saltware

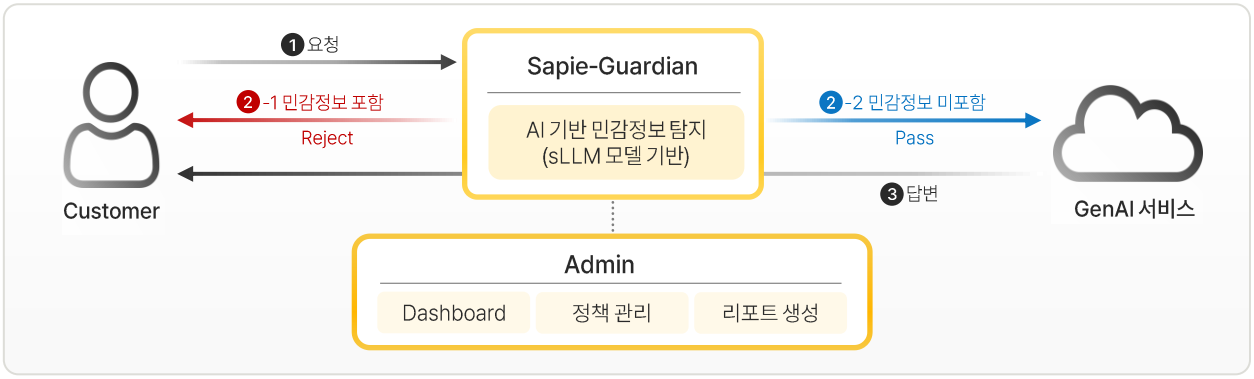
민감정보 유출 걱정 없는 안전한 AI 사용의 시작, 솔트웨어 Sapie-Guardian

Sapie-Guardian은 기업의 민감정보(개인정보, 기밀정보 등) 유출을 사전에 차단하는 AI 기반 보안 서비스입니다. ChatGPT, Gemini, Perplexity 등 생성형 AI 서비스 사용 중 발생할 수 있는 고객의 소중한 정보 유출을 자동으로 탐지하고 보호합니다.

01. 어떤 고객에게 필요할까요?

- 개인정보, 기밀정보, 영업비밀을 안전하게 보호하며 생성형 AI로 업무 생산성을 높이고자 하는 조직
- AI의 효율성은 인정하지만 데이터 유출 위험으로 안전한 활용 방안을 찾고 있는 조직
- AI를 이미 활용 중이지만 민감정보 유출을 실시간 차단·모니터링할 보안 솔루션이 필요한 조직
- 금융, 의료, 공공기관 등 개인정보보호법 관련 엄격한 규제를 준수하면서도 AI 도입으로 경쟁력을 강화해야 하는 조직

02. 어떻게 구성 되었나요?



※ sLLM: 경량화된 대규모 언어 모델 (smaller Large Language Model)

03. 어떤 특장점이 있나요?

다층 탐지 시스템

- 패턴, 키워드 기반 탐지
- 의미 및 문맥 기반 탐지(언어 모델)

실시간 차단

- 중요 정보 유출 전 실시간 차단

민감정보 탐지

- 다층 보안 탐지
- 학습 기반 고도화

모니터링

- 실시간 대시보드
- 허용 차단 이력 모니터링

통일된 전사 보안

- 중앙 정책 기반 전사 보안 적용
- 커스터마이징 지원

AI 보안 리포트

- 로그 기반 AI 사용 기록 추적
- AI 보안 리포트 자동 생성

© 2025. Saltware Co., Ltd. All Rights Reserved.

Sapie 서비스 문의 : csm@saltware.co.kr

04. 도입 시 어떤 이점이 있나요?

업무 혁신 및 생산성 향상

- 보안 걱정 없이 ChatGPT, Claude 등 최신 AI 도구를 자유롭게 업무에 활용
- 민감정보 검토·승인 프로세스 자동화로 업무 처리 속도 개선
- 중앙집중식 정책 관리로 일관된 보안 수준 유지 및 관리 부담 최소화

경제적 효과

- 데이터 유출 사고·과징금 리스크 원천 차단
- AI 보안 관리 업무 자동화로 시간 비용 대폭 절감
- 예상치 못한 보안 사고 대응·긴급 컨설팅 등 변동비용을 고정비로 전환

완벽한 리스크 관리

- 유출 사고로 인한 브랜드 이미지 실추 및 고객 신뢰 하락 방지
- 독점 정보와 영업기밀이 AI 학습 데이터로 활용되는 위험 차단
- 개인정보보호법, 정보공개법 등 국내 주요 규제 준수

05. 서비스 도입 절차는?

Step 1. 도입 협의 및 컨설팅

- 사용자 요구사항 분석 및 정의
- 도입 일정 및 단계별 계획 수립
- 민감정보 유형 및 보호 수준 요구사항 정의

Step 2. 제품 구축 및 테스트

- 고객 맞춤형 구축
- 시스템 연동
- 사용자 테스트 및 피드백

Step 3. 운영 및 유지 관리

- 운영 및 유지관리
- 운영 데이터 기반 보완 및 고도화
- 사용자 교육 및 가이드라인 제공

06. 지원 가능 모델 (예정)

ChatGPT　perplexity　Gemini

+ α

Claude　Copilot　기업 자체구축 LLM

© 2025. Saltware Co., Ltd. All Rights Reserved.

Sapie 서비스 문의 : csm@saltware.co.kr