

WebKeeper AI DLP

생성형 AI 서비스를 통한 개인정보 유출방지 솔루션

WebKeeper AI DLP는 생성형 AI 서비스 활용에 따른

조직 생산성 향상 및 IT 신기술 부작용(정보유출, 무단전송)을 최소화하는 DLP 솔루션입니다.

내부자 실수에 의한 생성형 AI 서버로의 정보전송, 정보유출 채널로의 악용을 차단하여 귀사의 정보자산을 보호합니다.

WebKeeper AI DLP는 국민, 신한, 하나 등 5곳 은행에서 사용 중이며

국세청, 국가유산청 등 공공기관에서 선제적으로 도입, 안정화까지 완료하여 성능을 인정받았습니다.

N2SF 국가망 보안체계 '업무환경에서의 생성형 AI 활용'에 최적화된 제품입니다.

1 생성형 AI를 통한 개인정보 유출방지 솔루션

- 국내 기업의 67%는 생성형 AI 서비스를 통한 생산성 향상 효과를 실제로 경험했으나 **55%는 개인정보 유출, 보안관리 문제**로 생성형 AI 서비스 활용을 보류
- WebKeeper AI DLP를 통해 생성형 AI 서비스 통제 및 감사로그 확보가 가능하며 이를 통해 조직 생산성 향상을 극대화함과 동시에 IT 신기술 부작용을 최소화, 기술적 보호조치 구축 가능

2 29년 간 네트워크 DLP 시장 점유율 1위 기업 '소만사' 에서 선제적으로 개발

- 국내 최초 Secure Web Gateway & 내부정보 유출방지 일체형 솔루션 개발
- 혁신금융서비스 정책에 따라 국내 최초로 제1금융권에 생성형 AI 서비스를 통한 개인정보 유출차단 환경 구축 (제 1금융 5곳에 도입 완료)
- N2SF 시행에 따라 국가/공공기관 선제적으로 도입 및 안정화 완료

주요 고객사



생성형 AI 시스템
모니터링 프로젝트



생성형 AI NDLP
내부정보 유출방지 시스템 구축



직원 인터넷 구간
정보보안 인프라 재구성 사업



사설메일 및 메신저
로그저장 시스템 교체 사업



WebKeeper AI DLP
도입 사업

특장점



대화내역 메신저 형태로 기록

대화기록은
메시지형태로 저장하여
프롬프트, 전송정보 내역
모두 파악 가능



생성형 AI 서비스 선별통제

생성형 AI 차단 카테고리 제공
특정 생성형AI 서비스만 허용하고
나머지는 모두 차단하여
오남용 최소화



유해차단 + 네트워크DLP + 프록시 일체형 솔루션

단일 암호화웹 가시성 확보장비로
악성코드유입 및 정보유출을 통한
사내 정보자산 유출/변조에
모두 대응

기능



생성형 AI 사용 감사로그 확보, 사후감사자료 활용

- 이용자, 이용목적, 이용일, 입출력 내용, 파일 원본 등 기록 및 저장
- 생성형 AI 서비스와의 대화기록 모두 저장 (사용자 질의 및 생성형 AI 서비스 답변)
- 패킷은 구문분류(Parsing)되어 메신저 형태로 재현되어 비전문가도 감사자료 파악 용이



개인정보 전송 실시간 차단 (텍스트, 파일)

- 질의사항 안에 개인정보/기밀정보/신용정보 포함 시 전송차단
- 개인정보 : 주민번호, 운전면허 등 고유식별정보를 포함한 개인정보 패턴 탐지 및 차단
- 기밀정보 : 대화에 특정 키워드 포함된 경우 탐지 및 차단 (ex: 생산수율, 매출액, 핵심기술 등)
- 탐지 저장된 개인정보내역은 마스킹 처리되어 2차 유출 방지



전송파일 원본저장 및 빅데이터 분석

- 전송된 파일은 원본 저장되어 사후감사 자료로 활용
- 생성형AI 서비스를 활용하여 누적된 수백만 건 질의응답 로그 속에서 원하는 정보 3분 이내 검색
- 키워드, 개인정보패턴, 부서, 사용자, 날짜 등
다양한 기준으로 검색 가능하며 복합 검색 시에도 속도 저하 없음

상용화된 대부분의 생성형 AI 서비스를 통제합니다.

WebKeeper AI DLP의 생성형 AI 서비스 커버리지는 지속적으로 확장되고 있습니다.

