SOMANSA

GS인증(1등급)

Server-i

시장점유율 1위, 금융권 도입 80%, 구축 서버 누적 5만 대 이상
서버, DB 개인정보 검출 서버 DLP 솔루션

대규모 해킹 사고는 대부분 서버 침투로 시작됩니다. 찰나의 작은 틈으로 침투한 공격자는
관리가 미흡한 서버 안에 무방비 상태로 방치된 개인정보를 1순위로 노립니다.
기업 · 기관은 사전 현황 점검을 통해 개인정보 보유를 최소화하여 개인정보 유출사고를 사전에 차단해야 합니다.
Server-i는 약 5만 대 서버에 구축된 제품입니다. 클라우드를 포함한 상용화된 모든 서버 플랫폼을 지원합니다.
제 1금융, 민간 대기업, 광역시도 지자체 레퍼런스를 통해 검증받은'이식성 보안성 안정성'을 귀사에도 적용하실 수 있습니다.

1 서버 데이터 유출사고 피해 최소화

- A사 75억 과징금, B사 1,300억 과징금 부과
  개인정보 유출사고의 원인은 해커의 서버 공격에 의한 서버침투 및 개인정보탈취
- Server-i는 서버 내 방치된 개인정보파일에 대한 주기적인 점검 실시하여
  개인정보 검출 및 삭제, 암호화 등의 보호조치 진행, 개인정보 보유 및 유출사고 피해 최소화 실현

2 개인정보보호법 준수 솔루션: 징벌적 과징금 부과 예방, 손해배상소송 최소화

- 기술적 조치를 취하지 않아 개인정보 유출시 전체 매출 3% 과징금 (주민번호는 5억원 과징금)
  Server-i는 전자금융거래법, 신용정보법, 개인정보보호법 준수로 집단소송 · 법적처벌 가능성 최소화
- 고시 미적용으로 개인정보 컴플라이언스 위반 시 ① 5천만원 이하 과태료 (DMZ 구간 내 검출)
  ② 매출액 3% 징벌적 과징금 or 손해배상 소송 피해액 5배 ③주민번호 유출시 과징금 5억원 부과

주요 고객사

서울특별시
본청 보유서버 내부자산 식별
및 데이터보호

경기도
본청 보유서버 내부자산 식별
및 데이터보호

우리은행
본행 보유서버 내부자산 식별
및 데이터보호 (클라우드 포함)

하나은행
본행 보유서버 내부자산 식별
및 데이터보호

신한은행
본행 보유서버 내 개인정보
검색 시스템 구축 및 데이터보호

국내 최다 레퍼런스 확보
5만 대 서버에서
성능 및 안정성 입증

상용화된
모든 서버 플랫폼 지원
리눅스 기반 서버 호환
유닉스/윈도우 중요서버 호환

클라우드 내
개인정보보호
선제적 개발 및 적용

AWS S3, Azure, 퍼블릭 환경 호환
NHN, Naver, KT, 스토리지 호환
GitLab, GitHub 내
개인정보 검출지원

서버·DB 개인정보 검출,
취약점 점검
통합 서버보안 솔루션

서버·DB 내 개인정보검출부터
취약점 점검까지
서버내에서 발생할 수 있는
모든 보안위협 예방

* 취약점 점검은 별도 라이선스 필요

데이터 보호관점에 기반하여 개인정보 유출, 파괴, 변조행위를 차단하는 통합 서버보안 서비스 제공

개인정보 검출 : 서버·DB 내 자산현황 파악

- 13종 이상 개인정보 패턴 분석/통제
  국내유일 고유식별정보 2종 (주민등록번호, 운전면허번호), 제 1금융권 8곳 계좌번호 체크섬 보유
- EU (GDPR준수), 북미, 중남미 국가 개인정보 패턴보유 글로벌 컴플라이언스 대응 가능
- 이미지 파일 내 개인정보 탐지 검출 (OCR/ FFR)
- 서버별 접근권한 관리 기능으로 담당서버 관리자에게 권한 차등 부여하여 오남용 방지

삭제/암호화 : 보유자산 최소화를 통한 유출사고 피해 최소화

- 검출완료 내역 토대로 파일삭제 또는 암호화 수행, 필요한 정보는 원격 암호화하여 보호
- 검출된 개인정보는 마스킹 처리 (2차 유출 예방)
- 유효기간 만료 불필요한 정보는 원격삭제 (보유자산 최소화 실현)

서버 담당자 관점 서버 개인정보 관리

- 수백, 수천개의 서버를 보안 담당자가 모두 관리하는 것은 보안 담당자의 업무 과부하 초래
- 보안 담당자가 서버 담당자를 직접 지정하고 전담 서버의 권한 부여,
  서버 내 개인정보 보유 현황 관리하도록 하여 보안 담당자의 업무 부담 최소화

SOMANSA

GS인증(1등급)

Server-i 지키미

서버 취약점 & 데이터 리스크 탐지 대응 솔루션

가장 기본적인 악성코드/랜섬웨어 차단법은 서버 내 보안 취약점을 미리 제거하는 것입니다.
Server-i 지키미는 보안위협 및 취약점을 사전에 진단하여 해커의 공격을 예방하고,
악성코드 및 랜섬웨어 감염위험으로부터 귀사의 정보자산을 보호합니다.
Server-i 지키미는 서버 내 취약점을 자동으로 점검하며 즉각적인 분석결과와 효과적인 대응 방안을 제공합니다.
이를 통해 기존 수작업 중심 점검방식의 한계를 해소하고 효율적인 보안 관리를 가능하게 합니다.

1 랜섬웨어 감염양상의 변화 : 단순 PC감염에서 서버감염으로 확대

- 서버에는 개인정보, 인증정보, 기밀문서 등이 집중보관되어 있어
  유출 시 PC감염보다 더 큰 피해를 초래할 수 있음
- 라자루스, 안다리엘, 솔트타이푼 등 국가단위 해킹그룹의 인프라 공격이
  지속 증가함에 따라 가장 기본적인 랜섬웨어 예방법인 '취약점 제거'의 중요성이 강조됨

2 수작업 중심 취약점 점검행위 비효율성 해소 : 서버 및 보안담당자 업무부담 최소화

- 공공기관은 '주요기반시설' 연1회 점검,
  금융기관은 '전자금융기반시설' 연1회 점검 필수 (평균 수십~수천대 보유)
- 점검 전용 솔루션 미도입 기관의 경우, 담당자가 수작업으로 서버별로 스크립트를 업로드하여
  점검을 수행해야하므로 업무부담 최소화를 위해 반드시 전용 솔루션 도입이 필요함

주요 고객사

서울특별시
본청 보유서버 내부자산 식별
및 데이터보호

경기도
본청 보유서버 내부자산 식별
및 데이터보호

우리은행
본행 보유서버 내부자산 식별
및 데이터보호 (클라우드 포함)

LG U+
본사 보유서버 내부자산 식별
및 데이터보호

kt
IDC 내 서버보호, 국내 초대형 규모
DBMS 서버팜 대상 약 10,000여대

* 'Server-i'는 서버 개인정보보호 솔루션으로 시작되었으며, 현재는 서버 백신 및 취약점 점검기능까지 확대되었습니다.
소만사는 서버 싱글 에이전트를 통해 고객의 정보자산을 보호하고 있습니다.

특장점

서버 싱글에이전트 (DLP, AV, 지키미)

단일 에이전트로
서버 취약점 점검, 개인정보 검출,
유출차단, 악성코드 탐지 실현
에이전트 업데이트 하나로
도입가능

단일 패키지 통합관리

하나의 패키지를 통해
리눅스·유닉스·윈도우
플랫폼 제한없이
서버 OS·버전 상관없이
통합관리

국내 및 글로벌 진단항목 DB 보유

주요정보통신 기반시설
취약점 평가기준(DBMS/서버),
글로벌 외부전문 취약점 점검
등 컴플라이언스에서 권고하는
보안사항 준수

기능

직관적 리포트 : 상세 리포트를 통해 서버 보안현황 파악

- 전체서버 점검현황 및 진단수준 단일 페이지 내 요약안내, 전사적 점검 진척도 제공
- 서버 점검결과 상세확인을 통해 제공된 권고기준 토대로 취약점 조치 수행
- 진단결과는 엑셀파일 형태로 제공되며 내부지침에 적합한 형식으로 가공 가능

서버 관리자 배정 기능 : 서버별 독립적 관리

- 보안담당자는 서버관리자의 전담서버 점검권한을 부여하여
  할당된 그룹만 점검할 수 있도록 설정
- 서버관리자의 전담서버에 대한 책임소재를 명확하게 부여하여 히스토리 관리
- 서버 데이터/관련업무에 해당하는 컴플라이언스 기준에 따라 점검 진행

취약점 DB 실시간 업데이트

- 법률개정, 항목 업데이트 등 취약점 점검항목 변경시 실시간 업데이트
  (금융감독원, 과학기술정보통신부, 한국인터넷진흥원)
- 솔루션 도입기관에서 보안허점/공백 없이 최신 점검 항목으로 실시간 점검할 수 있도록 지원

BPFDoor 악성코드 확산 방지 및 피해 최소화 실현 (S사 유출사고 재발 방지)

- BPFDoor 악성코드는 은닉성이 강해 포트 스캐닝 방법으로는 검출이 어려움
- Server-i 지키미는 특정 프로세스가 오픈한 소켓 및 특정 패턴을 가진 소켓,
  파일패턴 매칭 등을 검사해 BPFDoor 악성코드 감염여부를 판단, 사전 예방