SentinelOne

Prompt Security

기업 내 안전한 AI 생태계 조성 및 전사적 AI 거버넌스 체계 구축을 통해 진정한 AI 생산성을 경험하세요.

오늘날 보안 리더들은 AI 도입이라는 거대한 흐름 속에서 복합적인 보안 과제에 직면해 있습니다.

데이터 활용의 자율성과 보안 통제 사이의 균형이 무너지는 순간, 기업은 내부 정보 유출은 물론 모델 조작과 같은 치명적인 위협에 노출될 수 있습니다.

SentinelOne의 Prompt Security는 이러한 공백을 메우기 위해 설계되었습니다.

단순한 차단을 넘어 기업 환경에 최적화된 보안 가드레일을 구축하여 AI 활용의 전 과정을 투명하게 보호합니다.

이를 통해 조직은 보안에 대한 우려 없이 AI의 효용성을 극대화할 수 있으며, 탄탄한 보안 거버넌스 위에서 지속 가능한 기술 혁신과 비즈니스 성장을 실현할 수 있습니다.

안전한 기업용 AI 도입

도입 속도는 저해하지 않으면서, 모든 AI 애플리케이션과의 상호작용을 보호하여 조직의 리스크를 완벽히 차단합니다.

AI 기반 애플리케이션 보안 강화

자체 개발한 앱부터 통합 솔루션, 고객 접점 서비스에 이르기까지 모든 AI 기반 애플리케이션에 강력한 보안 및 거버넌스 체계를 구축하세요.

어디서나 안전한 데이터 보안

실시간 데이터 제어와 유연한 프라이버시 정책을 통해, 모든 AI 상호작용 과정에서 민감 정보 유출을 완벽히 차단합니다.

안전한 AI 혁신 가속화

자율형 에이전트부터 새로운 AI 공격 경로까지, 끊임없이 진화하는 위협에 선제적으로 대응하여 조직이 확신을 가지고 AI를 도입하도록 지원합니다.

Gartner
Peer Insights.

“

Prompt Security의 GenAI 플랫폼은 AI 관련 리스크에 대한 명확한 가시성을 제공하며, 통합 과정 또한 놀라울 정도로 간편했습니다. 실시간 모니터링과 정책 제어 기능 덕분에 생성형 AI 사용 환경을 더욱 자신 있게 보호할 수 있게 되었습니다.

★ ★ ★ ★ ★

BANKING, 50M-250M USD

Prompt:
A SentinelOne Company

Prompt Security가 해결하는 주요 AI 리스크

Shadow AI
미 승인된 AI 사용 현황을 식별하고 모니터링하여 보안 사각지대를 완전 제거

Prompt Injection
AI 모델 조작을 목적으로 설계된 악의적인 입력을 실시간 탐지하고 차단

민감 데이터 유출
기밀 정보나 규제 대상 데이터가 AI 도구로 유출되는 것을 방지

부적절한 LLM 응답
부적절하거나 유해한 내용, 브랜드 이미지에 반하는 AI 생성 콘텐츠로부터 사용자 보호

불안전한 에이전트
자율형 AI 에이전트에 보안 가드레일을 적용하여 대규모 자동화 환경의 안전을 보장

탈옥 및 프롬프트 유출
모델의 안전 장치를 무력화하려는 탈옥 시도나, 숨겨진 프롬프트를 탈취하려는 공격을 차단

서비스 / 비용 마비 공격
비정상적인 사용 패턴을 탐지 및 차단 하여 시스템 중단과 과도한 비용 발생 을 방지

Prompt for Employees
(직원을 위한 AI 가이드라인)

조직 구성원들이 Shadow AI, 데이터 프라이버시, 규제 위반에 대한 걱정 없이 안심하고 AI를 활용할 수 있는 환경을 제공합니다.

- **Observability:** 사내에서 사용 중인 모든 AI 도구를 감지하고 모니터링하여 섀도우 AI 리스크를 제거 및 위험도가 높은 앱과 사용자를 사전에 식별하고 관리
- **Data Privacy:** 자동 익명화 기술과 강력한 프라이버시 정책 적용을 통해 AI 사용 과정에서 발생할 수 있는 데이터 유출을 원천 봉쇄
- **Risk and Compliance:** 부서 및 사용자별로 세분화된 규칙과 정책을 수립하고 강제함으로써 법적·규제적 리스크를 철저히 관리
- **Employee Awareness:** 업무 흐름을 방해하지 않는 자연스러운 설명을 통해 직원들이 안전하게 AI 도구를 활용할 수 있도록 실시간 코칭을 제공

Prompt for AI Code Assistants
(AI 코드 어시스턴트 보안)

Copilot, Cursor와 같은 AI 기반 코드 어시스턴트와 연동하여 시크릿 정보를 보호하고 취약점을 상시 점검하며, 개발자의 생산성을 최상으로 유지합니다.

- **시크릿 및 PII 보호:** 코드 내에 포함된 인증 정보 (Secrets)와 개인정보(PII)를 실시간으로 감지하여 즉시 마스킹(Redact) 및 정제(Sanitize)
- **전체 가시성 및 거버넌스:** 전체 개발 주기 전반에서 AI 사용 현황을 추적하고 잠재적인 프라이버시 침해 요소를 식별하고 관리
- **폭넓은 호환성:** 수천 개의 AI 도구 및 어시스턴트와 통합 가능하며, 약 30개의 주요 프로그래밍 언어를 지원

Prompt for Homegrown AI Applications
(자체 개발 AI 애플리케이션 보안)

프롬프트 인젝션, 데이터 유출, 부적절한 응답에 대한 걱정 없이 자체 개발 애플리케이션의 강력한 AI 성능을 마음껏 활용하십시오.

- **AI 리스크 대응:** prompt injection, Jailbreak, Denial of Wallet, RCE 등 다양한 취약점으로부터 AI 앱을 보호
- **데이터 보호:** 자동 익명화 기술과 프라이버시 정책을 강제 적용하여, 민감한 정보가 외부로 유출되는 것을 원천 차단
- **콘텐츠 필터링:** 사용자가 LLM의 부적절하거나 유해한 답변, 또는 브랜드 이미지에 어긋나는 콘텐츠에 노출되지 않도록 방지
- **가시성 및 컴플라이언스:** AI 앱의 모든 인바운드 및 아웃바운드 트래픽을 기록하고 모니터링하여 운영 전반에 대한 완벽한 통제권을 확보

AI Red Teaming

제품 출시 전 Prompt injection, Jailbreak, Data Poisoning 등 잠재적 위협을 사전에 파악하십시오. 위험도 점수가 포함된 분석 결과와 조치 가이드를 제공하며, 개발 단계의 취약점 발견부터 실제 운영 환경(Runtime)의 보안까지 끊김 없는 통합 보호 경로를 구축합니다.

Prompt for Agentic AI
(Agentic AI 보안)

조직 내에서 운영되는 모든 AI 에이전트에 대해 실시간 가시성을 확보하고, 리스크 평가 및 정책 강제를 수행하십시오.

- **에이전트 및 MCP 탐지:** SaaS 앱, 데스크톱, 브라우저, 개발 도구 전반에 걸쳐 IT 부서 모르게 생성된 '섀도우 에이전트'를 포함한 모든 AI 에이전트와 MCP 서버를 탐지
- **지속적인 리스크 평가:** 권한, 행동 패턴, 데이터 접근 범위 등을 기반으로 리스크 점수를 동적으로 산출하며, 영향력이 큰 에이전트를 우선적으로 관리
- **보안 정책 강화:** 사용자·에이전트·작업별로 최소 권한 원칙(Least-Privilege)을 적용하여 CRM이나 금융 시스템, 데이터베이스에 무단 접근하거나 예기치 않은 연쇄 작업을 수행하는 것을 방지
- **감사 로그 기록:** 모든 AI 에이전트의 의사결정 과정과 수행 활동을 검색 가능한 기록으로 보존하여 컴플라이언스 준수 및 침해 사고 분석(Forensic)에 활용하도록 제공

About SentinelOne

SentinelOne은 세계에서 가장 진보된 사이버 보안 플랫폼입니다. SentinelOne Singularity™ 플랫폼은 '머신 스피드(Machine Speed)'의 압도적인 속도로 사이버 공격을 탐지, 방지 및 대응하며, 기업이 엔드포인트와 클라우드 워크로드, 컨테이너, ID(Identity), 모바일 및 네트워크 연결 기기 전반을 지능적이고 정확하며 간편하게 보호할 수 있도록 지원합니다. Fortune 10, Fortune 500, Global 2000 기업은 물론 주요 정부 기관을 포함한 11,500개 이상의 고객사가 내일의 안전을 위해 SentinelOne을 신뢰하고 있습니다.

UWS™
주식회사 유더블유에스
es@uws.co.kr / + 82 2 518 6291