개인정보·기밀정보 사전식별 솔루션
보안위협 발생시 중요정보 유출통제 및 악성행위 제어
엔드포인트 위협탐지 및 대응 솔루션

Privacy-i EDR V1.0

설치기간 최소 | 사전 식별된 개인·기밀정보 우선보호 | 악성행위 실시간 분석차단 | 머신러닝 기반 분석

SOMANSA

Privacy-i EDR 도입 필요성

신규 악성코드 생성
일 평균 390,000 개

이 중 알려지지 않은 악성코드가
기업을 공격하는 빈도는
시간 당 100개 이상

지능화된 악성코드는
안티바이러스, APT 솔루션 탐지 우회
엔드포인트에서
대량의 정보를 유출하거나 랜섬웨어 실행

엔드포인트 PC 감염,
보안사고 발생 후

해킹사실 인지에
소요되는
평균 시간
175일

해킹사실 인지에
2년이상
소요되는 기업
15%

해킹사고 원인을
파악하지
못하는 기업
55%

1차: 방어전략 — 2차: 탐지전략 — 3차: 대응전략

보안 위협
발생

Zero day exploit
Spam
APT
PowerShell
Ransomware

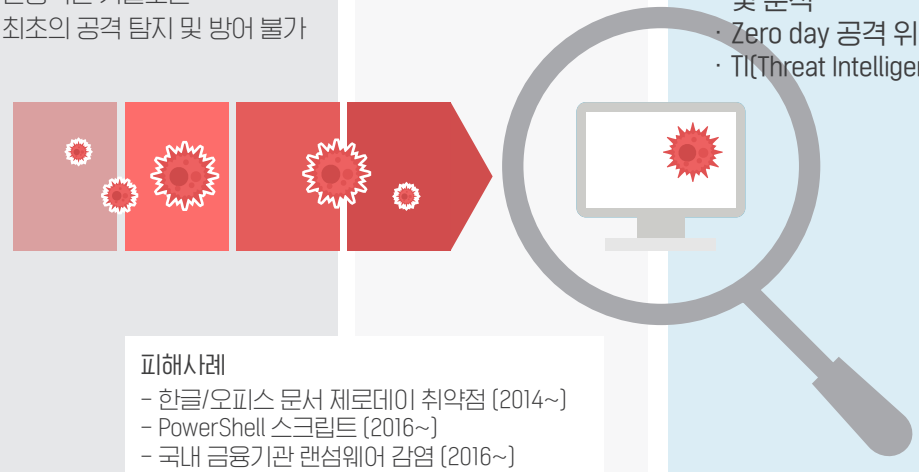
**기존
네트워크 및 엔드포인트
보안 영역**

시그니처 기반, 샌드박싱 등
전통적인 기술로는
최초의 공격 탐지 및 방어 불가

**엔드포인트
감염·실행·상주 등
악성행위를 통한
실제 데이터 수집**

EDR 탐지 및 대응 영역

- 실제 데이터를 통한
  이상행위 탐지 및 대응
- 사후 조사(Investigate)
  및 분석
- Zero day 공격 위험 감소
- TI(Threat Intelligence) 공유



피해사례
- 한글/오피스 문서 제로데이 취약점 (2014~)
- PowerShell 스크립트 (2016~)
- 국내 금융기관 랜섬웨어 감염 (2016~)
- 제조사 AD 서버 침해 (2018~)

Privacy-i EDR은
백신을 우회하는 위협을 탐지하고
실시간으로 공격에 대응할 수 있는
차세대 엔드포인트 보안 솔루션입니다

Privacy-i EDR 특장점

DLP + EDR

경량화된 통합 에이전트 활용

▶ EDR(Endpoint Detection & Response) & DLP(Data Loss Prevention) 기능을 동시에 제공할 수 있는 단일 에이전트
▶ Privacy-i의 데이터 분류 기능으로 **파일의 중요도에 따라 대응의 우선 순위 지정** (예: 고객정보 유출 > 개인 파일 유출)
▶ CPU, Memory, Disk 영향 최소화
▶ 에이전트 간 충돌 이슈 최소화 및 대응 지원

공격 요소 통합 분석

딥러닝 기반의 '공격관련 모든 요소' 통합 분석

▶ API 실행정보: API/ Arguments
▶ 커널이벤트: · 프로세스 · 파일
· 네트워크 · 레지스트리 · 모듈
▶ **딥러닝**을 통해 복잡한 이벤트 상관관계 추적, 탐지, 대응

Threat Intelligence (TI)

클라우드기반 TI 플랫폼을 통해 알려지지 않은 위협 적시대응

▶ 의심스러운 대상에 대하여 상위 서버로 악성여부 조회
▶ **각 구축사를 통해 수집/공유된 정보**를 토대로 악성여부 조회
▶ Global Threat DB 연동하여 탐지범위 확장

시각화

공격관련 세부정보 시각화

▶ 공격과 관련된 요소(프로세스, 네트워크, 파일 등)들을 자동으로 연결
▶ Timeline을 통해 공격 진행상황에 대한 세부정보 제공
▶ **대시보드를 통한 탐지 및 대응** 현황/추이 파악
· 위협정보(탐지/대응) · 엔드포인트 현황
· 경보 현황/종류 등 · 프로세스/네트워크/파일 등 정보

경쟁사 대비 비교

기능	Privacy-i EDR	타 EDR 솔루션
EDR 적용기간	기존 Privacy-i 에이전트 업그레이드만으로 설치 기간 최소화	EDR 전용 에이전트 배포와 안정화에 6개월 이상 소요
데이터 보호능력	사전에 식별된 주요 기밀/개인정보 파일 보호에 집중	(지원 불가)
네트워크 차단과 연계	자사 네트워크 차단 솔루션(WebKeeper) 연계	(지원 불가)
데이터 유출 통제와의 연계	DLP(Data Loss Prevention) 내재화	(지원 불가)
비용대비 효과	높음	고가의 도입비용
TI(Threat Intelligence) 적용	O	O
악성코드 실시간 행위 분석 및 차단	O	O
머신 러닝 기반 악성행위 분석	O	O

소만사는 DLP & 악성코드 차단 전문기업 입니다

Privacy-i

2008
컨텐츠 인식·분석
Endpoint
Data Loss prevention

2013
빅데이터(로그)
검색 엔진 탑재

2014
국내 에이전트 설치
100만개 이상

2016~2017
Forrester Research
Top 7 컨텐츠 분석 DLP
Gartner Magic Quadrant
Top 10 DLP

WebKeeper

2009
국내 최초 악성코드 배포사이트
및 유해사이트 차단 솔루션 출시

2012
WebKeeper 1,000 개 고객사 확보
CTAS, Virus Total 등
공신력있는 악성코드 DB 확보
악성코드 분석 전문팀 운영

2016
연간 2천만건 이상의
악성코드 보안업데이트

Privacy-i EDR

2019
Endpoint 보안 통합 에이전트 출시
Endpoint Detection & Response
Endpoint Data Loss Prevention

- 경량화된 통합 에이전트로 DLP + EDR 정보 연동 및 분석
- 국내 100만개 에이전트로 국내 최다 악성 행위 정보 수집 능력 보유
- 웹키퍼 Secure Gateway와 연동하여 악성코드 다운로드 및 악성 IP 접속 차단, 패킷상 그레이 파일 수집 및 탐지

Privacy-i EDR 제품사양

제품명	Privacy-i EDR 100	Privacy-i EDR 500	Privacy-i EDR 700	Privacy-i EDR 1000
사용범위	~ 300 Users	~ 500 Users	~ 1,000 Users	~ 3,000 Users
사양	· Intel® Xeon® QuadCore 1CPU · RAM 32GB over · HDD 1TB over	· Intel® Xeon® OctaCore 1CPU · RAM 32GB over · HDD 1TB over	· Intel® Xeon® OctaCore 2CPU · RAM 64GB over · HDD 1TB over	· Intel® Xeon® DecaCore 2CPU · RAM 64GB over · HDD 2TB over
특이사항	-	· 전원 이중화 · 기타 Raid 옵션 지원		
이미지				

*본 사양은 사전 예고없이 변경될 수 있습니다.

▶ 과학기술정보통신부지정 지식정보보안 컨설팅전문업체
▶ 신용평가등급 A, 재무안정성 상위 1%
▶ 행정안전부지정 개인정보 영향평가기관
▶ 창립 이래 무차입경영, 17년 연속 흑자기업
▶ 조달청 조달등록기업

서울특별시 영등포구 영신로 220 KnK디지털타워 9층
TEL 02)2636-8300 FAX 02)2636-8181 www.somansa.com

초판 제작: 2019.11.11