# Server-i

개인정보 유출방지
취약점 자동점검
리눅스 서버백신

SOMANSA

## 시장점유율 60%, 3만 대 이상 서버에서 검증
## 시장 1위 〈서버 보안 솔루션〉

서울특별시, 경기도청, 충청남도청, 대검찰청, 우정사업본부, 헌법재판소, 사회보장정보원, 한국수력원자력, 한국동서발전, 한국서부발전, 한국중부발전, 한국마사회, 한국철도공사, 한국도로공사, 한국무역공사, 한국주택금융공사, 공무원연금공단, 국방연구원, 서울시설공단 외

하나은행, 신한은행, 우리은행, IBK기업은행, 수협중앙회, 새마을금고중앙회, 삼성증권, 하이투자증권, 하나카드, 신한카드, 삼성카드, 현대카드, 비씨카드, 신한생명보험, 라이나생명, 동양생명보험, KB손해보험, 롯데손해보험, AIG손해보험, 삼성화재, KB증권 외

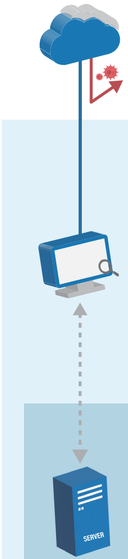
삼성전자, 삼성엔지니어링, 삼성SDS, 호텔신라, KT, LGU+, CJ대한통운, GS칼텍스 외

**서버 개인정보검출 국내최초 CC인증 획득** (Server-i V3.0 HyBoost EAL2등급)


- ▶ 과학기술정보통신부지정 정보보안 컨설팅전문업체
- ▶ 행정안전부지정 개인정보 영향평가기관
- ▶ 조달청 조달등록제품
- ▶ 신용평가등급 A+, 재무안정성 상위 1%
- ▶ 창립 이래 무차입경영, 20년 연속 흑자기업
- ▶ 국내제품 중 최초로 서버에 포함된 개인정보 파일보호 및 개인정보 보호분야 특허 20여건 등록

## 데이터보호는 유출통제 뿐만 아니라
## 취약점 점검, 악성코드 통제까지 수행해야 완성됩니다

### 데이터 보호관점에 기반하여 데이터 유출, 파괴, 변조행위를 차단하는 악성코드차단 토탈솔루션 제공




**네트워크**

**WebKeeper**
- 악성코드배포 및 유해사이트 차단
- 웹응답값에 포함된 악성코드, 바이러스 차단

**엔드포인트**

**Privacy-i**
- 패턴기반 안티 바이러스
- 행위기반 악성코드 위협탐지 및 대응
- DLP 출력물, 매체제어 개인정보 유출차단
- 취약점 탐지대응 PC 취약점 자동화 점검 상시탐지
- 개인정보보호 개인/기밀정보 자산식별 및 암호화

**서버**

**Server-i**
- 취약점 탐지대응 서버 취약점 자동화 점검 상시 탐지
- 백신 서버전용 악성코드, 랜섬웨어 바이러스 차단
- DLP 서버 내 개인/기밀정보 유출통제

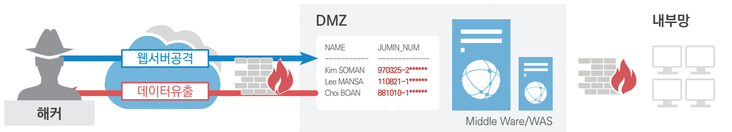
| 정보통신기반보호법 9조 1항 '취약점 분석 평가'에 따른 주요기반시설 취약점 점검 | 개인정보보호법 고시 9조 '악성프로그램 등 방지'에 따른 클라우드 서버백신 적용 | 개인정보보호법 고시 6조 3항 '접근통제'에 따른 서버 개인정보 유출통제 |
|---|---|---|
| 관리기관의 장은 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다 | 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등 보안 프로그램 설치·운영해야 한다 | 인터넷 구간 및 인터넷과 내부망 중간지점 (DMZ)에 고유식별정보 저장시 암호화해야 한다 |

SOMANSA
서울특별시 영등포구 영신로220 KnK디지털타워 9층
TEL 02)2636-8300 FAX 02)2636-9089 www.somansa.com

업데이트: 2022.10

# 도입필요성 서버 및 DB 내 데이터의 유출·변조·파괴행위 차단

## 1. 서버에 보관된 데이터 유출사고 방지 (Server Discover)




1. 해커는 개발용 웹서버, Test서버 등 관리가 소홀한 서버를 가장먼저 노림
2. 웹어플리케이션서버는 외부에 노출
3. 관리가 취약한 웹서버의 취약점 공격(웹쉘 등)
4. 무단 보관된 데이터파일 접근

**DMZ구간 웹어플리케이션서버는 외부에 노출되어 가장 손쉬운 해킹 대상**

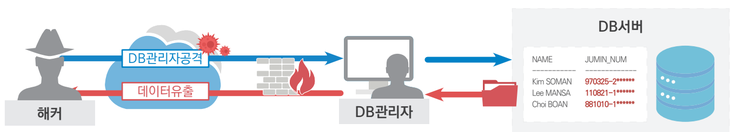
- DB서버 접근권한 없이 웹서버, WAS 해킹만으로도 무단보관 데이터 탈취 및 유출
- dump, tar, gzip 등 압축파일에 데이터가 포함된 경우 실태 파악은 수작업으로 불가

**보유기간 만기, 평문방치 데이터 사전점검을 통해 피해가 발생하더라도 사고규모 최소화**

- 미국 버라이즌 1,400만명 정보유출 협력사 시스템 클라우드 서버에 평문방치
- 개인정보보호법고시 7조 3항에 따라 DMZ 구간 내 개인정보 보관 금지

## 2. DB에 보관된 데이터 유출사고 방지 (DB Discover)

* 별도 라이선스




1. 해커는 DB관리자 PC를 타깃으로 하여 악성코드 배포
2. DB관리자 PC 감염 및 DB접속계정 탈취/접속
3. 조회정보는 Dump파일 생성 후 PC 전송
4. DB관리자 PC에서 외부 전송

**다수 직원이 사용하는 DB서버에는 평문 Table 방치, 관리 어려움**

- DB암호화 이후에도 Temp Table, 신규생성 Table에 데이터가 평문상태로 방치
- 주민번호 등 고유식별정보 암호화 보관규정 준수를 위해 모든 DBMS Table 전수검사 필요

**보유기간 만기, 평문방치 데이터, 테이블 사전점검을 통해 피해가 발생하더라도 사고규모 최소화**

- 모 쇼핑몰 2,500만명 정보유출 DB관리자 PC를 통해 해커 DB접근 및 정보탈취
- 모 포탈 3,500만명 정보유출 키로거 공격으로 DB관리자 계정 탈취 및 유출

## 3. 서버취약점 점검 자동화

* 별도 라이선스

**수작업 중심 서버취약점 점검행위 비효율성 극복**

**기존서버 취약점 점검방식** 솔루션이 없으면 수작업 부담발생, 지속적 추적관리 불가능


| 액티비티 | 수작업 | 자동화 |
|---|---|---|
| 취약점점검 스크립트 선정 | O | O |
| 서버 내 파일 업로드/실행 | O | O |
| 전체결과 다운로드 및 취합 | O | O |
| 기존점검 히스토리 분석/추적 | X | O |
| 상시 실행 | X | O |
| 신규발견 취약점 즉각분석 | △ | O |

- 수작업 28MD → 자동화 2MD로 수행시간 단축
- 상시적인 취약점 점검 및 신규발견 취약점 즉시 점검 가능

## 4. 서버 랜섬웨어 감염으로 인한 대형사고 예방

* 별도 라이선스

**랜섬웨어 공격대상이 PC에서 서버로 이동**

- 미국 콜로니얼 파이프라인 송유관 해킹으로 가동중단 및 지역 비상사태 선포, 몸값 440만 달러 지불
- 국내 웹호스팅 업체 153개 서버, 3400개 사이트 마비, 몸값13억 지불했으나 일부서버 복구실패

**서버감염은 PC감염보다 파급력, 피해규모가 더 큼**

- 기업/기관내 핵심 데이터는 서버에 저장됨
- 수많은 PC가 서버에 접속하므로 연쇄적인 피해확산
- 기업 생산성, 인프라와 직결되는 경우 많아 사회적 혼란 야기

**1차 사전예방**
서버 취약점 점검을 통한 익스플로잇 원천 차단

**2차 실시간 탐지**
리눅스 서버백신을 통한 악성코드/랜섬웨어 실시간 차단

## 5. 컴플라이언스 준수

**신용정보법** 고시 미적용으로 개인정보유출 시

- 과징금 : 최대 50억 or 매출액 3%
- 손해배상 : 피해액의 3배
- 제재 : 기관 업무정지, 임직원 직무정지 (중대한 경우)

**개인정보보호법**

- 고시 미적용으로 개인정보유출 : 관련매출 3% 이하 과징금
- 주민번호유출 : 5억원 이하 과징금

**전자금융거래법**

- 전자금융 기반시설 연 1회 이상 취약점 분석 평가 : 위반시 1천만원 이하 과태료

# 효과 하나의 솔루션으로 데이터 리스크 탐지대응

## 1. 자산현황 파악 (검출)

**기본 13종 패턴 이외에도 사용자 정의패턴 검출**
사번, 고객코드, 구매코드 등 소속기관에서만 사용하는 패턴도 추가등록 및 탐지

**중복패턴 제거 및 정밀분석**
단일파일 내 동일 주민번호 1천개여도 1건으로 계산
개인정보주체 및 정보자산현황 정밀 파악

**확장자 위변조 파일 검출**
확장자 변조한 파일 및 다중압축 파일도 누락없이 검출 및 생성/변조일시 조회가능

## 2. 보유자산 최소화 (삭제 또는 암호화)

- 검출완료 내역 토대로 파일삭제 또는 암호화 수행
- 2차유출 예방위해 검출된 개인정보내역은 마스킹처리
- 보관이 필요한 정보는 '원격 암호화'하여 보호
- 유효기한만료, 불필요한 정보는 '원격삭제'하여 보유자산 최소화 실현


## 3. 서버 취약점 점검 (서버지키미)

- 상시적인 취약점 자동점검 및 신규 취약점 발견 즉시 차단
- 단일 솔루션으로 주요기반시설, 금융기관, 외부취약점DB 점검

| 구분 | Server-i |
|---|---|
| 주요기반 시설 취약점 점검항목 | O |
| 금융기관 서버 취약점 점검항목 | O |
| 개발사 자체 취약점 점검항목 | O (소만사 자체 DB 보유) |
| 글로벌 외부 전문취약점 점검항목 | O |

## 4. 악성코드, 랜섬웨어 차단 (리눅스 서버백신)

**클라우드환경에 최적화된 리눅스 서버 백신 솔루션 라이선스 부담 최소화**

- 클라우드/모바일 환경변화로 모든 기업/기관들은 안정성 높고 라이선스 부담 낮은 리눅스 서버로 전환 중
- 1천 여 고객사를 통해 축적한 통합 데이터베이스 보유
- Mitre ATT&CK 프레임워크 적용하여 제로데이, 파일리스 공격대응