

AI로 보안하고, AI를 보안하다.

AI는 기존의 개발 환경과 보안 패러다임을 완전히 바꾸어 놓았습니다.

생성형 AI와 LLM이 개발 워크플로우에 들어오면서 코드의 생산 속도와 양이 폭발적으로 증가했습니다.

기존의 보안 방식만으로는 빠른 개발 속도를 따라잡기 어려우며, 애플리케이션 보안 역시 완전히 새로운 접근법을 요구하고 있습니다.



01

달라진 보안의 대상

AI가 빠르게 생성한 소스코드는 수많은 보안약점을 안은 채 배포될 위험이 있습니다. 폭발적인 개발 속도에 부합하는 자동화된 보안 검증 체계가 필수적입니다.



02

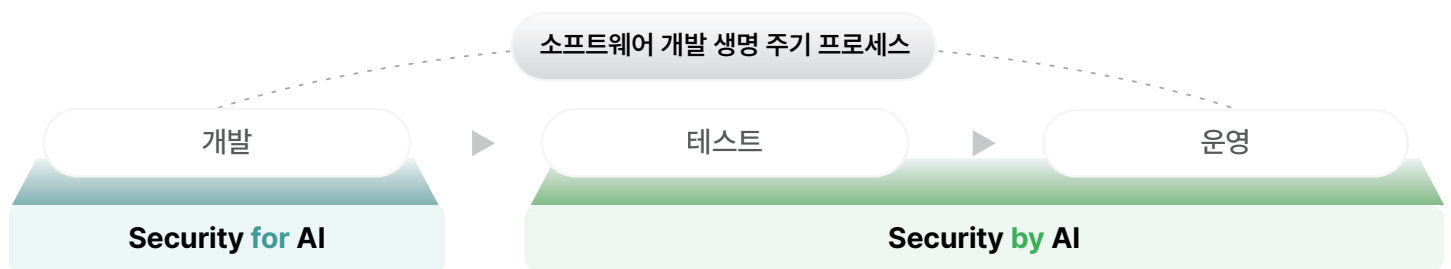
조치해야 할 수많은 이슈

취약점은 대량으로 쏟아지지만, '무엇부터 어떻게 조치할지' 판단하는 병목 현상은 여전합니다. 기존의 단순 룰 기반 방식으로는 조치 효율을 끌어올리는데 한계가 있습니다.

애플리케이션 보안은 이제, **AI가 만든 코드까지 보호**하는 동시에 **AI로 보안을 강화**해야 합니다.

스패로우는 AI를 두 가지 방향으로 활용합니다.

개발 단계에서는 AI 생성 코드의 보안을 강화하고, 테스트·운영 단계에서는 AI를 활용해 취약점 조치와 보안 운영 효율을 높입니다.
고객 환경에 맞춘 유연한 LLM 구성을 지원하며, 민감한 코드와 분석 데이터의 처리 경계를 환경에 맞게 분리합니다.



Security for AI

AI 생성 코드 보안 분석 자동화

AI 코딩 도구가 안전한 코드를 생성할 수 있도록 소스코드 및 오픈소스 분석이 가능한 MCP 서버를 연동하여 보안 테스트를 자동화합니다. 프롬프트 입력 단계부터 보안을 내재화하여 개발 생산성을 유지하면서 AI 생성 코드의 보안 리스크를 근본적으로 최소화합니다.

Security by AI

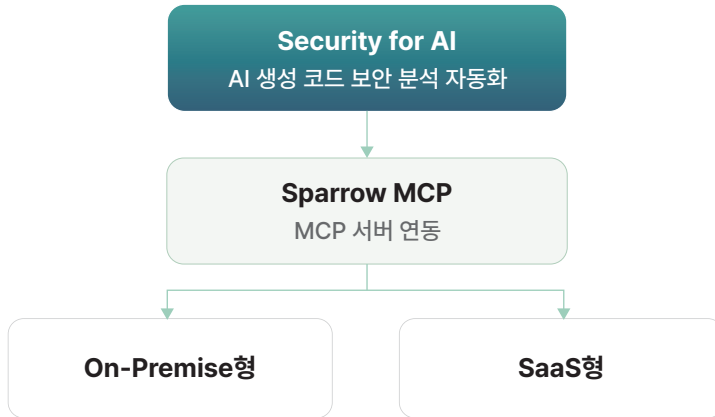
이슈 조치 강화 & 운영 효율 증대

AI가 검출된 취약점의 자산 중요도와 위험도를 종합 분석하여 맞춤형 조치 우선순위를 제시합니다. 또한 소스코드 분석 결과를 LLM과 연계해 탐지 근거를 구체화하고 정·오탐 판단을 뒷받침함으로써 보안 운영 전반의 효율성을 극대화합니다.

Security for AI

AI가 만든 코드까지 – AI 개발 워크플로우 내 보안 내재화

AI 개발 환경과의 연동을 통해 대화하듯 파일과 AI 생성 코드의 분석을 요청해 코드 안정성을 확보합니다.



보안 검증을 통한 코드 안전 확보

AI 개발 환경에서 코드를 생성하거나 수정할 때 즉시 보안 분석과 검증을 수행해 보안 리스크를 선제적으로 차단합니다.

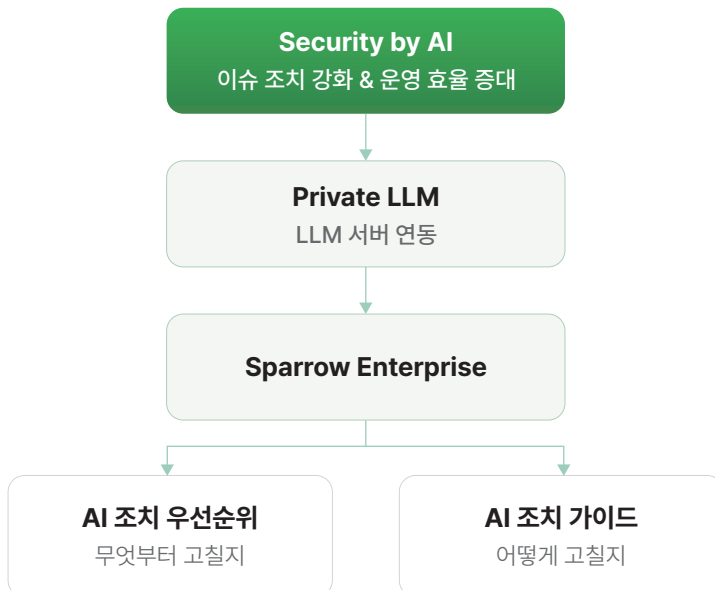
SW 공급망 보안

AI 생성 코드에 포함된 오픈소스 소프트웨어를 식별하고 SBOM을 생성해 SW 구성요소를 가시화합니다.

Security by AI

무엇부터, 어떻게 고칠지까지 – AI로 완성하는 보안 조치 자동화

'가장 중요한 취약점만, 가장 정확한 코드'로 탐색에서 조치까지 한 번에 해결합니다.



AI 조치 우선순위

AI가 자산 중요도와 위험도를 종합해 검출된 이슈의 우선순위를 자동으로 제안합니다.

AI 조치 가이드

AI가 소스코드의 수정 방법과 예시 코드를 제안해 개발자의 보안(수정/조치) 부담을 최소화합니다.

제품 라인업

Security for AI Sparrow MCP



브로슈어 다운로드

Security by AI Sparrow Enterprise AI Package



브로슈어 다운로드