DSPM # 보안상태관리 # 민감정보식별 # 데이터가시성

Fasoo DSPM
더 알아보고 싶다면?

Fasoo DSPM

차세대 데이터 보안 태세 관리

많은 기업 및 기관들은 확장성과 편의성, 비용적 이점을 찾아 멀티 및 하이브리드 클라우드 아키텍처를 도입하고 있습니다. 조직에서 사용하는 저장소가 다양해지고 데이터가 분산되면서, 데이터 유출의 가능성은 더욱 커졌습니다. 하지만 많은 조직들이 가장 중요한 클라우드 저장소 내 데이터의 보안 상태를 정확히 파악하지 못하고 있습니다. 이제는 클라우드 환경에서도 민감정보를 포함한 중요 데이터의 보안 현황을 파악할 수 있어야 합니다.
Fasoo DSPM (Data Security Posture Management)으로 사내 저장소의 보안 상태를 한 눈에 파악하고, 잠재적인 보안 위협을 최소화해 보세요.

제품 특장점

Fasoo DSPM은 멀티 및 하이브리드 클라우드를 포함한 다양한 저장소 내 데이터를 식별 및 분류해 보안 상태 현황을 제공합니다. 저장소 검사 및 모니터링으로 조직의 데이터 자산의 취약점을 분석하고, 보안 상태 유지를 위한 가이드라인을 지원합니다.

데이터 가시성 제고

대시보드를 통해 클라우드 저장소 내 개별 데이터의 암호화 상태, 접근 제어 활성화 여부 등 보안 상태 및 취약점을 파악하고 한 눈에 확인 가능

민감정보 검출 및 분류

관리되지 않는 다크 데이터와 섀도우 데이터를 포함한 정형·비정형 데이터에서 민감정보 검출 및 분류를 자동화해 중요 데이터 현황 파악

다양한 컴플라이언스 현황 제공

국내외 컴플라이언스 규정 준수 상태를 저장소 및 데이터 단위로 파악해 손쉽게 관리

FASOO

핵심 기능

직관적인 대시보드

- 각 저장소의 위치 및 민감 데이터 수량, 노출 위험 현황 등 다양한 정보를 한 페이지에서 확인 가능
- 인벤토리, 카탈로그, 검색 등 간결한 메뉴 및 편의 기능

보안 상태 스코어링 및 필터

- 저장소 보안 상태를 평가하고 위험도 순위 제공
- 컴플라이언스 준수, ACL 활성화 여부 등 보안 요소별 필터를 제공해 개별 스토리지 취약점 파악 가능

세부적인 정책 설정

- 저장소 단위 정책 생성, 수정, 삭제 가능
- 접근 권한 단위 일괄 정책 적용
- 각 컴플라이언스 규정 별 검출 정책 설정

활용 사례

금융권 활용 사례

도입 전

고객의 금융 정보와 거래 내역 등 개인정보가 지속적으로 저장소에 쌓이면서 관리 및 통제되지 않는 섀도우 데이터 등의 보안 취약점이 발생했습니다.

도입 후

데이터 저장소를 실시간으로 스캔해 중요 데이터를 발견하고 분류함으로써, 고객들의 민감 정보를 세밀하게 관리하고 유출 위험을 효과적으로 줄였습니다.

헬스케어 및 바이오 활용 사례

도입 전

생체 정보, 진료 기록 등 연구에 활용되는 의료 데이터가 백업, 사본 생성 등 다양한 원인으로 중복돼, 데이터의 일관성을 해치고 분석의 정확도를 저해했습니다.

도입 후

보유한 데이터의 위치와 민감도를 자세히 파악해, 중복 데이터를 식별 및 제거했습니다. 이를 통해 데이터 분석 결과의 신뢰도가 향상됐고, 클라우드 운영 비용도 절감하는 성과를 거뒀습니다.

법령/규제 대응 사례

도입 전

여러 클라우드 저장소에 분산된 데이터가 각각 어떤 컴플라이언스 규정을 위반할 위험이 있는지 정확하게 파악하기 어려웠습니다.

도입 후

저장소 및 데이터 모니터링 자동화를 통해 소수의 인력으로도 다양한 국내외 컴플라이언스 규정 준수 상태를 효율적으로 파악할 수 있게 됐습니다.

FASOO 서울 마포구 월드컵북로 396 비즈니스타워 6,17층 (상암동, 누리꿈스퀘어) (02) 300-9000 sales@fasoo.com www.fasoo.com