SOMANSA

GS인증(1등급) 보안기능확인서

Mail-i

28년간 시장 점유율 1위, 네트워크 DLP 솔루션

이메일, 웹, 메신저, P2P, 웹하드 등 네트워크를 통해 전송되는 정보를 기록, 통제, 관리하여
귀사 내 기밀정보, 개인정보 유출사고를 예방합니다.
특히 ChatGPT를 통한 기밀·개인정보 유출 차단 및 대화내역 기록하여 귀사의 정보자산을 보호합니다.

1 ChatGPT 사용 시 발생할 수 있는 보안위협 예방

2 네트워크를 통한 개인정보 유출 행위는 차단하고 기록하여 업무 생산성 향상과 정보보안 동시 준수 가능

① 내부기밀정보 유출 최소화
② 개인정보 유출 최소화
③ 생산성 향상과 기업리스크 간의 충돌 문제 최소화

주요 고객사

행정안전부
스마트워크 사업에 따른
네트워크를 통한 개인정보 유출 차단

고용노동부
가시성 확보를 위한
유해차단 구축사업

방위사업청
정보보안 체계 고도화
네트워크를 통한 기밀정보 유출차단

경기도교육청 GYEONGGIDO OFFICE OF EDUCATION
본청 및 25개 교육지원청
가시성 확보를 통한 유해차단 구축

LG전자
내부정보유출방지
및 비업무사이트 차단시스템 구축

LG유플러스
Network DLP 솔루션 구축
정보보안 시스템 고도화

SAMSUNG
웹DLP 구축 및
유해사이트 차단 솔루션 구축

신한은행
가시성 확보를 위한
유해차단 구축사업

KB 국민은행
웹서비스를 통한 유출차단,
제 1금융권 100% 이상 Mail-i 운영

ChatGPT를 통한 내부정보 유출차단
보안 5대 요구사항 만족

ChatGPT 사용 감사로그 확보

- 내부 지침에 따라 업무효율성과 정보보안을 동시에 준수할 수 있도록 업로드 행위 모두 기록
- 이용자, 이용목적, 이용일, 입출력 내용 기록 및 저장
- ChatGPT와의 대화기록 모두 저장하여 사후감사자료 활용
- ChatGPT-4 버전은 업로드 된 이미지도 모두 기록 및 저장하여 사후 감사자료로 활용

오남용 발생시 경보 및 차단

- 질의사항 안에 개인·기밀·신용정보 등이 포함된 경우 전송차단
- 주민번호, 운전면허번호 등 고유식별정보 포함 개인정보패턴 탐지 및 차단
  (운전면허번호 국내 유일 체크섬 보유)
- 대화에 특정 키워드가 포함된 경우에도 탐지 및 차단 (ex. 생산수율, 매출액, 핵심기술 등)
- 탐지·저장된 개인정보내역은 마스킹처리되어 2차 유출 방지

선별 통제 정책 (부서·시간대 등)

- 부서 또는 담당 업무 특성에 따라 ChatGPT 활용 차단/허용 가능
- 업무 상 ChatGPT 활용이 필요한 부서는 대화기록을 모두 저장하는 조건 하에 허용
- 시간대 별 접속통제 가능

감사로그 빅데이터 검색

- 3분내 초고속 검색 : 검색 DB방식대비 1천 배 단축
- 키워드 조건으로 검색 (ex. 생산수율, 예산, 대외비 등)
- 개인정보 패턴 및 반복횟수 기준으로 검색
- 부서, 사용자, 날짜, 허용/차단여부 기준으로 검색
- ChatGPT의 답변내용도 검색

ChatGPT 외 생성형 AI 서비스 차단

- ChatGPT, Gemini, Copilot 통제
- 이외 기타 생성형 AI서비스 또한 차단하여 정보 유출 예방 (2025.01, DeepSeek 선제적 차단 적용)