 보호, 익명화, 암호화하며, 해당 암호화 키가 안전하게 보보되고 오직 조직의 통제 하에만 관리되도록 보장합니다.

정적 위험 분석

시스템의 정적 위험 분석 기능은 데이터 인프라 내의 취약점을 사전에 식별하여 조직이 이를 악용당하기 전에 잠재적 위협을 제거할 수 있도록 합니다.

노출 위험 평가 및 식별

CipherTrust DSPM은 데이터 접근 경로와 노출 수준을 지속적으로 모니터링하여 무단 접근이나 데이터 유출을 신속히 탐지하고 차단하며, 민감 정보의 무결성을 보호합니다.

고위험 취약점 실시간 경보

실시간 경보 시스템은 심각한 취약점을 즉시 알리고, 잠재적 영향도에 따라 대응 우선순위를 자동으로 설정하여 신속하고 효과적인 조치를 가능하게 합니다.

위험 보고 및 평가

심층적인 위험 평가와 맞춤형 보고 기능을 제공하여 조직의 보안 태세를 정확히 파악하고, 선제적 대응이 필요한 취약점을 명확히 식별할 수 있도록 지원합니다.

개선 방안 제시

CipherTrust DSPM은 식별된 보안 취약점에 대한 구체적인 조치 방안을 제시하며, 업계 모범 사례 및 표준에 부합하는 실용적이고 실행 가능한 가이드를 제공합니다.

엔터프라이즈 환경 지원

확장 가능한 아키텍처로 설계된 CipherTrust DSPM은 기존 엔터프라이즈 시스템과 원활하게 통합되며, 복잡한 데이터 환경을 지원하고 조직의 변화하는 요구사항에 유연하게 대응합니다.

보안 오케스트레이션 통합

CipherTrust DSPM을 보안 오케스트레이션 서비스와 연계하여 보안 운영을 최적화하고, 다양한 보안 도구를 통합 관리하며, 전체 보안 운영의 효율성을 향상시킵니다.

플레이북 자동화

CipherTrust DSPM은 플레이북 기반 자동화를 통해 일반적인 보안 인시던트에 대한 표준 대응 절차를 제공하고, 위협 대응 프로세스를 간소화하며, 대응 시간과 피해 규모를 최소화합니다.

컴플라이언스 감사 및 보고

CipherTrust DSPM은 접근 로그부터 위험평가까지 데이터 보안 관리의 전 과정을 상세히 문서화한 보고서를 제공하여 규제 준수 및 감사 프로세스를 효과적으로 지원합니다.

Thales 소개

Thales는 글로벌 사이버보안 분야의 선도 기업으로, 기업, 정부 및 세계에서 가장 신뢰받는 조직들이 최고의 ROI로 대규모로 어디서나 중요 애플리케이션, 민감한 데이터, 아이덴티티 및 소프트웨어를 보호하도록 지원합니다. Fortune Global 500대 기업 중 58%를 포함하여 30,000개 이상의 고객사와 함께 전 세계 148개국에 솔루션을 배포하고 있습니다. Thales는 혁신적인 서비스와 통합 플랫폼을 통해 고객이 위험에 대한 더 나은 가시성을 확보하고, 사이버 위협을 방어하며, 컴플라이언스 격차를 해소하고, 매일 수십억 소비자를 위한 신뢰할 수 있는 디지털 경험을 제공하도록 지원합니다.