



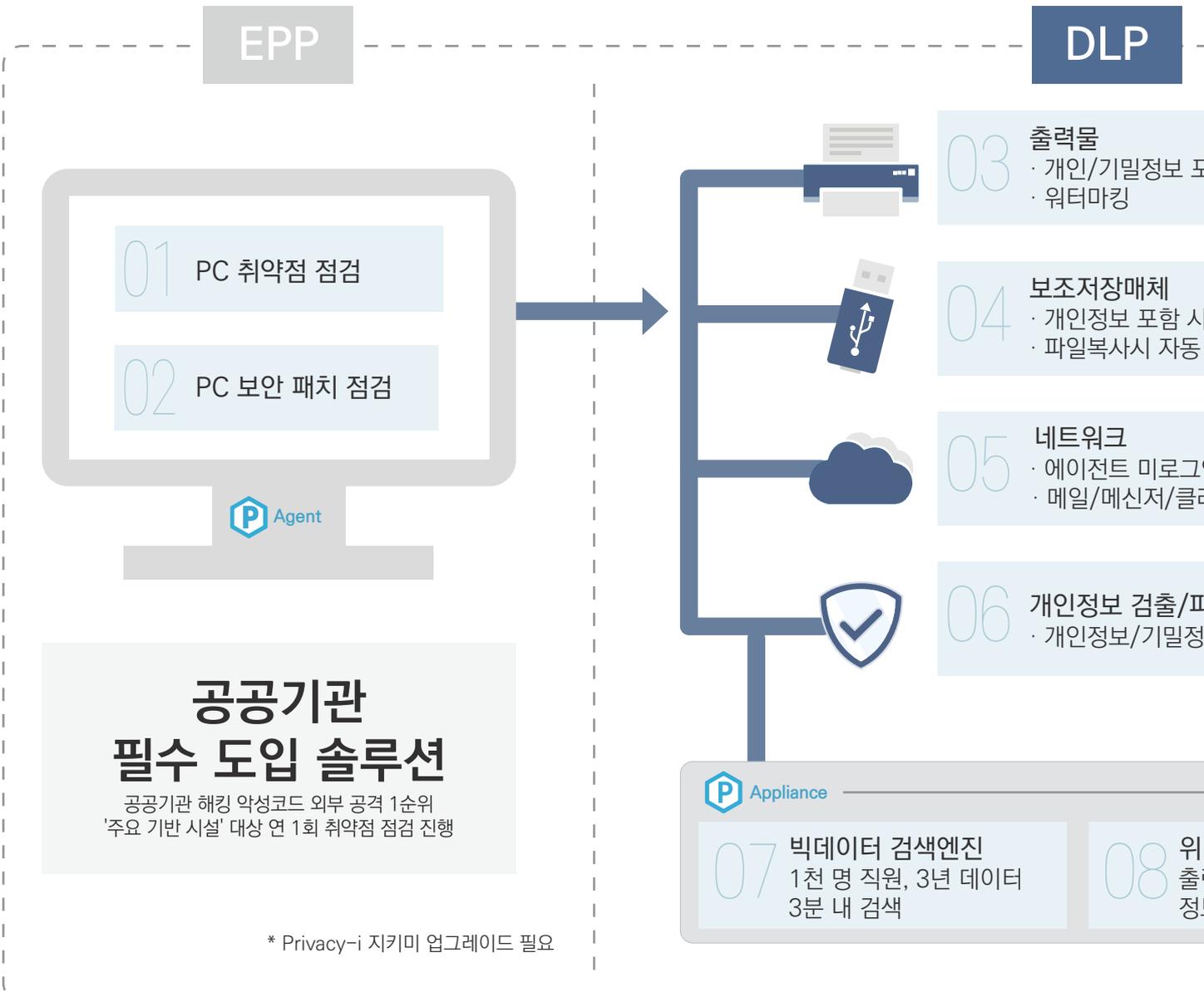
Privacy-i

시장 1위
엔드포인트 DLP 솔루션



 SOMANSA

Privacy-i 하나로 10여 개 보안 기능 통합, 생

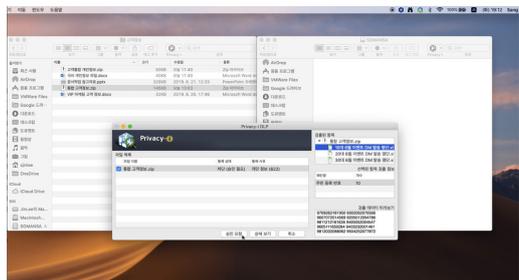


* Privacy-i 지키미 업그레이드 필요

맥OS, 리눅스(개방형 OS 포함) 전용 에이전트 지원

기존 윈도우 에이전트와 동일한 DLP, Discover 기능 제공

- 개인정보 검출, 파기, 암호화
- 이동식 저장장치, 프린터, 네트워크 전송 통제
- 미디어 통제 (카메라, USB Hub/젠더, AirDrop 등)
- 웹콘솔에서 Windows, 맥OS, 리눅스 에이전트 일괄 통합 관리



싱글 에이전트

EDR

포함 시 유출차단

Drag& Drop 차단
암호화

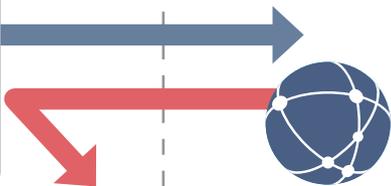
인 시 접속차단
클라우드를 통한 유출 차단통제

악기 및 암호화
보 파일 보유 현황 통제

EDR 탐지 및 대응 영역

- 09 TI(Treat Intelligence)
 - 글로벌 데이터 실시간 업데이트 및 배포
- 10 패턴기반(안티바이러스) 엔진
 - 정적분석을 통한 바이러스 탐지 차단
- 11 행위기반 동적분석 엔진
 - 랜섬웨어, 신변종바이러스, 파일리스어택, 제로데이 대응
- 12 인공지능 딥러닝
 - 고도화된 악성코드 분석대응

변조방지 스토리지
기록물, 반출 파일, 본문 등
보 반출 기록 및 원본 보관



탐지 일시	탐지 대상	탐지 유형	탐지 결과	탐지 위치	탐지 내용
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨
2024.10.10.10:10:10	192.168.1.100	악성코드 탐지	탐지됨	C:\Program Files\Internet Explorer\iexplore.exe	트러스트로 등록된 악성코드 탐지됨

* Privacy-i EDR 업그레이드 필요

외산 대비 성능 4배 '프라이버시 슈퍼엔진'

엔드포인트에서 발생하는 보안위협행위 탐지, 개인정보 분석속도 4배 개선

- 초기대비 3~10배 개선
(500TB 스토리지서버 확인 시 소요시간 5배 단축)
- 고유식별정보 등 서버 내 개인정보파일 분석 속도 개선
- 정규표현식 패턴의 탐지를 위한
아호코라식 오토마타 구축 장치 및 방법 적용



[자체 개발 주도 및 특허 보유]

Compliance 개인정보보호법 모든 공공기관, 기업, 단체에 적용 (2024.3.15 시행예정)

조항	내용	법규준수기능
21조 (파기)	① 개인정보 유효기간 만료, 처리목적 달성 시 지체없이 파기 ② 복구/재생되지 않도록 파기조치	· 맥OS, 윈도우 기반 PC에서 개인정보 검출→파기
24조 (고유식별정보 처리제한)	③ 고유식별정보 처리 시 암호화 등 안전성 확보조치 구축 ④ 행안부가 공공기관, 5만명 이상 고유식별정보처리자 대상으로 고유식별정보에 <안전성 확보에 필요한 조치>적용여부 격년조사	· 맥OS, 윈도우 기반 PC에서 개인정보 검출→암호화 · 고유식별정보 포함파일 보유현황 파악 · 고유식별정보 외부반출 통제/기록
24조의2 (주민등록번호 처리제한)	② 개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손(이하 유출)되지 아니하도록 암호화 조치를 통해 안전하게 보관	· 주민등록번호 포함 파일 보유현황 파악 · 주민등록번호 외부반출 통제/기록
32조 (개인정보파일 등록 및 공개)	공공기관에서 개인정보파일을 운용하는 경우 개인정보 파일명칭, 운영근거/목적, 개인정보 항목, 처리방법, 보유기간, 제공받는 자, 정보주체 수 등을 운용시작일로부터 60일 이내 보호위에 등록	· 보호위가 요구하는 개인정보 파일 운용 시 등록사항 기록
34조 (유출통지)	① 유출 인지 시 지체없이 해당정보주체에게 통지 (유출된 개인정보항목, 유출시점, 경위 등)	· 개인정보 외부반출시 경로, 시점, 항목, 보내는 이, 원본파일 모두 저장
34조의2 (과징금 부과)	① 개인정보처리자가 처리하는 주민등록번호가 유출된 경우 5억원 이하의 과징금을 부과·징수. 단, 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우 예외	· 개인정보 파일 암호화, 유출방지기능을 통해 고시 준수
39조 (손해배상책임)	고의 or 과실로 개인정보 유출시 ② 정보주체에게 손해가 발생한 때 손해액의 5배 내에서 손해배상	· 개인정보 파일 암호화, 유출방지기능을 통해 고시 준수 및 손해배상책임위험 사전예방
39조2 (법정손해배상)	고의 or 과실로 개인정보 유출시 ① 300만원 이하 손해배상	
64조의2 (과징금 부과 등에 대한 특례)	② 개인정보의 기술적, 관리적, 물리적 조치를 취하지 않은 상태에서 개인정보가 유출된 경우 위반행위 전체 3%이하 과징금	
74조의 2 (몰수 추정)	민감정보, 고유식별정보에 <안전성 확보에 필요한 조치>를 하지 아니하여 유출 시 위반행위로 취급한 금품 및 이익을 몰수	· 민감/고유식별정보 포함 파일암호화, 유출방지기능을 통해 고시 준수
75조 (과태료)	② 3천만원 이하 과태료 4. 처리목적이 완료, 보유기간이 지난 개인정보를 파기하지 않은 자 5. 민감, 고유식별, 개인정보에 관한 안전성 확보조치를 취하지 않은 자 8. 주민등록번호를 암호화하지 않은 자	· 맥OS, 윈도우 기반 PC에서 개인정보 검출→암호화 · 개인정보 파일 암호화, 유출방지기능을 통해 개인정보보호법고시 준수

인증



엔터프라이즈 DLP
Magic Quadrant 2년 연속 등재



DLP분야 10대기업
Vendor Landscape 등재



아시아 유일
엔드포인트DLP 4.5 Rating



CC인증



보안기능확인서



GS인증

강점 01 국내 최대 개인정보 검출 커버리지 확보

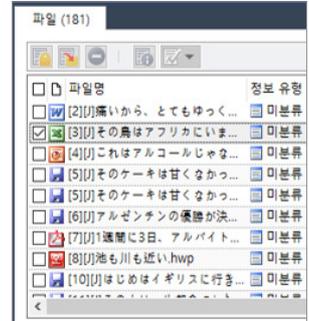
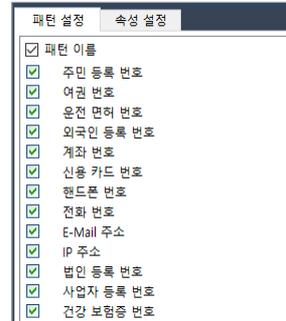
고유식별정보

(주민번호, 운전면허번호, 여권번호, 외국인번호),
카드번호, 계좌번호 등 13종 이상 개인정보,
미국, 유럽연합, 일본 등 해외 컴플라이언스 패턴
분석 및 개인정보유출 차단

※ 2020.10월 주민등록법 개정에 따른
'변경된 주민번호 패턴' 검출 지원

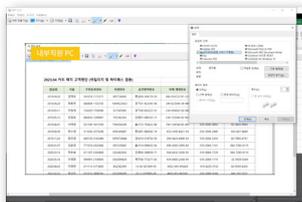
다국어 파일명/컨텐츠 내에서도 개인정보 패턴검출

DRM, 다단계 압축파일, 확장자 변조 탐지 차단



강점 02 이미지파일 내 개인정보 검출 및 통제 (OCR)

이미지 파일 출력 시 출력물 내 개인정보패턴 분석 및 로그 저장



개인정보가 포함된
이미지 출력 후
OCR 서버에서
분석 및 로그 저장



- 개인정보가 포함되어 있는 스캔 파일
(예: 주민등록등본, 카드 신청서, 대출 신청서 등)
기존 DLP솔루션이 분석할 수 없는 이미지 내
개인정보 분석 및 검출내역 로그 저장
- 이미지 내 텍스트는 전용 OCR 서버에서
추출되어 DLP 서버에서 개인정보 포함 여부 분석
- 관리자 페이지에서 파일명, 개인정보패턴
종류 및 개수, 파일 보유 직원정보, 출력일자 확인가능

강점 03 사용자 관점 로그 검색 및 리포트

웹기반 콘솔 DLP + CENTER

단말, 브라우저 제한없이 웹기반 관리자 페이지에서
사내 중요파일 및 에이전트 일괄관리

사용자 관점에서 리포트/보고서 산출

부서/사용자/패턴별 리포트,
개인정보 보호현황 대시보드

원본 파일 로깅

포렌식 관점에서 유출데이터 100% 구현
법적 증거자료/감사자료 확보, 책임소재 추적



Best Practice

1천여 고객사에서 27년 동안 축적/개발한 엔드포인트 보안기술



12만 유저
개인정보보호 및 유출방지



국내S사 E제품 원백
15만 유저 개인정보 유출방지



3만 유저
PC 개인정보보호 및 유출방지



공공

에이전트 도입대수 1위
광역시/도 교육청
제품 도입 1위

금융

주요 금융사에 도입·운영중
S사 등 외산 솔루션
원백 사례 다수 확보

기업

메이저 제조·통신·서비스
기업 고객사 보유
모기업, 계열사 및 해외법인에서
운영중