COHESITY

구매자 가이드

데이터 및 AI 위험을 적절한 DSPM 솔루션으로 탐색

요약

민감한 데이터는 이제 클라우드 플랫폼, SaaS, 데이터베이스, 백업, 하이브리드 인프라, NAS 등 다양한 환경에 분산되어 있습니다. 이미 손쉽게 관리하기 어려울 정도로 많은 데이터를 보유하고 있을 가능성이 높습니다. 하지만 가장 민감한 데이터가 어디에 저장되어 있는지, 얼마나 광범위하게 노출되어 있는지, 누가 해당 데이터에 접근할 수 있는지, 그리고 그 접근 권한이 적절한지 파악하기는 쉽지 않습니다.

이는 이사회 차원의 비즈니스 리스크를 더욱 가중시키는 최악의 상황을 초래합니다. 그리고 그 도전 과제는 점점 더 커지고 있습니다. 사람들이 이 데이터에 계속 접근하고 수정하고 이동시키는 가운데, AI 에이전트는 새롭고 점점 더 커지는 위험 요소를 추가하고 있습니다.

이러한 보안 및 보호 공백 때문에 DSPM(Data Security Posture Management, 데이터 보안 태세 관리)은 현대 기업 리더들에게 전략적 우선 과제가 되었습니다.

89% 의 보안 리더들은 회사의 데이터 보안 현황이 문제라고 답했습니다.

39% 의 보안 리더들은 기존 기술이 현재 요구 사항을 충족하기에 불충분하다고 답했습니다.

60% 의 기업들은 자사 데이터 자산의 절반 이상에 대한 가시성을 확보하지 못하고 있습니다.[1]

[1]Omdia 백서: 실행 가능한 데이터 인텔리전스를 통해 사이버 레질리언스 확보

현대적인 DSPM 솔루션은 단순히 데이터를 목록화하는 수준을 훨씬 넘어서는 역할을 해야 합니다. 리스크를 능동적으로 줄이고, 사이버 레질리언스를 강화하며, 사고 대응, 보안 훈련 또는 감사 과정에서 다음과 같은 중요한 질문에 답할 수 있도록 지원해야 합니다.

- 우리의 민감한 데이터는 어디에 있으며, 어떤 데이터인가?
- 누구 또는 어떤 주체가 해당 데이터에 접근할 수 있는가?
- 무엇을 가장 먼저 해결해야 하는가?
- 비즈니스 혁신과 성장을 저해하지 않으면서 어떻게 리스크를 줄일 수 있는가?
- 데이터가 보호되고 있으며, 신속하고 안전하며 규정을 준수하는 방식으로 복구할 수 있는가?

보안 리더에게 이는 공격 발생 전후 모두에서 단순한 가시성 확보를 넘어, 실행 가능한 리스크 해소로 나아가는 것을 의미합니다.

이 가이드는 DSPM 솔루션을 평가하는 팀이 자사 요구에 적합한 솔루션을 선택할 수 있도록 돕기 위해 마련되었습니다.

단순한 데이터 인벤토리만으로는 충분하지 않습니다.

실제 구매 결정에서 중요한 질문은 솔루션이 데이터의 위치를 보여줄 수 있는지가 아닙니다. 해당 데이터가 왜 높은 위험 요소인지 식별하고 보여줄 수 있는지, 그리고 그 위험을 해결하기 위해 지금 무엇을 해야 하는지 제시할 수 있는지가 핵심입니다.

DSPM이 해결하는 문제

DSPM을 평가할 때 조직이 저지르는 가장 흔한 실수 중 하나는 이를 단순한 검색 도구로 취급하는 것입니다. DSPM 솔루션은 가시성 그 이상입니다. 올바른 솔루션이라면 데이터 위험 태세와 관련된 문제를 해결하는 데 도움이 되어야 합니다.

다음은 DSPM 솔루션이 해결할 수 있어야 하는 5가지 핵심 과제입니다.

당면 과제	DSPM이 이를 해결하는 방법
민감한 데이터가 어디에 있는지 모르겠습니다.	많은 조직은 클라우드, SaaS 및 하이브리드 환경 전반에서 가장 중요한 데이터나 규제 대상 데이터가 어디에 있는지 확신 있게 파악하지 못하고 있습니다. 왜 이러한 상황이 계속되고 있을까요? 기존 데이터 보안 도구는 특정 데이터 유형, 특정 배포 모델 또는 특정 사용 사례에만 국한되어 있는 경우가 많기 때문입니다. 일부 인벤토리 정보를 보유하고 있더라도, 그 정보는 불완전하거나 오래되었거나 리스크 맥락과 분리되어 있는 경우가 많습니다. 데이터의 양과 확산 속도에 대응하려면 현대적인 클라우드 네이티브 아키텍처가 필요합니다.
어떤 사람이나 시스템이 내 데이터에 접근하고 있는지(또는 접근할 수 있는지) 알 수 없습니다.	일반적인 직원은 매일 200개 이상의 협업 도구 전반에서 약 36개의 클라우드 서비스를 사용합니다. 민감한 정보는 여러 플랫폼에 퍼져 있으며, 정해진 거버넌스 통제를 벗어나 공유되는 경우도 많습니다. 민감한 데이터는 과도하게 노출되거나, 권한이 지나치게 부여되거나, 지나치게 광범위하게 공유되거나, 잘못된 위치에 저장되거나, 의도보다 더 많은 사용자 ID 및 비인간 ID가 접근 가능할 때 위험 요소는 훨씬 더 커집니다. DSPM 솔루션은 단순히 분류 정책에 부합하는 데이터를 제시하는 데 그치지 않고 실제로 어떤 데이터가 위험에 노출되어 있는지 파악하도록 지원해야 합니다.
어떤 데이터 리스크를 가장 우선적으로 해결해야 할지 알 수 없습니다.	대부분의 엔터프라이즈 환경에는 대량의 민감한 데이터가 존재합니다. 그러나 모든 데이터 위험은 긴급성이 서로 다릅니다. 팀에는 단순한 배경 잡음과 실제로 의미 있는 노출 위험을 구분할 수 있는 방법이 필요합니다. 올바른 솔루션이라면 데이터 민감도, 접근 권한, 노출 수준, 환경, 그리고 학습된 비즈니스 맥락을 기반으로 가장 큰 비즈니스 영향을 초래할 수 있는 문제에 집중할 수 있도록 지원해야 합니다.
데이터 리스크를 신속하게 또는 자동으로 해결할 수 없습니다.	고위험 데이터에 대한 대응 및 복구 과정에서 MTTR(평균 대응 시간)을 단축하려면 데이터 컨텍스트가 반드시 보안 툴체인 전반에 걸쳐 긴밀하게 통합되어야 합니다. 기존 데이터 보안 방식은 패턴과 태그에 지나치게 의존하기 때문에 신뢰성이 부족한 과도한 경고를 쏟아내는 경우가 많습니다. DSPM 솔루션은 실제 조치로 이어질 수 있어야 합니다. 조사 결과는 이해하기 쉽고, 담당자 지정 및 추적이 가능해야 합니다. 또한 보안 및 IT 팀이 이를 바탕으로 확신을 갖고 대응할 수 있어야 합니다.
데이터를 복구해야 할 때마다 과정이 느리고, 위험 부담이 크며, 비용도 많이 듭니다.	보조 데이터(예: 백업 데이터)는 사고 대응 및 복구 과정에서 매우 중요한 역할을 합니다. 하지만 이러한 데이터 역시 해결해야 하는 리스크와 잠재적인 규제 준수 위반 요소를 초래할 수 있습니다. 현대적인 DSPM 솔루션은 사이버 레질리언스를 강화하고, 적절한 수준의 보호 조치가 적용될 수 있도록 데이터 인텔리전스를 제공해야 합니다. 또한 사고 대응 과정에서는 민감 데이터를 우선적으로, 그리고 규제를 준수하며 복구할 수 있어야 합니다.

‘좋은’ 모습이란 무엇인가

벤더를 평가하기 전에 ‘좋은’ 것이 무엇인지 결정해야 합니다. 다음은 최신 DSPM 솔루션이 탁월해야 할 5가지 영역입니다.

신속하게 배포하고 제한 없이 원활하게 확장

우수한 데이터 탐지 기능은 가치를 얻기 전에 길고 복잡한 구현 주기를 요구하지 않고도 노출을 더욱 완전하게 파악하는 데 도움이 되어야 합니다.

조직은 성능 저하 없이 수백 페타바이트 규모의 데이터를 지속적으로 스캔할 수 있어야 합니다. 적합한 벤더는 필요에 따라 클라우드 데이터 저장소, SaaS 애플리케이션, 파일 시스템, 온프레미스 데이터베이스 등 주요 환경 전반에 걸쳐 폭넓은 지원을 제공해야 합니다.

정확한 데이터 탐지 및 분류로 사각지대 제거

강력한 데이터 탐지 기능은 부정확한 결과가 모든 후속 결과를 오염시키는 것을 방지하는 데 도움이 됩니다. DSPM 도구가 중요한 위치를 놓치거나, 민감한 정보를 잘못 분류하거나, 지나치게 많은 수동 조정을 필요로 한다면, 그 결과는 유용성이 떨어지거나 심지어 무의미해질 수 있습니다.

적합한 DSPM 솔루션은 환경에 맞게 유연하게 대응하고 데이터를 자동으로 분류함으로써(IP 및 비즈니스에 고유하게 중요한 데이터 포함) 사각지대를 찾아낼 수 있어야 합니다.

잡음이 아닌 실제 위험을 우선순위로 지정

시간은 한정적이며, 어떤 팀도 모든 문제를 한 번에 해결할 수는 없습니다. 강력한 DSPM 솔루션을 사용하면 노출 위험과 맥락 정보를 결합해 가장 큰 위험 요소에 집중할 수 있습니다. 특히 광범위하게 노출된 고도의 민감 데이터를 우선적으로 위험 관리할 수 있어야 합니다.

이를 위해서는 데이터 민감도, 비즈니스 목적, 사용자 ID, 접근 활동, 노출 수준을 연계 분석하여 실제 비즈니스 리스크를 식별할 수 있는 고급 기능이 필요합니다.

대규모 자동 대응 지원

현대적인 DSPM은 단순히 관찰하는 것이 아니라 조직이 위험에 노출하는 횟수를 줄일 수 있도록 지원해야 합니다. 조직은 기본 제공 대응 기능을 제공하는 DSPM 솔루션을 검토해야 합니다. 예를 들어, 선도적인 솔루션은 클릭 한 번으로 액세스 권한을 철회하고, 데이터를 마스킹하며, 사전 정의된 워크플로우를 실행하고, 문제를 데이터 소유자에게 직접 전달할 수 있는 기능을 제공합니다. 또한 문제를 신속하게 해결하는 데 필요한 맥락 정보도 함께 제공합니다.

이는 특히 여러 팀이 관여하는 엔터프라이즈 규모의 환경에서 매우 중요합니다. 보안 팀이 문제를 식별하더라도, 실제 대응 및 해결은 스토리지 관리자, 데이터 소유자, ID 관리 팀 또는 비즈니스 이해관계자 등 다른 조직의 협업에 의존하는 경우가 많습니다. 솔루션이 이러한 인계 및 협업 과정을 얼마나 명확하게 지원하는지에 따라, 보안 상태를 실제로 개선하는 의미 있는 성과로 이어질 가능성이 높아집니다.

사고 전후 보안 강화

사고 발생 전의 선제적 리스크 해소에 대해서는 이미 살펴보았습니다. 올바른 DSPM 솔루션이라면 복구 역량을 강화하는 데 필요한 데이터 인텔리전스와 맥락 정보도 제공할 수 있어야 합니다. 이를 통해 보안 및 데이터 보호 팀은 민감한 데이터가 어디에 저장되어 있는지, 어떤 자산이 가장 중요한지, 그리고 조직의 핵심 자산에 적절한 보호 조치가 적용되었는지를 파악할 수 있어야 합니다.

민감 데이터와 비즈니스 핵심 데이터에 대한 명확한 가시성을 바탕으로, DSPM은 사이버 레질리언스를 뒷받침하는 데이터 보호 전략을 지원하고 강화해야 합니다. 이를 통해 복구 과정에서 가장 중요한 데이터를 우선적으로 처리하고, 더 풍부한 맥락 정보를 기반으로 사고 대응 속도를 높이며, 오래되었거나 중복되거나 가치가 낮은 데이터를 식별·제거함으로써 비용과 복잡성을 줄일 수 있습니다.

그 결과, 가시성 확보, 보호, 대응, 복구 간의 지속적인 피드백 루프가 형성됩니다. 적합한 DSPM 솔루션을 사용하면 이러한 기능들을 서로 연결하여, 분절된 보안 활동에서 벗어나 더욱 통합적이고 엔드투엔드 방식의 데이터 보안 및 사이버 레질리언스 전략으로 전환할 수 있습니다.

공급업체 평가 키트

공급업체에 물어볼 중요 질문

다음 질문은 DSPM 제품의 최종 후보 목록을 평가하는 데 도움이 됩니다.

데이터 탐지 및 적용 범위:

- 현재 어떤 클라우드, SaaS, AI, 데이터베이스 및 하이브리드 환경을 지원하고 있습니까?
- 다양한 데이터 유형 가운데 민감한 데이터를 어떻게 식별하고 분류하고 있습니까? 일반적으로 시간이 얼마나 소요됩니까?
- 정형 및 비정형 데이터를 어떻게 처리합니까? 어느 한쪽에 더 나은 지원을 제공합니까?
- 결과를 실제로 활용할 수 있기까지 어느 정도의 조정이 필요합니까?
- 고객이 초기 단계에서 적용 범위와 신뢰도를 검증할 수 있도록 어떻게 지원합니까?

노출 및 액세스 제어:

- 민감한 데이터가 과도하게 노출되어 있는지를 어떻게 판단합니까? • 어떤 ID, 그룹 또는 사용자가 민감한 데이터에 접근할 수 있는지 보여줄 수 있습니까?
- 광범위하거나 과도하거나 위험한 접근 권한을 어떻게 식별합니까?
- 접근 맥락 정보를 데이터 민감도와 어떻게 연계합니까?
- AI 모델 및 시스템에 민감한 데이터가 입력되거나 외부로 유출되는 것을 차단할 수 있습니까?
- 솔루션이 가장 위험도가 높은 문제를 어떻게 식별하고 강조하는지 보여줄 수 있습니까?

위험 우선순위 지정 및 복구에 대해:

- 조사 결과를 어떻게 등급을 평가하거나 우선순위를 지정합니까? 심각도 또는 리스크 점수에 어떤 요소가 영향을 미칩니까?
- 다수의 조사 결과를 실행 가능한 수준의 대응 계획으로 전환하는 과정을 어떻게 지원하는지 보여줄 수 있습니까?
- 솔루션은 대응 및 해결 과정을 어떻게 안내합니까?
- 조사 결과를 적절한 팀 또는 담당자에게 할당할 수 있습니까?
- 인사이트를 데이터 보호 플랫폼과 원활하게 연계하여 더 나은 보안 및 복구 성과를 제공할 수 있습니까?

가치 실현 시간 및 구축 관련:

- 초기 구축 과정에서 우리 팀은 어떤 작업을 수행해야 합니까?
- 유용한 조사 결과를 얼마나 빨리 예상할 수 있습니까?
- 도입 후 30일, 60일, 90일 시점에서 각각 어떤 상태를 성공적으로 볼 수 있습니까?

주의해야 할 위험 신호

접근 위험에 대한 제한된 가시성

민감한 데이터에 대한 접근이 가장 큰 위험 요소입니다. 벤더가 누가(또는 무엇이) 데이터에 액세스할 수 있는지, 어떤 위험이 존재하는지 명확하게 보여줄 수 없다면 이는 심각한 한계입니다.

결과가 개별 비즈니스 위험 및 맥락과 연결되지 않습니다.

모든 비즈니스는 서로 다릅니다. 민감한 데이터나 노출된 지적 재산이 초래하는 위험은 해당 조직에서 무엇을 중요하게 여기는지에 따라 달라질 수 있습니다. 조사 결과는 학습된 맥락 정보와 분류 기준을 기반으로, 정확한 리스크 대응 권장 사항을 제공할 수 있어야 합니다.

사이버 레질리언스 성과와 데이터 리스크를 연결하지 못하는 경우

데이터 및 AI 리스크 상태를 최적화하는 것은 사이버 레질리언스 확보에 매우 중요합니다. 데이터 인텔리전스는 선제적 데이터 보안 전략의 방향성을 제공하고 더 나은 복구 성과를 지원하는 데 활용되어야 합니다. 조사 결과는 특정 부서에만 고립되어서는 안 됩니다. 특히 리스크 대응에는 여러 유관 부서 간의 협업이 필요한 경우가 많기 때문입니다.

가치는 과도한 수작업에 달려 있습니다

광범위한 조정, 해석 작업 또는 고객 맞춤형 프로세스 설계를 요구하는 제품은 지속적인 운영 비용과 복잡성을 증가시킬 수 있습니다.

벤더 비교 표

효과적인 DSPM 전략에 필요한 핵심 기능을 기준으로 벤더를 나란히 비교할 수 있도록 이 표를 활용하십시오. 각 항목을 검토할 때는 단순히 기능의 존재 여부뿐 아니라, 실제 환경에서 얼마나 효과적으로 제공되는지도 함께 고려해야 합니다*.

벤더 비교를 더 일관되고 객관적으로 수행하기 위해, 각 기능은 0~5점의 간단한 점수 체계를 사용해 평가할 수 있습니다. 이 접근 방식은 팀이 단순한 체크리스트식 비교를 넘어, 각 기능의 상대적인 강점, 성숙도, 실제 활용성을 평가하는 데 도움이 됩니다. 높은 점수는 해당 기능이 단순히 제공된다는 의미를 넘어, 엔터프라이즈 환경에 적합하고, 운영 효율성이 뛰어나며, 대규모 환경에서도 검증된 가치를 제공할 수 있음을 나타내야 합니다.

점수	정의
5	완전하게 구현되어 있으며, 높은 수준의 자동화·확장성·통합성을 갖춘 업계 최고 수준의 기능
4	견고한 기능성을 제공하며 일부 사소한 한계만 있는 우수한 기능
3	핵심 요구 사항은 충족하지만 깊이, 확장성 또는 사용성 측면에서 일부 제한이 있는 기능
2	눈에 띄는 기능 공백, 수작업 부담 또는 제한적인 적용 범위를 가진 기본적이거나 부분적인 지원
1	최소한의 기능, 초기 단계 기능 또는 매우 제한적인 지원
0	지원되지 않거나 유의미한 증거가 제공되지 않음

범주	벤더 1	벤더 2	벤더 3	참고
빠르고 에이전트 없는 배포를 위한 클라우드 네이티브 아키텍처				
규모와 속도에 맞춘 지속적인 데이터 탐지				
AI 기반 데이터 분류				
데이터 맥락화				
규제에 매핑된 위험				
적응형 접근 권한 제어 및 적용				
실시간 데이터 탐지 및 대응				
상황별 알림				
통합 복구 워크플로우				
데이터 보호 플랫폼과의 원활한 통합				
총계				

*점수 평가는 로드맵상의 계획이 아니라 현재 일반적으로 제공 가능한 기능을 기준으로 이루어져야 합니다. 각 점수는 제품 데모, 고객 레퍼런스, 문서, 구축 요구 사항, 그리고 통합 수준에 대한 검증 자료를 통해 확인되어야 합니다.

결론

DSPM 솔루션을 선택하는 일은 단순한 툴 선택 이상의 의미를 지닙니다. 그 대가는 너무 큽니다. 데이터는 놀라울 정도의 속도로 계속 증가하고 분산되고 있으며, 수작업 방식이나 레거시 기술로는 이를 따라갈 수 없습니다. 적합한 DSPM 솔루션은 가시성을 확보하고, 팀의 역량을 핵심 영역에 집중시키며, 위험을 줄이고, 데이터 보안과 사이버 레질리언스를 모두 강화하는 데 도움을 줍니다. 이 솔루션은 장기적으로 큰 가치를 제공할 것입니다. AI 모델, 시스템 및 에이전트를 뒷받침하는 데이터를 보호하고 안전하게 관리하는 데 도움이 되기 때문입니다.

당사의 DSPM 솔루션과 이것이 데이터 및 AI 위험 태세를 최적화하는 방법에 대해 자세히 알아보세요. 또는 지금 바로 저희에게 연락하십시오.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-KO 5-2026