Privacy-i EDR

차세대 안티바이러스 솔루션

소만사는 **<분석중심의 전통적 EDR 솔루션 한계>**를 극복하고
악성코드 선제적 차단에 집중하고 있습니다.
안티바이러스 엔진과 EDR행위기반 엔진을 모두 보유하고 있어 정교한 탐지가 가능합니다.
악성코드 분석력은 국내 제품 중 최상입니다.

1 전통적 엔드포인트 보안솔루션의 한계 극복

- 파일리스 공격은 악성코드의 시그니처가 탐지되지 않으므로 전통적 보안솔루션의 패턴기반 차단방식으로는 차단불가
- 랜섬웨어는 엔드포인트PC 감염으로 시작되며 행위기반 엔진으로 판단하고 실시간으로 차단하는 것이 확산을 막는 가장 효과적인 방식

2 파일리스 및 랜섬웨어 공격 실시간 탐지 선제적 차단

- 악성코드는 하루에도 수백건의 신 · 변종이 생성되므로 실시간 업데이트가 불가능함
- 패턴기반 엔진 단일 솔루션으로는 사내데이터를 온전하게 보호할 수 없음
- 발생 원인-결과를 중심으로 악성행위를 판별하는 EDR만이 보안위협을 실시간으로 탐지하고 선제적으로 차단할 수 있음

주요 고객사

2024 국가유산청 엔드포인트 단말 통합보안 솔루션 구축	2022 서울시설공단 공단 정보보호 강화 장비 도입	2021 성남시 Seongnam City 단말보안 고도화 구축
2024 시흥시 단말지능형 위협탐지 대응시스템 구축	2023 BGF리테일 임직원PC 랜섬웨어 보안솔루션 도입 구축 사업	2020 posco 포스코이앤씨 지능형 위협 대응 통합보안 구축 사업

악성코드 선제적 차단 자동화
보안담당자의 수작업 없이 패턴기반엔진, 행위기반엔진 단계별 전략을 통해 보안위협 발생 시 선제적 차단

경계선 보안 솔루션 역할 축소
클라우드 기반 근무환경 변화로 회사 내부망/외부망 경계 희미 EDR은 엔드포인트단에서 악성행위 스스로 탐지 후 차단

사이버 킬체인보고서 Mitre ATT&CK 프레임워크 적용
글로벌 프레임워크 기반 자동분석 악성여부 분석 및 탐지, 대응 자동화

사후 분석중심의 전통적 EDR 한계극복, 선제적 차단에 특화된 자동화솔루션

패턴 및 행위기반 엔진을 통한 악성코드 2단계 분석 (차단율 99.6%)

- 패턴기반 엔진으로 보안위협 필터링, 데이터베이스에 등록된 악성패턴과 대조, 탐지 및 차단
- 행위기반 엔진으로 실제 행위를 분석하여 악성여부 판단
  ① 취약점 공격선제차단
  ② 신종·변종/파일리스 공격 차단

실시간 격리 및 복구기능 탑재

- **실시간 격리 :** PC에 바로가기 파일이 저장되기만 해도 악성코드 포함여부를 탐지하고 격리
- **실시간 백업 복구 :** 이상행위를 빠르게 탐지하여 암호화 직전 최신 변경점까지 복구

세계 3대 악성코드 평가기관 <바이러스 불러틴> (Virus Bulletin) <VB100> 인증 최고등급 A+획득

바이러스 불러틴 VB100 테스트 결과	
10만 건 샘플 테스트	결과 (%)
오탐율	0%
탐지율	99.52%