엔터프라이즈 시장 1위
클라우드 DB보안 1위
DB접근통제 솔루션

왜 DB-i인가?

업계 최장 1997년 데이터보호 시장 개척, 27년 차 데이터보호 전문기업
업계 최다 국내 클라우드 DB 보안시장 1위 (KT, 삼성, LG, 국가정보자원관리원 등 클라우드 DB 3만 여 대 구축완료)
업계 최대 동종업계 기술인력대비 2배 이상 '240여 명' 기술인력 보유

업계 최장

DB접근제어 기술개발

27년

- **1997년 창립 27년 차 보안 기술력 1위, 개인정보보호 1위**
- 해당사업에 가장 장기 종사한 데이터보호 전문기업
- 창립 이후 무차입 경영, 신용평가등급 A+, 현금흐름등급 A 재무안정성 중소기업 상위1%

업계 최다

클라우드 DB보안 레퍼런스

30,000여 대

- **KT, 삼성, LG, 국가정보자원관리원 등 클라우드 DBMS 전환 시스템 3만 대 이상** (경쟁사 대비 2배)
- 공공 최대 '클라우드 데이터관리' **국가정보자원관리원 대구센터 BMT 수행결과 1위** (99.25점/100점 만점 기준)

업계 최대

기술인력

240 여 명

- **임직원 3명 중 2명은 기술인력 (전체인원의 66%)**
- **동종업계 기술인력 대비 2배 이상 확보하여 인력 변동 시에도 원활한 기술지원 수행**
- 제품개발 및 기획에 직접 참여한 전문인력이 직접 기술지원 수행

목차

1. 회사소개

01. 시장 1위 데이터보호 전문기업 소만사

02. 재무 안정성 상위 1%

03. 조직 및 기술지원능력

04. 인증 및 지적 재산권

05. 레퍼런스

01. 시장 1위 데이터보호 전문기업 소만사

1997년 창립 이후 27년간 데이터보호에 집중한 '데이터 보호 전문기업'

2023

국가정보자원관리원 대구센터 47개 행정/공공기관 업무서비스 지원체계 구축

KT 1만여대 클라우드 DB 접근제어 구축 (국내최대 클라우드 DBMS 서버팜)

삼성그룹 ERP 구축 (국내최대 SAP Site)

2021

클라우드 DB서버용 접근제어 솔루션 'DB-i Cloud' 출시

2020

DB-i 6.0 출시, DB DLP 개인정보 유출 통제 강화

Gartner Magic Quadrant 'Enterprise DLP' 보고서 2년 연속 등재

2015

Web Applications 접속기록관리 Was-i 출시, SAP 관리 App-i 출시

고객사 1,000개사 달성 (공공/금융/기업 등)

DB-i 솔루션으로 대한민국 신 SW대상 국무총리상 수상

2007

광주 통합전산센터 분리발주 1호 사업 수행 및 운영 중

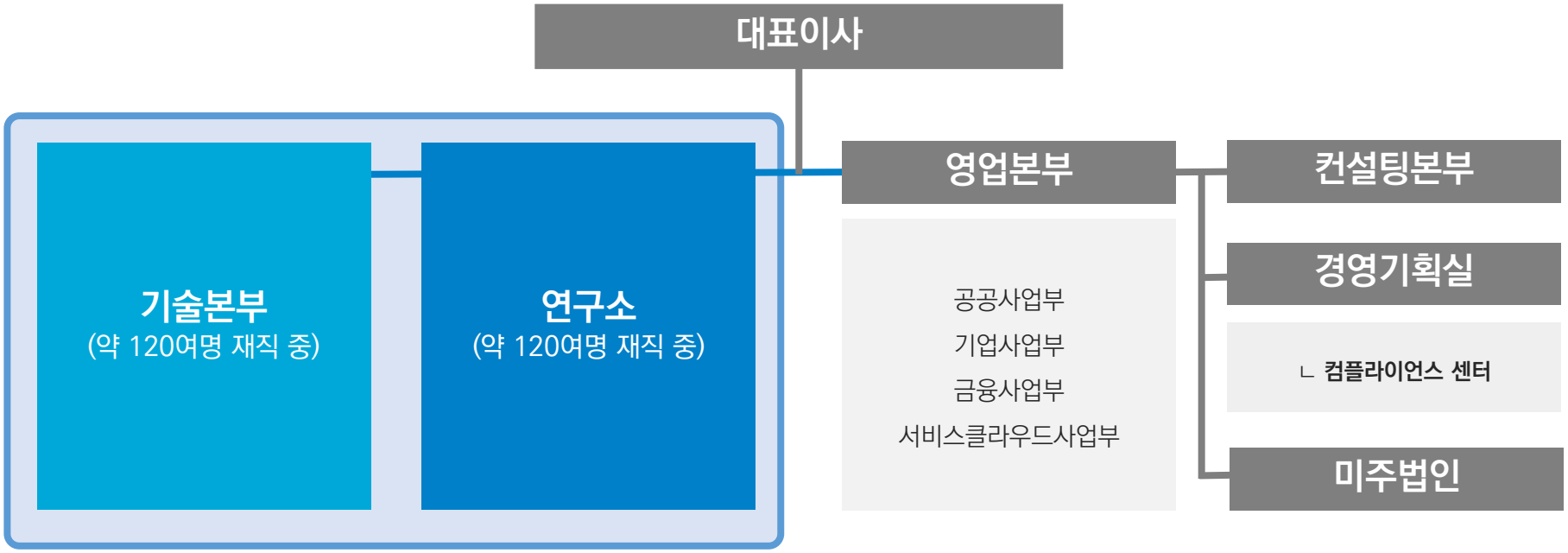
DB접근통제 솔루션 'DB-i' v1.0 출시

1997

㈜소프트웨어를 만드는 사람들 설립

03. 조직 및 기술지원능력

- **소만사는 전체 임직원 350명 중 240여 명이 기술인력(70%)으로 재직 중입니다.**
- **데이터보호업계 최대 수준인 연구개발자 120여명, 기술엔지니어 120여명**을 바탕으로 지속적인 R&D와 서비스를 제공합니다.
- **실제 개발구축에 참여한 DB 접근제어 전문가를 통한 신속하고 명확한 제품구축과 기술지원**을 약속 드립니다.



02. 재무안정성 상위 1%

- 중소기업 **재무안정성 상위 1%(A+), 유일한 무차입 기업**입니다
- **신용평가등급 A+, 현금흐름등급 CR-1로 중소기업 상위 1%의 재무적 안정성**을 바탕으로
  소만사는 중장기 R&D 및 기술지원에 투자하고 있습니다


Korea Rating & Data

I. 기업신용등급

회사명 : (주)소만사 대표자명 : 김대환 사업자번호 : 214-86-14882

기업개요

기업명	(주)소만사
대표자	김대환
법인(주민)번호	110111-1394115
사업자번호	214-86-14882
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
업종	(J58222) 응용 소프트웨어 개발 및 공급업
주요제품명	개인정보보호, 내부정보유출방지, 엔터프라이즈 및 악성코드차단 솔루션
종업원수	338명 (연구소 소속 117명 포함)
기업규모	중기업 (중소기업확인서 (중소벤처기업부))

신용등급

기업신용평가등급	현금흐름등급
A+	CR-1

평가기준일	2023년 04월 14일
재무기준일	2022년 12월 31일

경영규모 (단위:백만원)	재무기준일	총자산	납입자본금	자기자본	매출액	순이익
	2022-12-31	84729	543			

신용등급이력

평가기준일	재무기준일	신용등급	변동
2023-04-14	2022-12-31	A+	-
2022-04-15	2021-12-31	A+	
2021-04-19	2020-12-31	A	

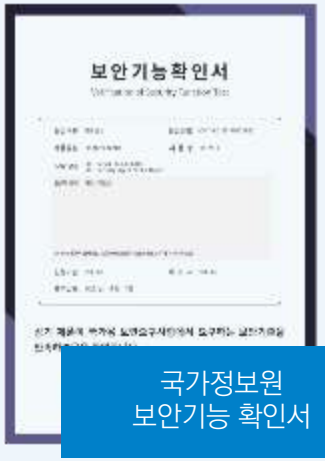
(단위: 억원)

구 분	2022년	2023년	2024년
매출액	535	577	653
영업이익	83	124	145
당기 순이익	88	140	161
차입금	0	0	0
총자산	847	1,014	1,221

7
SOMANSA

04. 인증 및 지적재산권

- **국정원 보안기능확인서, 과학기술정보통신부 CC인증/GS인증** 획득
- 데이터보호 분야 50건 이상 기술 특허 등록 (해외 9건 포함)
- 타 보안기업 대비 지적재산권 3배 이상 확보



국가정보원
보안기능 확인서

과학기술정보통신부
소프트웨어 품질인증서

과학기술정보통신부
CC인증서

기업용 클라우드 서비스의
접근통제 방법

클라우드 상에 구현되는
정보유출방지시스템 및 방법

파일시스템에 저장된
중요정보의 검사방법/장치

내부사용자에 의한 개인정보
유출방지 쿼리툴 통제방법시스템

애플리케이션 경유 DB접근보호
데이터베이스 보안시스템

05. DB-i 레퍼런스

엔터프라이즈 시장 1위

삼성, LG, KT그룹 표준 제품입니다

SAMSUNG 삼성전자 **ERP** 세계최대 ERP시스템 DBMS 서버팜	SAMSUNG 삼성전자 **CRM** 세계최대 고객관리 서비스 시스템	SAMSUNG 삼성전자 **MES** 국내최대 생산자동화 서비스 시스템	SAMSUNG 삼성엔지니어링 **전사 DBMS** 글로벌 설계, 구매, 시공 전문기업	SAMSUNG 삼성SDS **클라우드센터 DBMS** 국내최대 SI, IT 전문기업
SAMSUNG 삼성중공업 **조선해양 DBMS** 국내최대 선박, 해양플랜트 제조기업	엘지전자 **전사 DBMS** 글로벌 가전분야 1위 기업	LG디스플레이 **전사 DBMS** LCD, OLED 디스플레이 1위 기업	LG에너지솔루션 **전사 서버 700여대** 글로벌 배터리 제조 전문기업	LG생활건강 **전사 DBMS 클라우드 전환** 국내 최대 생활용품 제조,판매기업
LG CNS **전사 DBMS 클라우드 전환** SI, SW개발, 컨설팅 전문 기업	kt **전사 DBMS 클라우드 전환** 국내최대 클라우드 DBMS 보유기업 (1만 여 대, 계정 사용자 2천명)	kt **유무선망 DBMS 접근제어 보안** 국내 최대 유무선망 서비스 제공기업	SK **전사 DBMS** 전산센터 내 DBMS 통합 보안	LOTTE **전사 DBMS** 클라우드 DB포함 전산센터 내 DBMS 통합 보안
CJ **전사 DBMS** 사내 인사정보 시스템 포함 전사 고객관리 시스템 DBMS 보안	DOOSAN **전사 DBMS** 고객관리 및 생산서비스 시스템 접근통제 및 보안			

05. DB-i 레퍼런스

국가정보자원관리원 광주센터 및 대구센터 구축

행정안전부, 국가정보자원관리원 광주/대구센터 구축경험을 통한
행정업무 이해도가 높은 기업입니다

책임운영기관 국가정보자원관리원 대구센터 국내최대 클라우드 전산센터 47개 행정기관 클라우드DB 보안	책임운영기관 국가정보자원관리원 광주센터 국내최대 전산센터 26개 입주기관	KLID 한국지역정보개발원 차세대 지방세 프로젝트
행정안전부 전자정부 클라우드 플랫폼 DB접근제어 프로젝트	기상청 기상청 관리 서버 구축 프로젝트	전라남도 JeollaNamdo 전라남도청 관리서버 구축 프로젝트

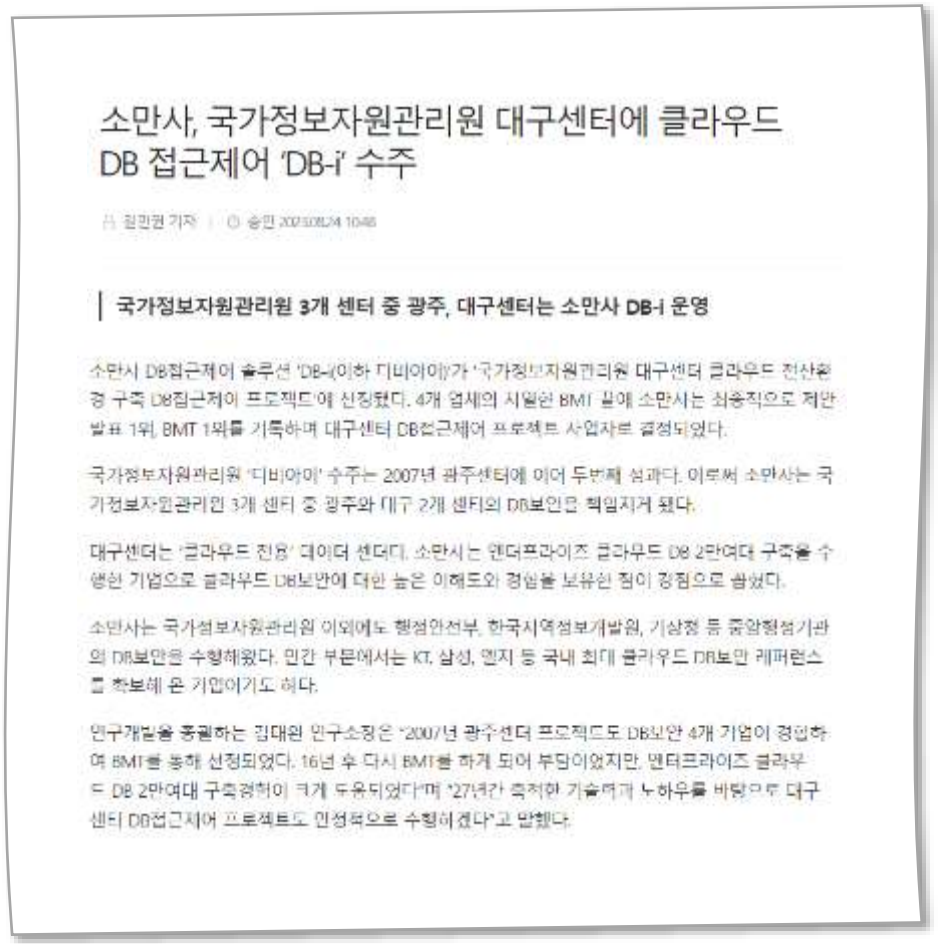
05. DB-i 레퍼런스

공공 부분 최대 DBMS 서버팜

국가정보자원관리원

광주, 대구센터

- 50여 중앙부처 전산시스템 통합운영
- **대한민국 국민 전체 개인정보를 보유한 국내 최대 공공 시스템 운영센터**
- **공공 최대 전산센터인 광주센터 17년 연속 운영** 경험 및 3회 이상 DBMS 보안 고도화 수행
- **공공 최대 클라우드 DBMS 전산센터인 대구센터** 내 약 700여 클라우드 DBMS, 400여 **대민시스템 통제관리**



소만사, 국가정보자원관리원 대구센터에 클라우드 DB 접근제어 'DB-i' 수주

| 국가정보자원관리원 3개 센터 중 광주, 대구센터는 소만사 DB-i 운영

소만사 DB접근제어 솔루션 'DB-i'(이하 디비아이)가 '국가정보자원관리원 대구센터 클라우드 전산환경 구축 DB접근제어 프로젝트'에 선정됐다. 4개 업체의 치열한 BMT 끝에 소만사는 최종적으로 제안 발표 1위, BMT 1위를 기록하며 대구센터 DB접근제어 프로젝트 사업자로 결정되었다.

국가정보자원관리원 '디비아이' 수주는 2007년 광주센터에 이어 두번째 쾌거다. 이로써 소만사는 국가정보자원관리원 3개 센터 중 광주와 대구 2개 센터의 DB보안을 책임지게 됐다.

대구센터는 '클라우드 전용' 데이터 센터다. 소만사는 엔터프라이즈 클라우드 DB 2만여대 구축을 수행한 기업으로 클라우드 DB보안에 대한 높은 이해도와 경험을 보유한 점이 강점으로 꼽혔다.

소만사는 국가정보자원관리원 이외에도 행정안전부, 한국지역정보개발원, 기상청 등 중앙행정기관의 DB보안을 수행해왔다. 민간 부문에서는 KT, 삼성, 엔지 등 국내 최대 클라우드 DB보안 레퍼런스를 확보해 온 기업이기도 하다.

연구개발을 총괄하는 김대원 연구소장은 "2007년 광주센터 프로젝트도 DB보안 4개 기업이 경합하여 BMT를 통해 선정되었다. 16년 후 다시 BMT를 하게 되어 부담이었지만, 엔터프라이즈 클라우드 DB 2만여대 구축경험이 크게 도움되었다며 "27년간 축적한 기술력과 노하우를 바탕으로 대구센터 DB접근제어 프로젝트도 안정적으로 수행하겠다"고 말했다.

05. DB-i 레퍼런스

국가정보자원관리원 대구센터 DB접근제어 BMT 1위
P, W, S사 포함 4개사 BMT 수행 (2023.05)

[입찰결과]

입찰공고번호	20230412616-00	공고상세	참조번호	00236049800
공고명	대구센터 클라우드 전산환경 구축 DB 접근제어 SW 도입			
공고기관	조달청		수요기관	행정안전부 국가정보자원관리원

[참여 업체수 : 4 개사]

제안평가 1위

			대표자	투찰금액(원)	투찰률(%)	추첨번호	투찰일시	비고
1	2148614882	(주)소만사	김대환	720,000,000			2023/05/08 16:02:36	
2	1078644093	주식회사		720,000,000			2023/05/08 17:55:49	
3	1388125547	주식회사		720,000,000			2023/05/08 10:55:47	
4	2118100569	(주)		720,000,000			2023/05/08 15:15:15	

국가정보자원관리원

행정안전부

수신 주식회사 소만사 대표이사

(경유)

제목 「대구센터 클라우드 전산환경 구축 DB접근제어 SW 도입 사업」 BMT 결과 알림

1. 귀사의 무궁한 발전을 기원합니다.

2. 관련
가. 조달청 구매관리번호 제00236049800호
나. 국가정보자원관리원 정무회사업개-678호(2023. 5. 10., 「대구센터 클라우드 전산환경 구축 DB접근제어 SW 도입」 사업 정량평가 결과 알림)

3. 위의 관련하여, 귀사에서 입찰에 참여한 「대구센터 클라우드 전산환경 구축 DB접근제어 SW 도입 사업」 입찰 참여업체에 대한 BMT 결과를 아래와 같이 알려드립니다.

업체명	제품명	BMT 점수		
		계 (55점)	기능확인 (52점)	성능확인 (3점)
(주)소만사	DB-i v5.*	55점	52점	3점

붙임 BMT 평가항목별 평가점수 1부. 끝.

국가정보자원관리원장

기술평가 1위

	(주)소만사
입찰가격점수	10
기술평가점수	89.25
종합평점	99.25

상호명	주식회사
입찰가격점수	10
기술평가점수	88.
종합평점	98.

2. 도입 필요성

01. 개인정보보호 법규정 준수

개인정보보호법 고시 '개인정보의 안전성 확보조치 기준' **접근통제 규정을 100% 준수하는 유일한 솔루션입니다**

구분	조문내용	DB-i 법규충족/제공기능
5조 접근권한의 관리	① 개인정보처리시스템 접근권한을 업무수행에 필요한 최소범위로 업무담당자에 따라 차등부여	• 사용자 ID/IP 기준으로 로그인 통제 및 접속가능한 DB지정 • 업무시간을 지정하여 해당 시간에만 접근하도록 제한 • 2-Factor 인증방식으로 사용자 신원확인
	② 개인정보취급자 변동시 지체없이 변경말소	• 개인정보 취급자 계정 변경말소 및 해당기록 3년 보관
	③ 권한부여/변경말소 기록 최소 3년 보관	
6조 접근통제	① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고를 방지	• 개인정보가 포함된 Table/Column 전수검사를 통해 보호자산 식별 • IP, ID, 시간대, Table/Column, Query유형, Application별 통제 • Telnet(SSH) 로그인 및 명령어 통제 • **유일** FTP(SFTP) 로그인 및 Download/Upload통제 • RDP 통제
	1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 **인가받지 않은 접근을 제한**	
	2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 **불법적인 개인정보 유출 시도 탐지** 및 대응	• DB 응답값에 개인정보가 대량으로 포함된 경우 사전차단 **예시)** · Query 응답 값에 주민번호 다량보유시 실시간 경보 및 차단 · Query 응답 값에 개인정보 다량보유시 사후 추적 및 리포팅
	② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 **안전한 인증수단**을 적용해야 함	• DB클라이언트와 DB방화벽 사이 암호화 채널 제공 • 2-Factor 인증방식으로 사용자 신원확인

01. 개인정보보호 법규정 준수

개인정보보호법 고시 '개인정보의 안전성 확보조치 기준' **접근통제 규정을 100% 준수하는 유일한 솔루션입니다**

구분	조문내용	DB-i 법규충족/제공기능
6조 접근통제	③ 개인정보처리자는 처리하는 개인정보가 홈페이지, P2P, 공유설정 등을 **통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 관한 조치**를 취해야 함	• **DB 접속후 개인정보 유출통제** · 유일 Query의 응답값 확인 후 단말기에 파일생성시 경보안내 · 유일 DBapp의 Query 결과값 복사 후 편집기(ex: Excel)에 붙여넣기 시 통제
	④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속 차단해야 함	• 장기미사용 DB세션 통제 • 세션 유휴시간 설정, 초과시 차단
8조 접속기록의 보관 및 점검	① 개인정보처리자는 개인정보처리시스템에 접속한 자에 대한 접속기록을 생성하고 3개월 이상 보관·관리해야 함.	• 누구의 개인정보를 조회했는지 '정보주체' 정보 기록 • 개인정보 대량조회, 소량 다회조회 기록 • 쿼리결과 FTP 다운로드 현황 기록 • 유일 쿼리결과 클립보드 복사/붙여넣기 차단 **DB접근제어 솔루션이 반드시 기록해야 할 정보** 1. 쿼리응답값 2. Telnet,SSH 세션에서의 개인정보 조회기록 3. FTP/SFTP를 통한 파일다운로드 기록 4. RDP 세션저장(Playback)
	② 제1항에도 불구, 개인정보취급자의 접속기록은 1년 이상 보관·관리해야 함. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리해야 함. 1. 5만명 이상의 개인정보를 처리하는 개인정보처리시스템 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템 3. 기간통신사업자	
	④ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검해야 함.	
	⑤ 개인정보처리자는 제1항 및 제2항에 따른 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하기 위한 조치를 해야 함.	• 로그 위변조 방지 기능

3. 기능소개

01. 특장점

02. 기능

03. 구성도

01. 특장점

업계 최장 1997년 데이터보호 시장 개척, 27년 차 데이터보호 전문기업
업계 최다 국내 클라우드 DB 보안시장 1위 (KT, 삼성, LG, 국가정보자원관리원 등 클라우드 DB 3만 여 대 구축완료)
업계 최대 동종업계 기술인력대비 2배 이상 '240여 명' 기술인력 보유

업계 최장

DB접근제어 기술개발

27년

- **1997년 창립 27년 차 보안 기술력 1위, 개인정보보호 1위**
- 해당사업에 가장 장기 종사한 데이터보호 전문기업
- 창립 이후 무차입 경영, 신용평가등급 A+, 현금흐름등급 A 재무안정성 중소기업 상위1%

업계 최다

클라우드 DB보안 레퍼런스

30,000여 대

- **KT, 삼성, LG, 국가정보자원관리원 등 클라우드 DBMS 전환 시스템 3만 대 이상** (경쟁사 대비 2배)
- 공공 최대 '클라우드 데이터관리' **국가정보자원관리원 대구센터 BMT 수행결과 1위** (99.25점/100점 만점 기준)

업계 최대

기술인력

240 여 명

- **임직원 3명 중 2명은 기술인력 (전체인원의 66%)**
- **동종업계 기술인력 대비 2배 이상 확보하여 인력 변동 시에도 원활한 기술지원 수행**
- 제품개발 및 기획에 직접 참여한 전문인력이 직접 기술지원 수행

02. 기능

DB 접근통제 쿼리응답값 유출차단

- 클라우드 DB 포함 20여종 DBMS 지원
- 계정·부서·시간대별 통제
- 쿼리툴(Dbeaver, Toad, Orange, Golden 등) 통제
- 테이블/칼럼 별 통제
- SQL Commands (DDL, DML, DCL) 구문탐지 통제
- 내용기반 개인정보 이상조회 통제
- 개인정보 포함 DB 자동식별 기능

서버 접근통제 서버접근 및 개인정보파일 유출차단

- Telnet/SSH (Secure Shell Protocol)
- FTP/SFTP (File Transfer Protocol)
- RDP (Remote Desktop Protocol)

접속기록관리

- 법에 명시된 세부이력 로그저장 및 사후감사 활용
- 개인정보 마스킹
- 빅데이터 검색

관리자 페이지/리포트

- 웹콘솔 기반 관리자 페이지
- 대시보드
- 리포팅

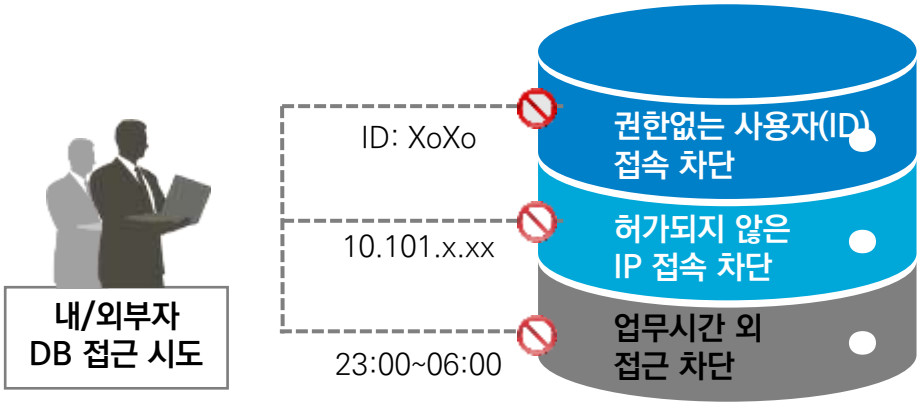
02. 기능 : DB 접근통제

클라우드 DB 포함 20여종 DBMS 지원

- Oracle, MS SQL, DB2(UDB), SAP HANA 등 DBMS 20여종 통합관리
- PostgreSQL, MongoDB, MairaDB 등 8종 이상의 클라우드 DB 지원
- **삼성그룹 SAP HANA** 기반 DB접근제어 프로젝트 수행 **(2천 Core규모)**
- **삼성그룹 G-ERP**(전사적 관리 시스템) DB접근제어 수행 **(1만 Core 규모)**
- 국내최대 클라우드 DB보유사업자 **KT 클라우드** DB접근제어 수행 **(1만여 대 규모)**
- 국내최대 공공 클라우드 DB 보유기관 **국가정보자원관리원 대구센터** DB접근제어 수행

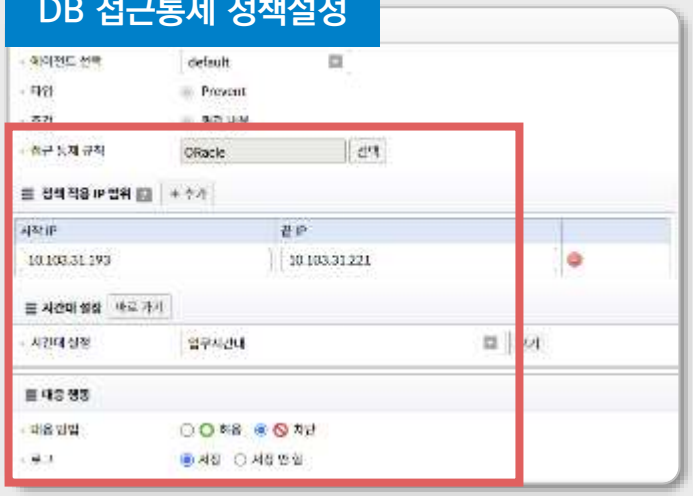
02. 기능 : DB 접근통제

계정·부서·시간대별 접근통제

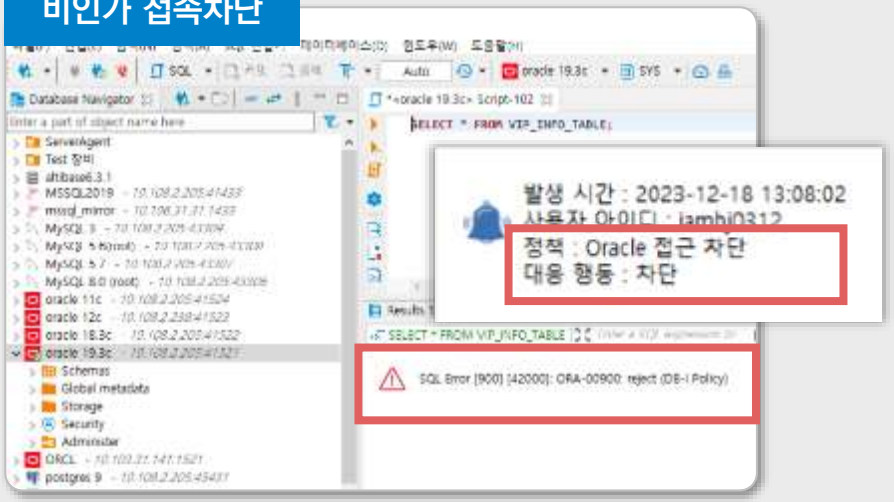


- 사용자 IP 및 IP 대역 차단/허용
- DBMS 접속 계정별 접속 차단/허용
- 시간대별 접근 차단/허용
- Telnet, FTP, SFTP, SSH 등의 원격 프로토콜 통제
- DDL, DML, DCL, TCL 등 쿼리 유형/명령어 사용통제

DB 접근통제 정책설정



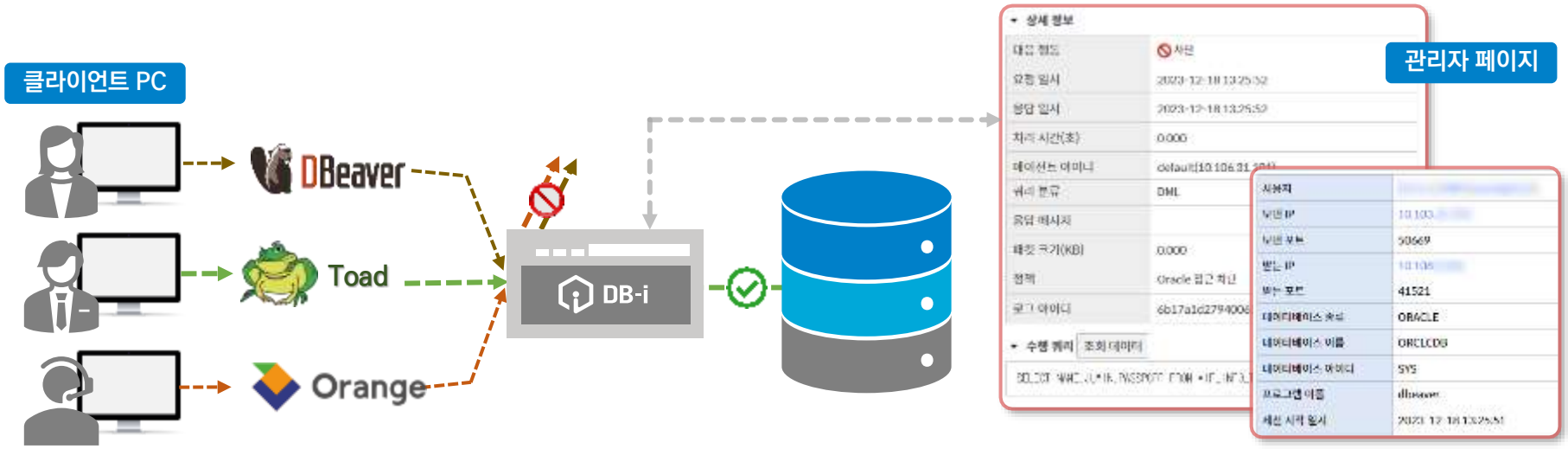
비인가 접속차단



02. 기능 : DB 접근통제

DBMS 툴 (쿼리툴 : Dbeaver, Toad, Orange, Golden 등) 접근통제

시나리오 : 특정 DBMS 툴 (ex: Toad)을 통해서만 DBMS 접속/조회가 가능하도록 설정



DBMS 조회를 위해 쿼리툴을 이용

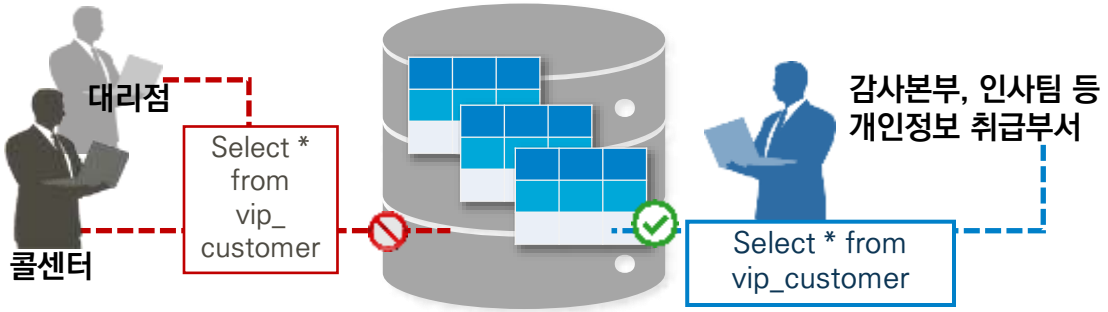
접속을 시도하더라도 허용된 DBMS 툴만 접속허용 이외 툴은 접속차단

접속차단 내역 로그저장
사용자, IP, 시간, 차단 DBMS 툴

접속허용 내역도 로그저장
사용자, IP, 시간, + 허용 DBMS 툴, 조회 개인정보

02. 기능 : DB 접근통제

Table·Column 별 접근통제



- ✓ 개인정보 포함된 테이블과 칼럼 접근통제
- ✓ 권한에 따른 접근권한 차등 부여
- ✓ 권한 외 부서에서 특정 테이블/칼럼 접근시 접속차단
  - 알림창을 통해 접속 차단 사유 확인
  - 차단내역은 로그저장, 사후 감사자료로 활용

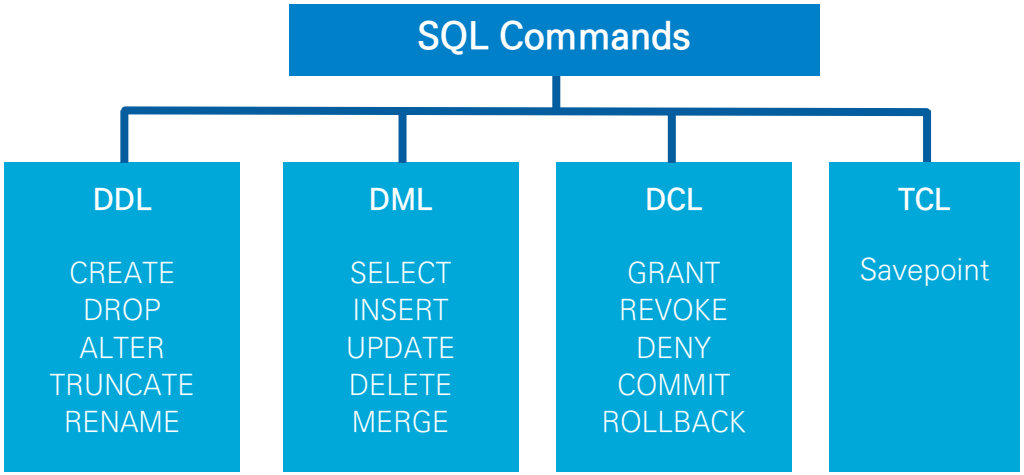
쿼리툴을 사용하여 DB 내 임직원 테이블 접근시 접속차단

임직원 테이블의 '주민번호' 컬럼 접근시 접속차단

Table, Column 차단로그 및 상세 SQL정보 확인

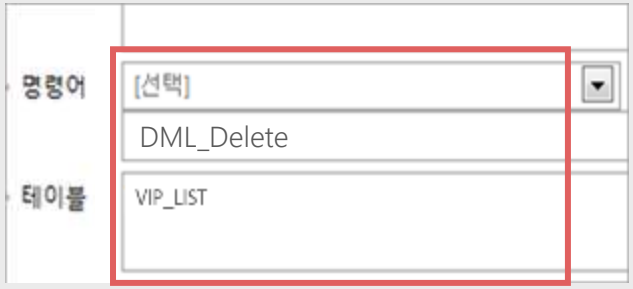
02. 기능 : DB 접근통제

SQL Commands (DDL, DML, DCL) 구문 탐지 통제

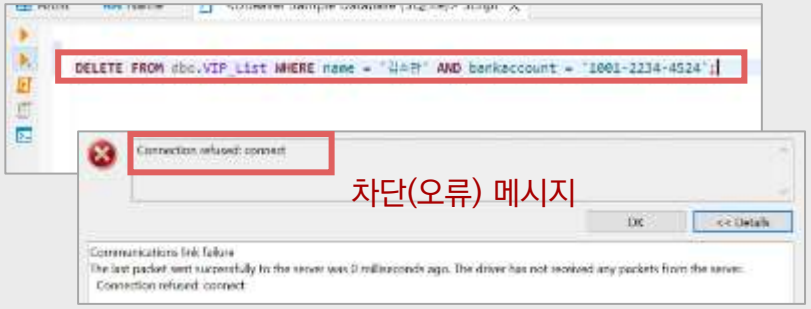


- ✓ DDL (Data Definition Language): DB 구조 정의
- ✓ DML (Data Manipulation Language): DB 테이블 내 데이터 검색, 삽입, 업데이트, 삭제 조작
- ✓ DCL (Data Control Language): DB 접근 권한 설정
- ✓ **업무와 무관한 명령어 사용을 사전에 통제하여 개인정보 조회 오남용 차단**

① DB 규칙에서 통제대상 명령어 설정



② Delete Query 입력 시 정책에 따라 통제



02. 기능 : DB 접근통제

내용기반 개인정보 이상조회 통제

쿼리 응답값에 포함된 개인정보 분석, 차단 및 기록

개인정보처리시스템 접속 후 대량조회 시 통제

→ 조회되는 데이터를 정확히 검출 / 유출 시도 사전차단

- 개인정보 보호 솔루션 27년 개발 노하우,
  타사 솔루션들이 모방할 수 없는 데이터 분석능력/정확도
  (타사) DB접근 보안 외 DB 개인정보 유출방지 정책 미지원
- 법령에 명시된 고유식별정보 외 개인정보 패턴 모두 지원
  (타사) 주민번호를 제외한 개인정보패턴 미지원/오탐률 높음
- 국내 유일, 고유식별정보 체크섬 3개 보유
  (타사) 주민번호/외국인번호 체크섬 2개 보유 - 마스킹/스캐닝 전용
- EU GDPR(유럽 개인정보보호법) 준수를 위한
  EU 개인정보 패턴 분석 지원
  (타사) 글로벌 컴플라이언스 대응 불가

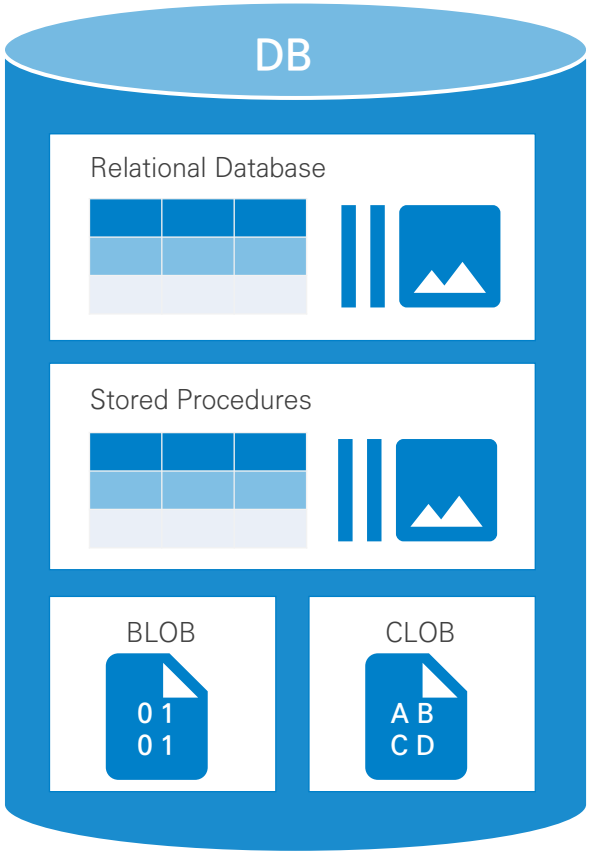
'누구의 개인정보'를 조회했는지 모두 기록

개인정보 대량조회 또는 최소정보 다회조회 등

이상행위 발생시 차단 및 조회된 데이터 확인가능

02. 기능 : DB 접근통제

개인정보 포함 DB 자동식별 기능



데이터 마이닝 (Data Mining)
DB를 풀스캔하여 DB내 개인정보현황 식별

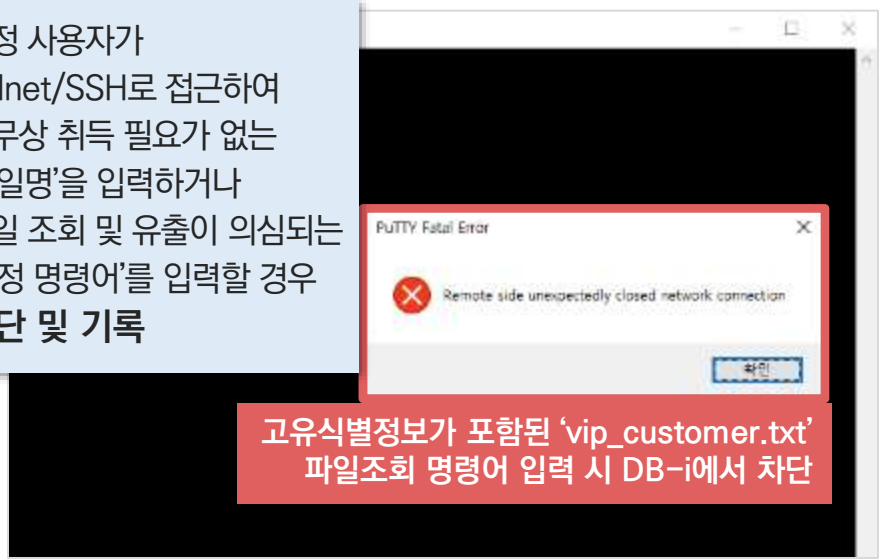
- 개인정보 포함된 Table에 접속통제 정책 수립 시 기초자료 제공
- 불필요한 개인정보가 포함된 Table(Temp 포함) 탐지
- 주기적 점검을 통해 신규생성된 개인정보 포함 Table 자동식별

- Table, Column에 포함된 개인정보 및 Stored Procedure에 포함된 개인정보 검출
- **유일** CLOB(Character large object), BLOB(Binary large object)에 저장된 개인정보 자동검출
- **유일** 이미지 형태로 DB에 저장된 개인정보 자동 검출

02. 기능 : 서버 접근통제

Telnet/SSH 통제 (텍스트 기반의 Unix, Linux 원격터미널 서비스)

특정 사용자가
Telnet/SSH로 접근하여
업무상 취득 필요가 없는
'파일명'을 입력하거나
파일 조회 및 유출이 의심되는
'특정 명령어'를 입력할 경우
차단 및 기록



고유식별정보가 포함된 'vip_customer.txt'
파일조회 명령어 입력 시 DB-i에서 차단

사용자	연구소 /
보낸 IP	10.103.31.193
보낸 Port	53561
받는 IP	10.103.31.226
받는 Port	22
서버 타입	Telnet/SSH
에이전트 아이디	default(10.106.31.101)
세션 시작 일시	2023-12-18 14:06:48
세션 종료 일시	2023-12-18 14:06:52
세션 지속 시간(초)	4.413
로그인 실패 횟수	0
정책 이름	Telnet SSH 차단
대응 행동	차단

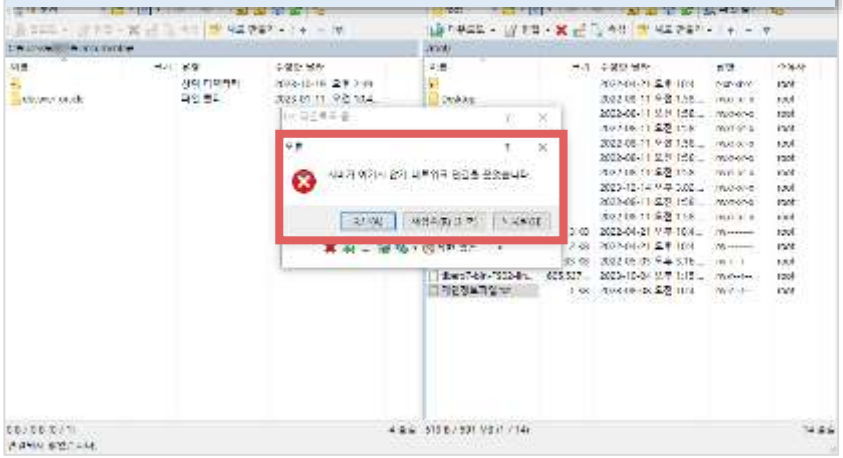
세션 시작 일시	세션 종료 일시	대응 행동	부서 이름	사용자 이름	보낸 IP	받는 IP	서버 타입	정책 이름
2023-12-18 14:06:48	2023-12-18 14:06:52		연구소		10.103.31.193	10.103.31.226	TELNET/SSH	Telnet SSH 차단

차단 내역은 로그 저장되어 차단사유 확인 및 사후감사자료로 활용

02. 기능 : 서버 접근통제

FTP/SFTP 통제 (네트워크를 통한 파일전송 서비스)

업무와 연관 없는 사용자가 FTP로 접속을 시도하거나 (ID, IP)
특정 **개수** 또는 **용량**이상의 **개인정보**가 포함된 **파일**을
변조하여 PC **다운로드** 시 **차단**



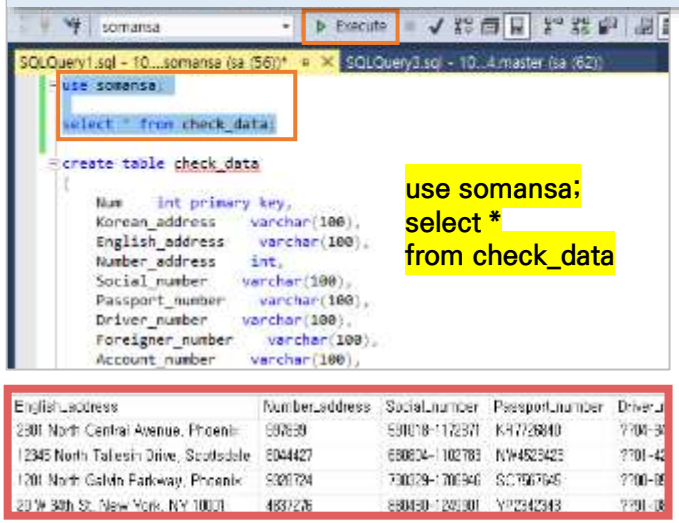
주민번호가 포함된 'vip_social_number.**xlsx**' 파일을
'관악산.**jpg**' 파일로 확장자 변경 및 압축하여 PC 다운로드 시
네트워크 연결이 중단되며 다운로드 차단

차단 내역은 로그 저장되며
다운로드 시도한 직원정보, 발생시점, 차단사유,
파일 내 포함된 개인정보 개수 등 원격 터미널 서비스를 이용한
다운로드 세부정보 관리자 페이지에서 한 번에 확인

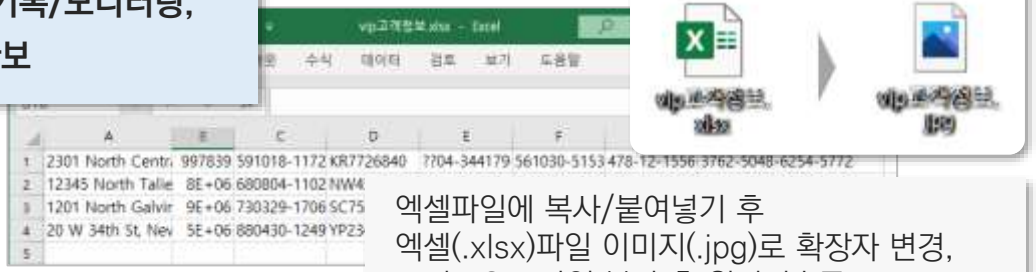
02. 기능 : 서버 접근통제

RDP 통제 (Remote Desktop Protocol:원격 데스크톱 프로토콜)

Windows는 자사 서버 접속을 위해 RDP 연결 기능 제공
DB-i는 RDP를 통한 접속은 허용하되 **수행활동 모두 기록/모니터링,**
이후 **Playback**을 통해 개인정보 유출시도 **감사자료 확보**



RDP를 통해 서버에 접속한 후
해당 서버에서 DBMS 구동
쿼리문을 실행하여 개인정보 조회

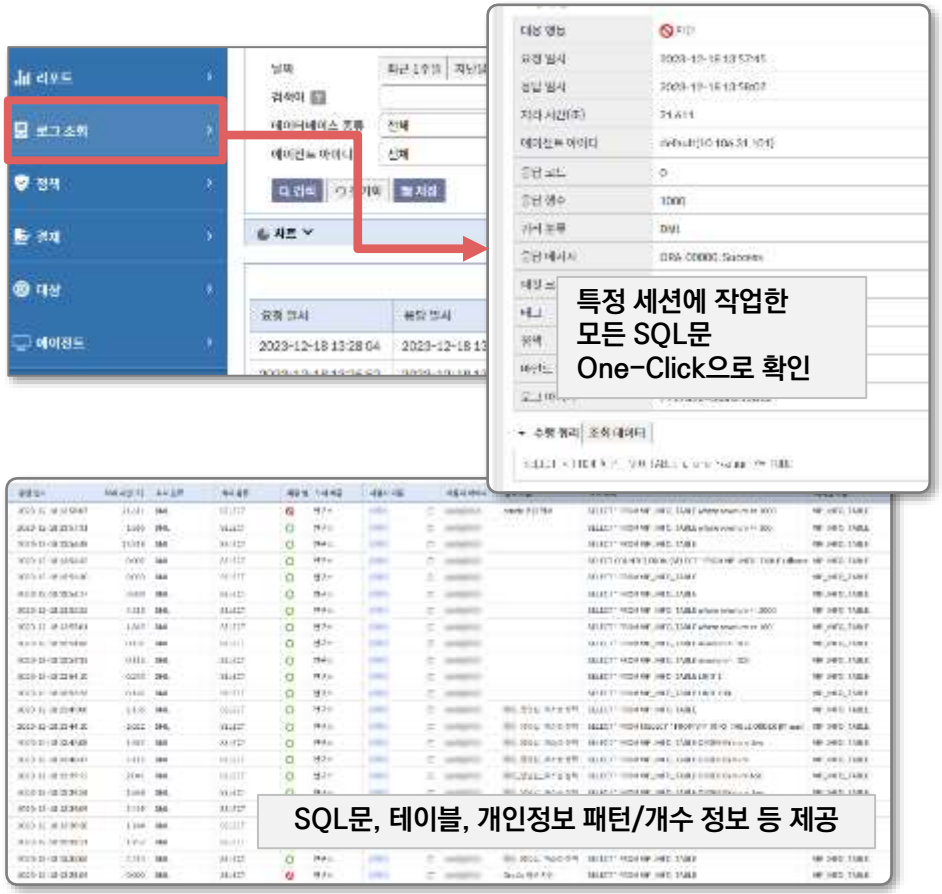


엑셀파일에 복사/붙여넣기 후
엑셀(.xlsx)파일 이미지(.jpg)로 확장자 변경,
로컬 PC로 파일 복사 후 원격접속종료

RDP 접속 이후의
사용자 행위 로그저장
Playback 기능을 통해
모니터링 및 사후감사자료 확보

02. 기능 : 접속기록 관리

법에 명시된 세부이력 로그저장 및 사후감사 활용



법에서 요구하는 세부 이력정보 모두 기록
(법, 시행령, 고시 등 하위법령, 지침 및 감독규정 포함)

세션 로그	SQL 로그	원격터미널 접속로그
사용자 정보 접속 일시 세션 정보 수행시간 DBMS정보 접속프로그램명 …	수행내역 쿼리 종류 테이블, 칼럼 차단/허용 여부 개인정보 패턴 조회 데이터 등 …	Telnet SSH FTP SFTP RDP

**정기적(월 1회 이상) 접속기록 점검 시,
비인가 개인정보 처리, 대량의 개인정보 조회 등의
행위 탐지 및 대응조치 가능**

✓ 빅데이터 검색엔진을 통해 대량의 접속기록에서
비정상 행위를 최대 1~3분 이내 검색/확인

✓ 추가 분석을 위한 로그 Export 기능

02. 기능 : 접속기록 관리

개인정보 마스킹 처리 : 2차 유출 방지

- 관리자 페이지에서 접속기록 조회 시 개인정보 패턴은 마스킹처리되어 공개됨 (고유식별정보 포함)
- 조회된 개인정보 주체의 정확한 개인정보는 관리자도 알아내기 어려움
- 전체 개인정보를 파악할 수 없으므로 **관리용 단말기 화면 촬영, 화면캡쳐 유출 등 2차 유출행위로 부터 안전함**

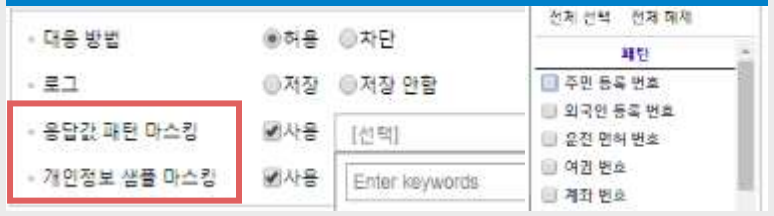
DB서버 응답값(고객정보 노출)

NAME	JUMIN_NUM
Kim Eunju	790211-2594863
Lee Minseo	830717-1564724

사용자 화면(패턴 마스킹 처리)

NAME	JUMIN_NUM
Kim Eunju	790211-2******
Lee Minseo	830717-1******

① 10여종 이상의 개인정보 패턴 식별 및 마스킹 제공



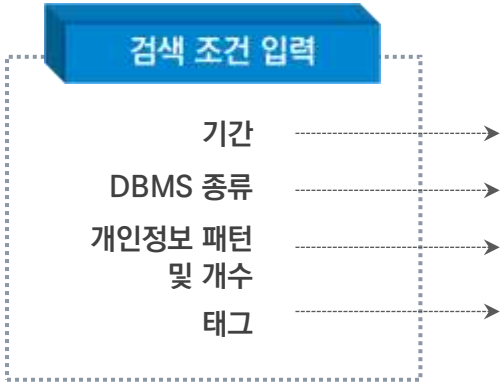
② 사용자 화면 및 접속기록 로그 내 개인정보 패턴 마스킹 처리

NUM	NAME	JUMIN	PASSPORT	DRIVER
67	안아리	500712-*******	GN564****	25-13-******-**
68	풍하나	710430-*******	GP364****	22-10-******-**
69	서세롬	701120-*******	GR564****	15-74-******-**
70	권샛별	761030-*******	GS544****	22-73-******-**

02. 기능 : 접속기록 관리

3년 대용량 3분내 초고속 빅데이터 검색

- 기존 DB 검색 방식 대비 처리속도 100배 이상 단축, 3년치 대용량 접속 로그에서 1~3분 내 초고속 검색
- 이상징후 또는 사용자 과거 로그 검색 시 드릴다운 방식으로 빠르게 조회
- **감독기관 감사자료 요청 시 신속대응**



해당 조건의 로그 검색 및 취합

3분내 검색 완료

복합조건 검색

(기간, DBMS, 허용/차단, 패턴 및 개수 등)으로

재검사 없이 원하는 로그 즉시 확인

개인/민감정보 관련 30개 키워드 동시 검색

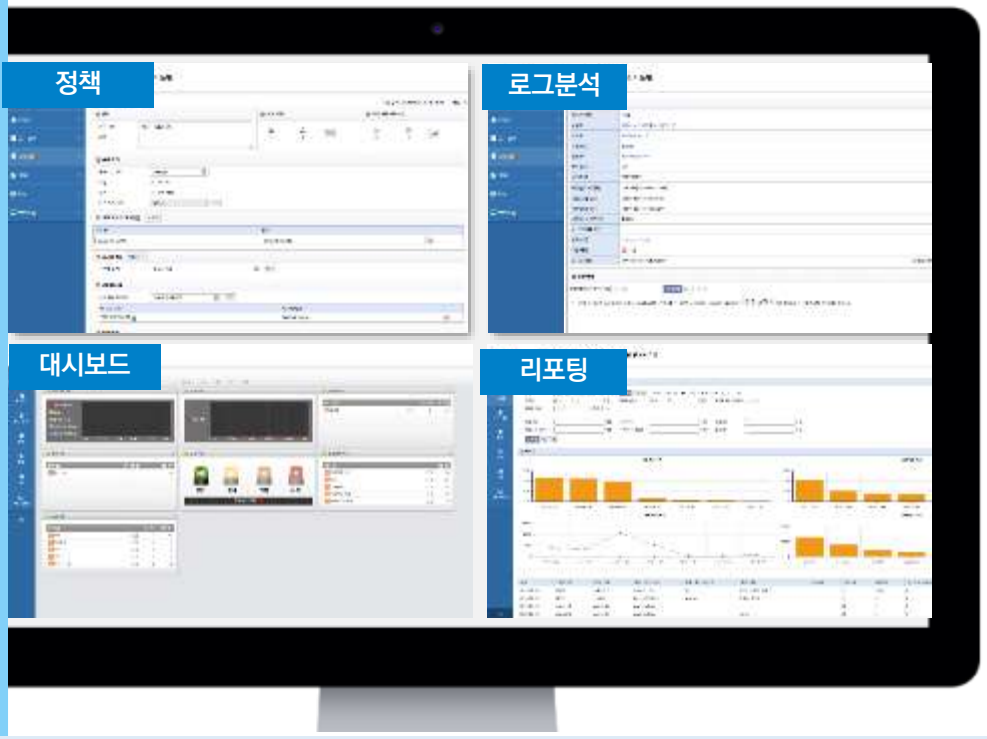
DB-i 빅데이터 검색 vs 타사 DB 검색 방식 비교분석

항목	DB-i 빅데이터 검색	타사 DB 검색
대량로그 검색속도	고속검색 (1~3분)	저속검색 (수 시간 소요)
복수조건 검색 성능영향	성능저하 없음	성능 저하
동시다수자 검색 시 성능영향	성능저하 없음	성능 저하
로그 저장소 안정성/가용성	이중화 구성 가능 (고가용성), 샘플링 저장 없이도 CPU 부하 없음	이중화 불가 (가용성 낮음), 샘플링 저장 불가 시 CPU 부하로 속도 저하

02. 기능 : 관리자 페이지/리포트

웹콘솔 기반 관리자 페이지

- 별도의 어플리케이션(CS) 다운/설치 없이, 브라우저창에서 DB-i 중앙관리 콘솔인 DLP+ Center 접속
- 디바이스, OS, 브라우저 종류 종속되지 않고 어디서든 접속 가능
- 사용자 브라우저와 DB 접근통제 장치간 SSL/TLS 방식으로 안전한 통신 제공



02. 기능 : 관리자 페이지/리포트

대시보드

- 관리자 관점에서 데이터 가시성 확보
- 다양한 위젯 및 레이아웃을 통한 데이터 분석 및 정보흐름 시각화

02. 기능 : 관리자 페이지/리포트

리포팅

- 사용자/부서/대상 DB 서버 인시던트*(사건사고 발생)* 추이, 응용프로그램 순위 리포트 제공
- 특정기간 내 개인정보 조회 상위 유저 리포트 *(누적 데이터 기준, 장기간에 걸친 개인정보 조회자 추적)*
- 정기 리포트 이메일 발송, 정책 위반사항 발생 시 알림

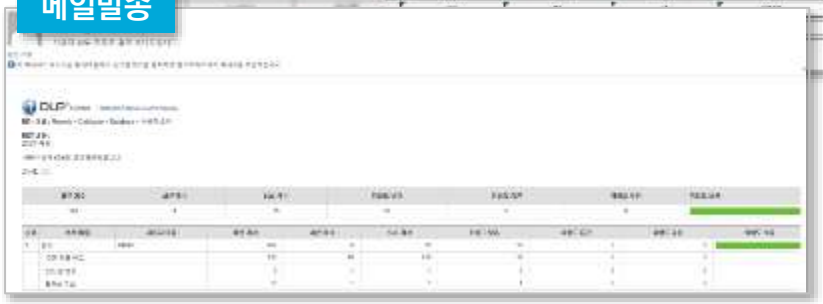
사용자 세션 및 쿼리 순위

데이터베이스 접속조회 사용자 순위

내보내기

엑셀

메일발송



03. 구성도

Proxy, Mirror 방식의 장점을 반영
Hybrid 방식

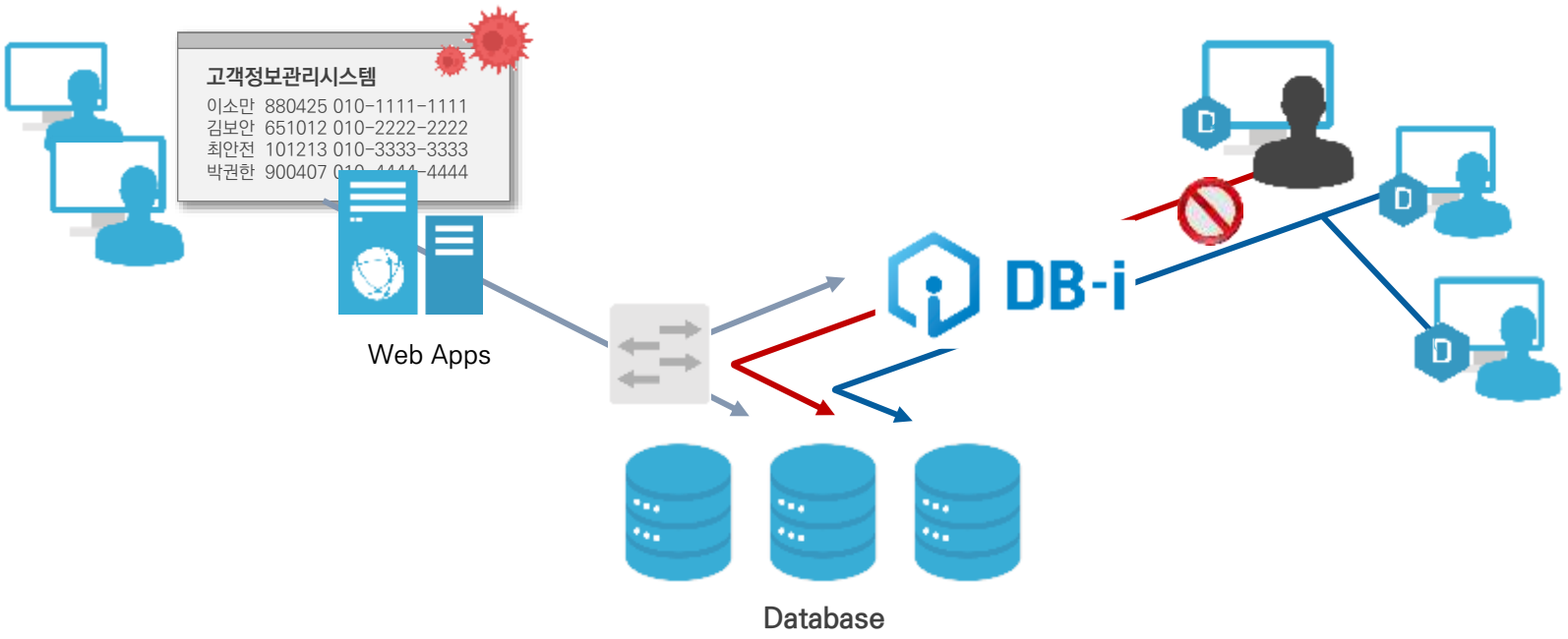
- 개발자 DB직접 접속 통제는 Proxy 방식이 효과적
- Mirror와 Proxy방식의 장점을 혼합한 Hybrid 방식 운영 가능

[Mirror 방식]

고객, 대리점, CRM, VOC, Hacker 조회/취득

[Proxy 방식]

DBA, DB엔지니어, (비권한 엔지니어) 조회/취득



4. 제품 비교표

제품 비교표 :프로젝트 수행역량

항목		소만사 DB-i	P사	W사
클라우드 DB 접근통제 분야 시장 점유율	공공기관 프로젝트 지속 수행경험	**국가정보자원관리원** **광주센터** : 2007년, 2015년, 2022년 3회에 걸쳐 수행진행 **대구센터** : 2023년 클라우드 DB접근통제 프로젝트 수행 **한국지역정보개발원, 행정안전부, 기상청, 전라남도청 외**	국가정보자원관리원 프로젝트 없음	국가정보자원관리원 대전센터
	글로벌 대기업 프로젝트 수행 1위	· 전세계 72개국 197개 거점 22만명 삼성임직원 대상 약 1만 core 규모 **삼성 G-ERP 프로젝트 수행** · 삼성, LG, KT, CJ, 롯데, 두산 그룹 DBMS 표준화 제품 · **엔터프라이즈 시장 1위**	기업 시장 점유율 낮음	
	클라우드 DB 프로젝트 수행 1위	· **3만대 이상** (A사 DB 1만대, B사 6천대, C사 5천대) 수행 · **지역정보개발원** 차세대 클라우드 DB접근통제 프로젝트 · **국정자원관리원 대구센터** 클라우드 DB접근통제 프로젝트 등 DB서버 대수 기준 경쟁사 대비 2배 이상	클라우드 DB접근통제 제한적 (대부분 100여대 DB 보유 사이트 대상)	
	최근 3년 내 공공기관 검증 BMT 1위 실적	**국가정보자원관리원 대구센터 BMT 수행결과 1위** (99.25점/100점 만점기준)	대구센터 BMT 수행결과 2위	대구센터 BMT 수행결과 4위
인증	보안기능확인서	O	O	O
	CC인증	EAL4	EAL4	EAL4
재무	신용등급	A+등급	A+등급	BBB등급
기술 전문성	자체 보유 전문 기술인력	240명(전체인원 340명)	130명(전체 인원 170명)	40명 이하(전체 인원 40명)

제품 비교표 :기능

항목		소만사 DB-i	P사	W사
DB 접근 통제	DBMS 커버리지 (Cloud DB포함)	20여종 이상	20여종 이상	20여종 이상
	계정, 시간, 툴, 채널 별 접근통제	○	○	○
	Table/Column 접근통제	○	○	○
	쿼리툴 통제	○	○	○
	DB접속기록 저장	○	○	○
	소량씩 다회조회 등 비정상 조회행위 탐지 및 경보	○	△	○
서버 접근 통제	RDP/SSH/Telent/FTP 원격터미널 서비스 통제	○	○	△ FTP 파일 다운로드 제한적
	RDP 콘솔 원격접속시 개인정보유출조회 등 모니터링	○	○	X
쿼리툴 통제	**클립보드 통제** (쿼리툴을 통해 외부로 데이터를 붙여넣기할 경우 차단)	○	X	△
	쿼리결과값 통제 (Export, 파일저장시 차단)	○	X	△
	파일저장 통제 (클라이언트 PC에 개인정보 저장시 경고메시지 발송)	○	X	△
로그 저장/ 관리	**법에서 요구하는 세부이력 모두 기록** (사이즈, 행수, 패턴, 반복횟수 등)	○	○	○
	관리자 페이지 개인정보 로그기록 마스킹	○	○	○
	리포팅	○	○	○

5. 프로젝트 관리 및 교육

01. 기술평가등급 T2

02. 프로젝트 수행

03. 기술지원 및 정기적 서비스

01. 기술평가등급 T2

- 기술평가등급 T2 → 기술력 상위 1% 이내
- 200여명 기술인력 보유
- 인프라 구축부터 유지관리까지 단일 벤더에서 일괄지원대응

기업체명	(주)소만사
대표자명	김대환
사업자등록번호	214-86-14882
법인등록번호	110111-1394115
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
산업분류	[J58222] 응용 소프트웨어 개발 및 공급업
유효기한	2024년 08월 08일
제출처 및 용도	적격심사 및 공공기관 제출용

기술평가등급

T2

평 가 일	2023년 08월 09일

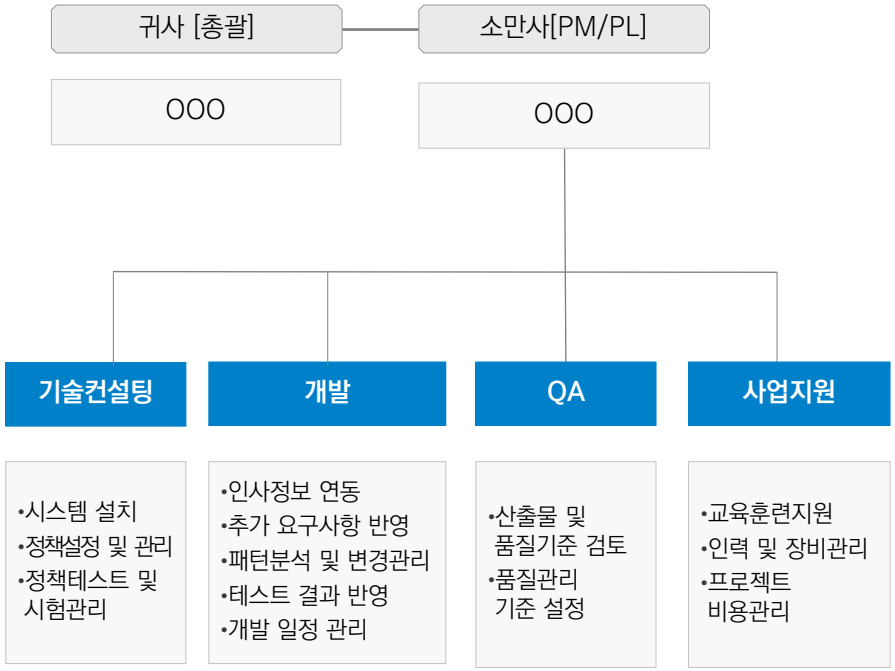
기술평가등급	매우취약	취약	미흡	보통이하	보통			보통이상			양호			우수			매우우수	최우수
	T10	T9	T8	T7	T6-	T6	T6+	T5-	T5	T5+	T4-	T4	T4+	T3-	T3	T3+	T2	T1
	기술력이 매우 우수한 수준으로 산업 및 시장환경의 급격한 변화에도 어느 정도 대응능력을 갖추고 있어 안정적임																	

02. 프로젝트 수행

소만사는 DB-i 구축사업의 성공적 수행을 위해 계약부터 완료까지 귀사와의 유기적 관계를 유지할 수 있는 조직을 구성합니다
또한 완벽한 품질의 산출물이 생성되도록 독립적인 품질보증 팀의 지원을 받아 원활하고 효율적인 프로젝트 수행이 가능하도록 하며,
프로젝트 관리자가 전체 프로젝트 팀을 효율적으로 관리할 수 있도록 조직을 구성합니다

인력확보 방안 및 인적 구성의 적정성

〈 수행 조직 〉



〈 업무분장 〉

조직	역할
귀사	▪ 계약체결, 사업관리 및 사업비 신청내역 확인 ▪ 검사 및 인수, 사후관리 ▪ OOO에서 담당할 필요가 있는 세부적인 업무
소만사 (PM)	▪ 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 품질보증, 투입인력, 자원 및 예산 관리 ▪ 주요 이해당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
소만사 (PL)	▪ 기술적인 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 기술적인 품질보증, 투입인력, 자원 및 예산 관리 ▪ 기술 당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
기술컨설팅	▪ 시스템 설치 및 구축(하드웨어, 소프트웨어 - 운영체제, 로그서버 등) ▪ 정책설정, 관리 및 운영 지원 / 주요 산출물 작성
개발	▪ 추가요구사항 반영/ 패턴분석 및 변경관리/ 테스트 결과반영/ 개발일정관리
QA	▪ 산출물과 품질기준 검토 및 품질관리 기준 설정 ▪ 표준화가 필요한 업무에 대하여 프로세스 및 정보항목 도출 ▪ 표준화 추진방안 제시

03. 기술지원 및 정기적 서비스

교육지원 담당자의 책임아래 교육훈련을 진행합니다
교육준비, 교육실시, 평가 및 분석 3단계로 나누어 시행하여 훈련효과를 극대화 합니다
훈련 실시 후 교육내용 활용도를 조사, 부족한 부분을 추가 교육하여 대상 그룹의 시스템 적응력과 운용능력을 극대화 합니다

교육훈련 일정

교육과정	주요내용	교육일정	교육대상	관련자료/장소
기초교육	▪ 솔루션사용법 – 사용자 환경설정 및 접속방법 – 로그조회 등 감사활동 방법 ▪ 솔루션 개념 및 구축 기법 ▪ 솔루션 시스템 운영 및 활용 방안 ▪ 집합교육	▪ 1일(2시간소요) (프로젝트 초기: M) – 계약 후 4개월이내	▪ 총괄 담당 직원	▪ 운영 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 기본 교육	▪ 솔루션의 운영관리 – 시스템 운영환경(H/W및 S/W)에 대한 이해 – 솔루션 운영교육 – 보안규칙 적용방법 – 모니터링 및 감사활동 방법 ▪ 운영 지침 ▪ 시스템 전반적인 이해 ▪ 각 모듈 별 요소 기술 ▪ 보안관리자 ▪ 매뉴얼 사용 방법 ▪ 집합교육 또는 쿠폰	▪ 1주일(일1시간) (솔루션 설치 완료시: M+1) – 계약 후 5개월이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 심화 교육	▪ 운영단계에서 실제 운영 시 상세 제품교육 ▪ 보고서 활용 관련 리포트 활용법 ▪ 집합교육 또는 쿠폰	▪ 1일(3시간) (시스템 안정화 단계 시: M+2) – 계약 후 6개월 이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정장소

03. 기술지원 및 정기적 서비스

제안사의 운영기술 지원 서비스는 다음과 같이 5가지 영역으로 나뉘어 제공됩니다

유지관리 정책은 검수 후 1년간 무상 지원되며, 이후 별도의 유지관리 계약을 통해서 지속적인 서비스를 제공합니다

운영기술 지원 서비스

구 분	지원 방안	비고
예방정비 (PM)	• 전담 A/S 요원 정기점검 및 요청 시 방문 • 모듈 및 시스템 성능 검사 및 종합 테스트 • 정기적인 이론 실습 교육 • 전산 마인드 교육 • 업무시스템의 효율적인 사용을 위한 교육	• 전담 요원 확보 • 충분한 예비 시스템 확보
긴급정비 (EM)	• 유지관리를 위한 전담 엔지니어 확보 • Help Desk 운영을 통한 신속 정확한 장애 조치 • Diagnostic Program을 통한 정확한 고장부위 파악 및 조치	• 4시간 이내 착수하여 조치 이행함
서비스망 접수처리	• Help Desk를 구축 신속한 장애 접수 처리	• 상시 지원 체제 구축
기술지원	• Version Upgrade 관련 최신 기술정보 제공 • 대상 업무 검토 및 협의 • 시스템 성능향상을 위한 기술자문 및 신기술 세미나	• 유지관리 전담팀 활용
무상유지관리 기간	• 시스템 구축 후 1년	

03. 기술지원 및 정기적 서비스

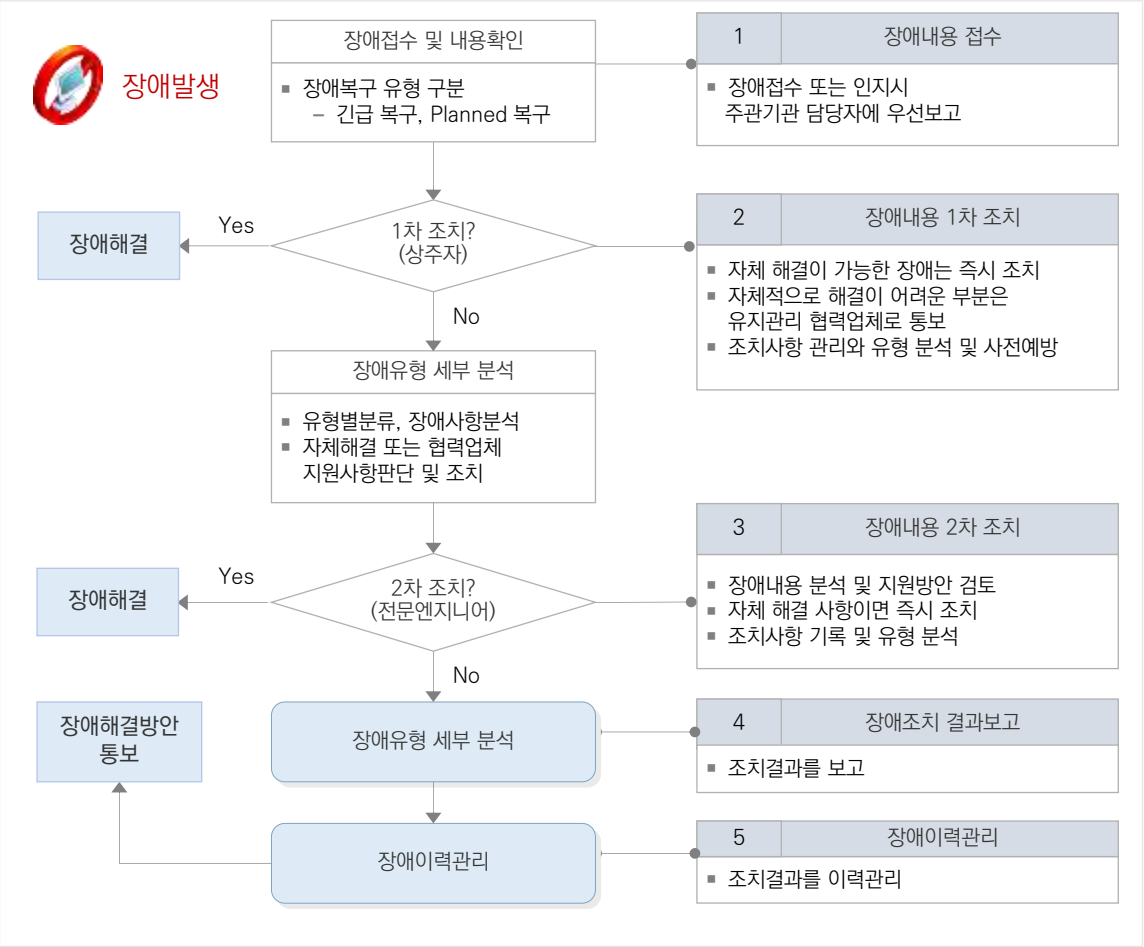
1,000여개 유지관리 사이트 지원경험과 200여명의 전문가를 통한 대응체계를 고객에게 제공합니다

03. 기술지원 및 정기적 서비스

제안사 기술컨설팅 단일창구를 통해 장애접수 후

유지관리팀 및 주관기관 내 자체 운영조직에 의한 해결 또는 협력업체 현장방문으로 신속히 장애문제를 조치합니다

절차에 의한 체계적이고 신속한 장애처리



장애복구 유형별 조치방안

구분	내용	조치 담당자	비고
긴급 복구	장애요소제거 및 교체	유지관리 담당자	유지관리 수행팀은 전단계에 걸쳐 지속적인 지원
	시스템 (HW 및 SW) 가동	시스템 및 SW 운영자	
	서비스 가동 및 확인	업무담당자	
Planned 복구	복구작업 계획수립	관련자 전체	
	서비스 및 시스템 중지	업무담당자, 시스템 및 SW 운영자	
	장애요소 제거 및 교체	유지관리 담당자	
	시스템 및 서비스 가동, 확인	시스템 및 SW 운영자, 업무담당자	

성공적인 프로젝트로 보답하겠습니다

감사합니다

SOMANSA

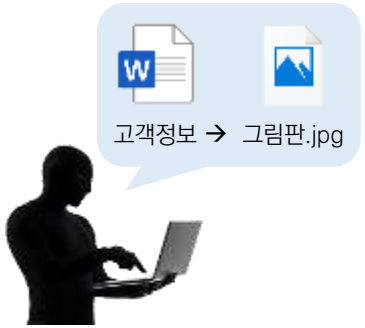
서울특별시 영등포구 영신로220 KnK디지털타워 9층 소만사
대표번호 : 02-2636-8300 | 기술문의 : tech@somansa.com
제품구매 : 02-2655-4040 / sales@somansa.com

별첨: DB 유출통제 * 별도 라이선스 필요

차별화 기능 **개인정보 패턴 식별 탐지 통제 : 포맷변조, 다중압축파일 100% 탐지**

확장자 변경 파일검출 (예: docx → jpg 변경)

- 원본포맷이 변조된 파일에서도
  원본파일 확장자 식별 및 누락 없이 패턴 검출
- 한글, 오피스, PDF 등 50여개 파일포맷 위변조 모두 탐지



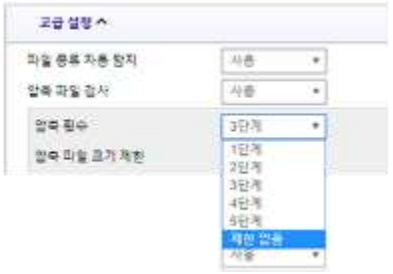
❶ 개인정보파일 확장명
변경 (docx → jpg)

❷ DB-i에서
누락없이 패턴 검출

다중압축파일 검사 및 분석

- 다중압축파일 내 개인정보파일을 정확히 식별
- 압축 횟수 검사 단계별 설정가능

〈검사 설정〉



❶ 보안담당자가 압축파일 내
모든 파일을 일일이 찾을 필요없음

❷ DRM 문서를
5단계로 압축해도 검출

USB 등 외부저장매체
파일복사 반출 시 탐지

DB CLOB, BLOB 필드 내
개인정보파일 분석탐지

FTP(SFTP)/RDP로
개인정보파일 다운로드 시 분석탐지

별첨: DB 유출통제 * 별도 라이선스 필요

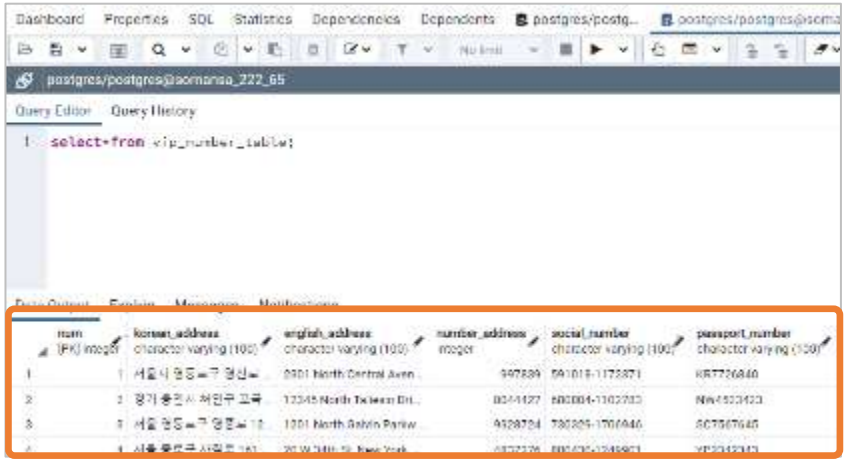
차별화 기능

DB접속 후
개인정보 파일 저장 시 실시간 경보

Example

- DB Apps(Query Tool)에서 데이터를 파일로 내보내기(Export)시 경보
- DB Apps DB조회값 개인정보를 Excel로 Copy& Paste하여 파일 저장
- FTP/RDP로 다운로드 받은 파일 PC에 저장

DB Apps(Query Tool)에서 데이터를 파일로 내보내기(Export)시 경보



쿼리툴 사용하여 'vip_number_table' 테이블 개인정보 조회,
PC에 '핵심고객정보파일'로 내보내기 (Export)

고유식별정보를 포함하는 개인정보 파일이 생성된 경우
실시간 경보 및 알림창 팝업

별첨: DB 유출통제 * 별도 라이선스 필요

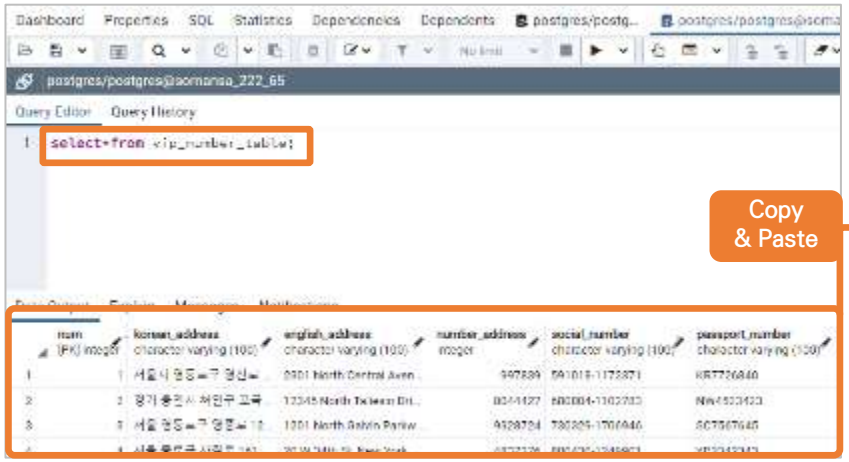
차별화 기능

DB접속 후
개인정보 파일 저장 시 실시간 경보

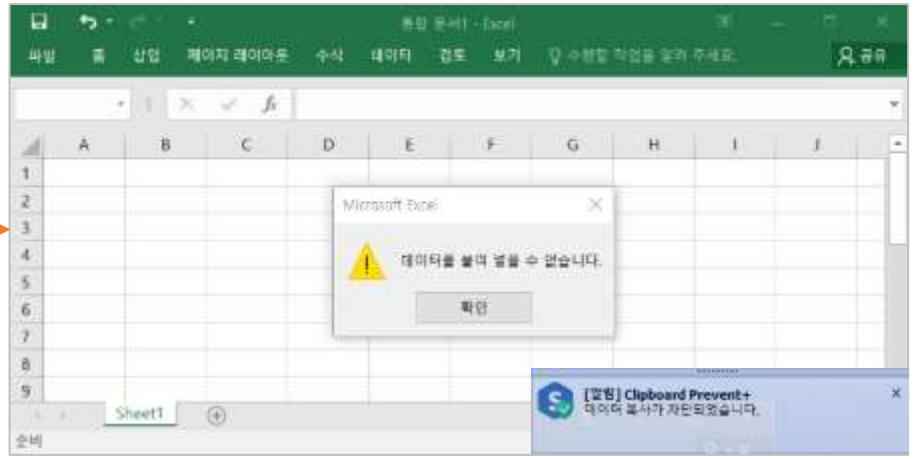
Example

- DB Apps(Query Tool)에서 데이터를 파일로 내보내기(Export)시 경보
- DB Apps DB조회값 개인정보를 Excel로 Copy& Paste하여 파일 저장
- FTP/RDP로 다운로드 받은 파일 PC에 저장

DB Apps DB조회값 개인정보를 Excel로 Copy& Paste하여 파일 저장



Copy & Paste



쿼리툴을 사용하여 'vip_number_table' 테이블 내 개인정보 조회

쿼리 응답값 복사(Ctrl+c)하여 엑셀파일에 붙여넣기(Ctrl+v)할 경우 **개인정보 포함시** 데이터 복사 차단

별첨: DB 유출통제 * 별도 라이선스 필요

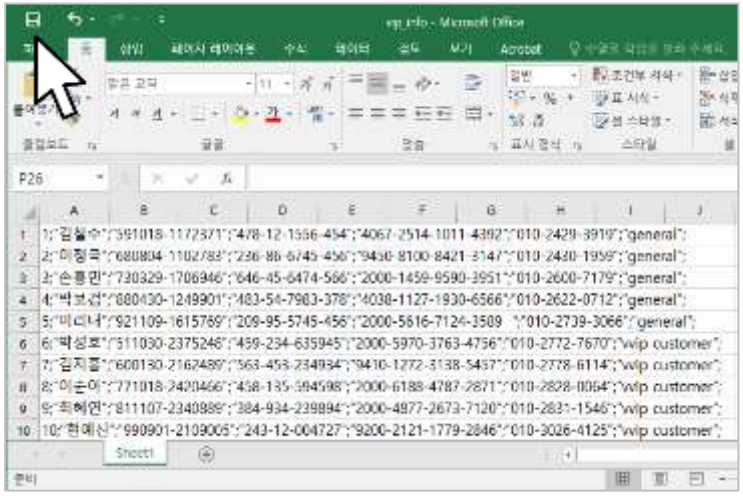
차별화 기능

DB접속 후
개인정보 파일 외부유출방지

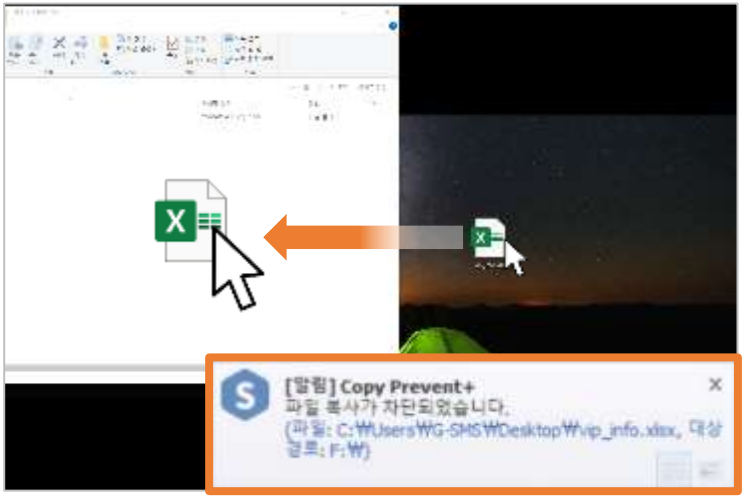
Example

- USB, 외장하드 등을 통한 개인정보 복사반출
- 출력물을 통한 개인정보 외부반출
- 웹메일, SNS 등을 통한 개인정보 외부전송

USB 반출 통제



엑셀파일에 고유식별정보 저장



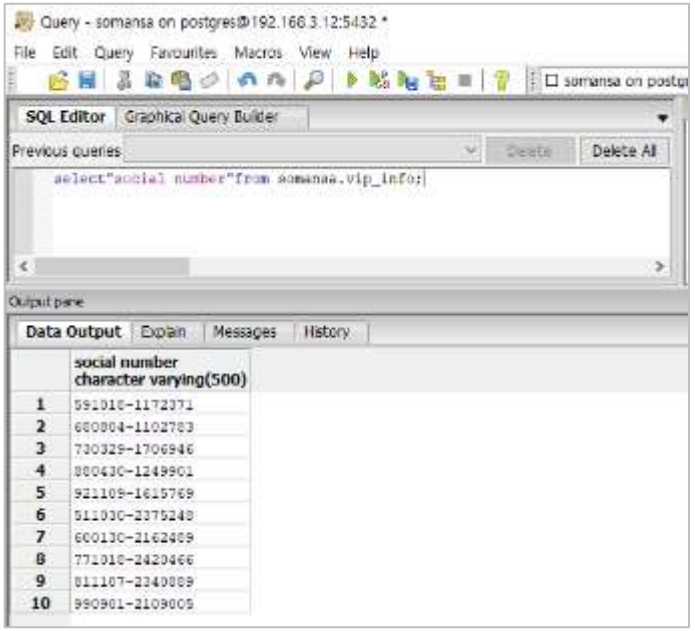
차단 정책에 의해 USB 파일복사시
차단정책에 의해 UB 파일복사 차단

별첨: DB 유출통제 * 별도 라이선스 필요

차별화 기능

DB접속 후
개인정보 파일 외부유출방지

출력 통제



개인정보 조회 후 쿼리 결과값 복사

1 워드파일에 주민번호 1건 저장 후 출력 시
워터마크 포함되어 출력허용

2 워드파일에 주민번호 10건 저장 후 출력 시
출력차단과 동시에 출력시도기록 로그저장

별첨: DB 유출통제 * 별도 라이선스 필요

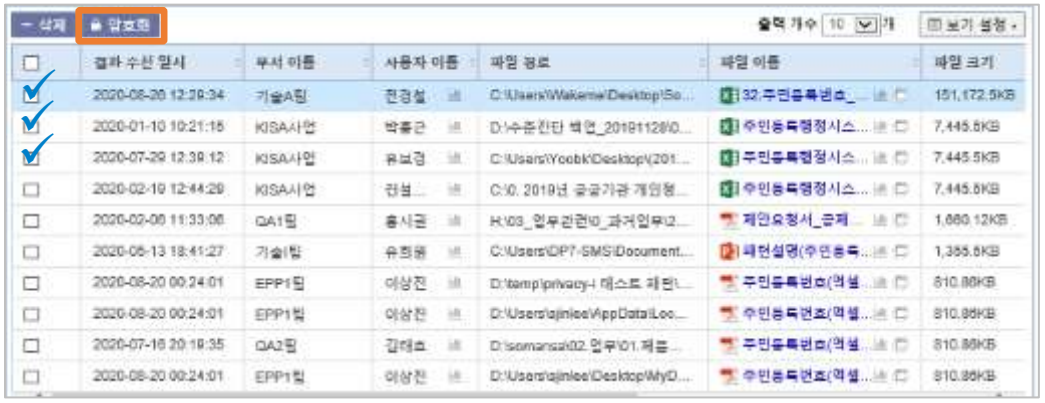
차별화 기능 DB접속 PC 내 개인정보 파일 암호화 (2차유출방지)

- DB접속 후 PC에 생성된 개인정보파일 검색, 중앙에서 암호화
- 특정조건에 해당하는 파일을 조회한 후,
  해당 로그정보 유출 시 심각도가 클 경우
  중앙에서 원격으로 암호화

개인정보보호법 고시 준수 **7조 개인정보 암호화**

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에
고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어
또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장해야 함

DB접속 및 개인정보 조회 후
쿼리 결과값 PC 저장



- 업무환경, 파일성향에 따라 자동 암호화 or 동의 받은 후 암호화
- 활용여부에 따라 즉시 암호화 or 예약일자에 맞추어 암호화

별첨: DB 유출통제

제품 비교표

항목	DB-i	P사	W사	비고
개인정보포함 DB Data 자동식별	○ Table, Column, CLOB, BLOB, 이미지, 서버 내 파일 검출 경보	△ CLOB, BLOB, 이미지 미흡	△	
관리용 단말기 보호/유출통제 기능	○ DB접속 단말기 보호기능 (내PC지키미 수준)	△	△	개인정보 법규준수
DB접속 후개인정보 PC 저장시 실시간 경보	○ 개인정보 파일 PC저장시 실시간 경보	△	△	1천만 건 이상 개인정보 유출사고 재발방지
DB접속 후 개인정보 데이터 Copy & Paste 통제	○ Clipboard 통제	△	△	
DB접속 후 개인정보 USB복사, 출력, 네트워크 반출 통제	○ 개인정보 유출사고 방지	△	△	
빅데이터 검색기능	○ 3년치 대용량 접속로그 1~3분내 검색가능	△ DB방식	△ DB방식	
높은 개인정보 패턴 정합성	○ 10가지 이상 패턴 제공 고유식별정보 체크섬 3개 보유	△ 제한적 고유식별정보 체크섬 2개	△ 제한적	
파일 포맷변조, 다중압축파일 탐지	○ 위변조를 통한 유출시도 탐지	△ 제한적	△ 제한적	

차세대 안티바이러스
(Next Generation Anti-Virus)

Privacy-i EDR V 7.0

목차

1. 회사소개

01. 엔드포인트 시큐리티 1위기업 소만사

02. 재무 안정성 상위 1%

03. 조직 및 기술력

05. 보안성 지속서비스

06. 레퍼런스

01. 엔드포인트 시큐리티 1위기업 소만사

1997년 창립 이후 27년간 데이터보호에 집중한 '엔드포인트 시큐리티 전문기업'

2024

글로벌 3대 바이러스 연구기관 Virus Bulletin사의 'VB 100' A+등급 획득

Privacy-i EDR 2.0 출시 : 싱글 에이전트로 데이터보호 및 유출통제 동시지원

Server-i 5.0 출시 : 서버 취약점 점검 솔루션

2023

Privacy-i 지키미 출시 : PC 취약점 점검 솔루션

Privacy-i 리눅스OS 버전 국내최초 개발

2022

Privacy-i EDR 1.0 출시 : 엔드포인트 위협탐지 및 대응 솔루션

Gartner Magic Quadrant 'Enterprise DLP' 보고서 아시아 최초 등재

Privacy-i macOS 버전 국내최초 개발

2021

WebKeeper SG 출시 : SSL/TLS 기반 유해사이트 차단

Privacy-i DLP 버전 출시 :복사, 출력, 인터넷 업로드 통제

고객사 1,000개사 달성 (공공/금융/기업 등)

1998

Privacy-i Discover 출시 : 국내 최초 개인정보 검출 및 보호조치 솔루션

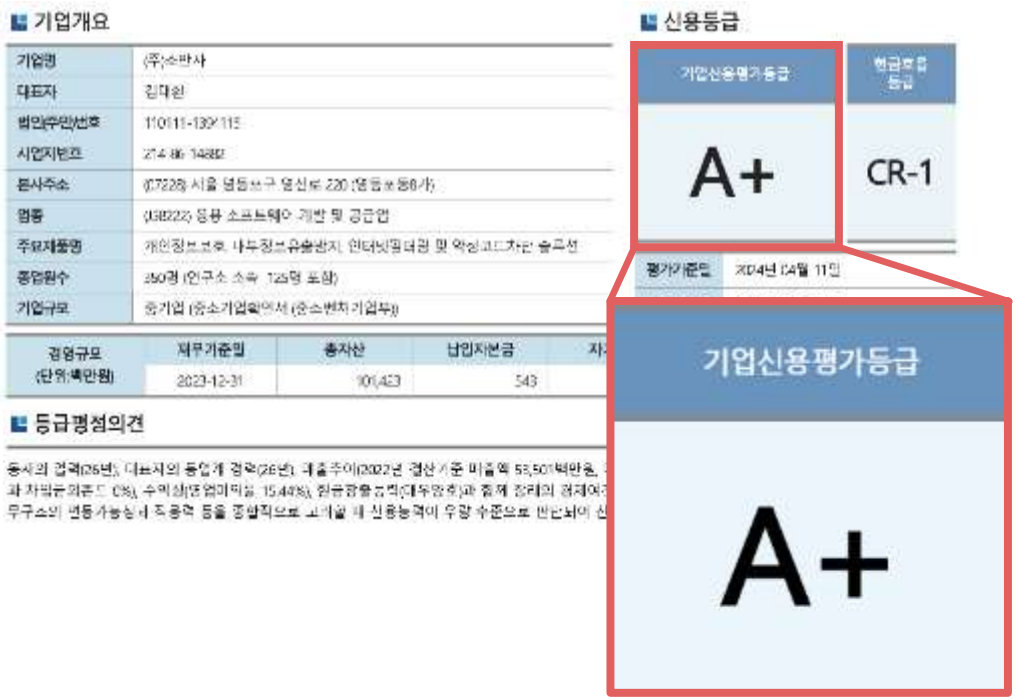
1997

WebKeeper 출시 : 유해사이트 차단 솔루션

㈜소프트웨어를 만드는 사람들 설립

02. 재무안정성 상위 1%

- 중소기업 재무안정성 상위 1%(A+), 유일한 무차입 기업입니다
- 신용평가 A+, 현금흐름등급 CR-1로 중소기업 상위 1%의 재무적 안정성을 바탕으로
  소만사는 중장기 R&D 및 기술지원에 투자하고 있습니다

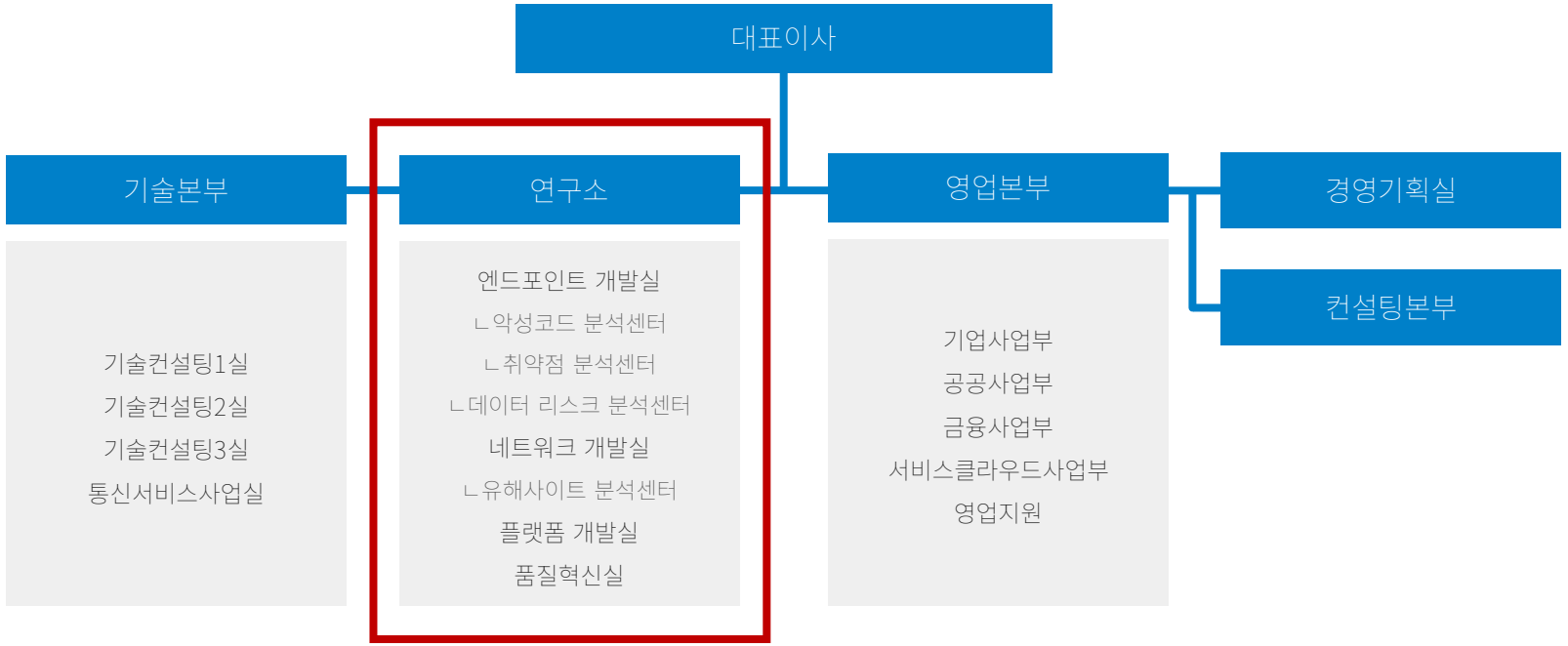


(단위: 억원)

구 분	2022년	2023년	2024년
매출액	535	577	653
영업이익	83	124	145
당기 순이익	88	140	161
차입금	0	0	0
총자산	847	1,014	1,221

03. 조직 및 기술지원능력

- 소만사 임직원 350명 중 240여명이 기술인력(약 70%)으로 재직중입니다
- 연구개발자 120여명, 기술엔지니어 120여명 재직
- 악성코드 분석센터 (악성코드/랜섬웨어 분석), 취약점 분석센터 (엔드포인트 보안 플랫폼 개발, 취약점 분석), 데이터 리스크 분석센터 (개인정보/기밀정보 유출차단), 유해사이트 분석센터 (악성코드/유해사이트 분석) 운영
- 컨설팅 본부 (50여개 주요기반 시설 취약점 점검 프로젝트 수행)



03. 조직 및 기술력 : 인증 및 지적재산권

- 엔드포인트 보안 솔루션으로 CC인증, GS인증 획득
- 데이터 유출 및 악성코드 차단 등 핵심특허 20건 이상 등록출원

인증 수상

CC 인증

GS 인증

국정원 암호검증모듈 탑재

등록/출원 특허

- 악성행위정보에 근거한 악성코드 자동 분류방법 및 장치
- 엔드포인트의 트래픽에 대한 포워딩 시스템 및 방법
- 파일 시스템에 저장된 중요정보의 검사방법 및 장치
- 금융사기 방지 시스템 및 방법
- 엔드포인트 DLP를 위한 2계층 기반의 기밀 정보 검출 시스템 및 방법
- 가상화 기반 논리적 망분리 기법을 이용한 개인정보보호시스템
- (미국) System and method for tracking information leakage at endpoint

03. 조직 및 기술력 :

영국 바이러스 연구기관 바이러스 불러틴 'VB 100' A+ 인증 획득

오탐율 0%, 탐지율 99.53%로
2023년 1분기부터 2024년 2분기까지
지속적으로 A+ 등급 유지 중

	항목	차단율
바이러스 불러틴 VB100 탐지 결과	오탐율	0%
	탐지율	99.52%

04. 보안 지속성 서비스:

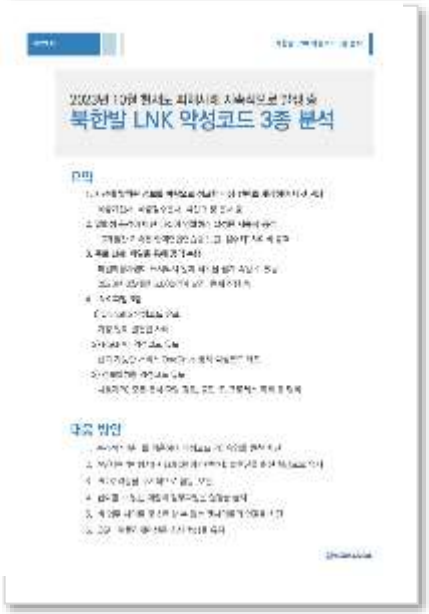
악성코드 랜섬웨어 분석리포트 월간 발행 및 배포

2015년 한글 악성코드 분석 보고서부터 2024년 와이퍼 악성코드까지

9년 연속 악성코드/랜섬웨어 상세분석 및 보고서 발행

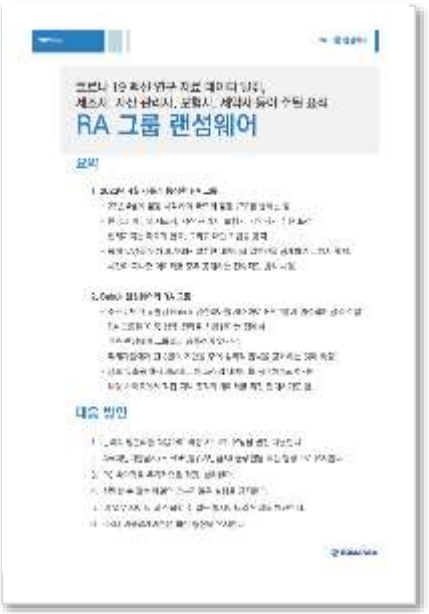
2024.02
친팔레스타인 단체 개발 인프라 파괴 목적
BiBi 와이퍼 악성코드

2023.10
Chinotto,RokRAT 정보탈취형 3종
북한발 LNK 악성코드분석



2024.01
CVSS위험도 최고점 10점 중 7.8점 평가
WinRAR 원격코드 실행 취약점

2023.06
코로나19 백신 연구데이터 1.4TB 탈취,
RA 그룹 랜섬웨어



04. 보안 지속성 서비스: 악성코드 배포 웹사이트 분석

국내 최대 DB 수집 → 분석 → 배포 인프라 확보

1천여개 소만사 고객사를 통해 실시간으로 축적되는 데이터 인프라 보유

수집

사이트 리포터
1,000여개 국내 고객사에서
미분류 접속 사이트 자동수집

시큐랩닷컴
보안담당자 미분류 사이트 직접신고

키사이트 콜렉터
검색엔진 키워드별 검색결과 자동분류

분석

AI 인공지능기반 자동 분석센터
웹사이트 내 이미지, 텍스트를 추출하여
비업무, 유해, 불법, 음란사이트 여부를 자동 판단

Google, KISA 등 DB 분석
공신력 있는 기관 제공 악성코드DB 3종 이상 보유

전문가로 구성된 자체 분석센터
1~4차 분석프로세스 제공,
피해규모가 큰 악성코드/랜섬웨어는 상세리포트 제공

배포

30분 이내 배포
수집-분석-배포까지
30분 이내

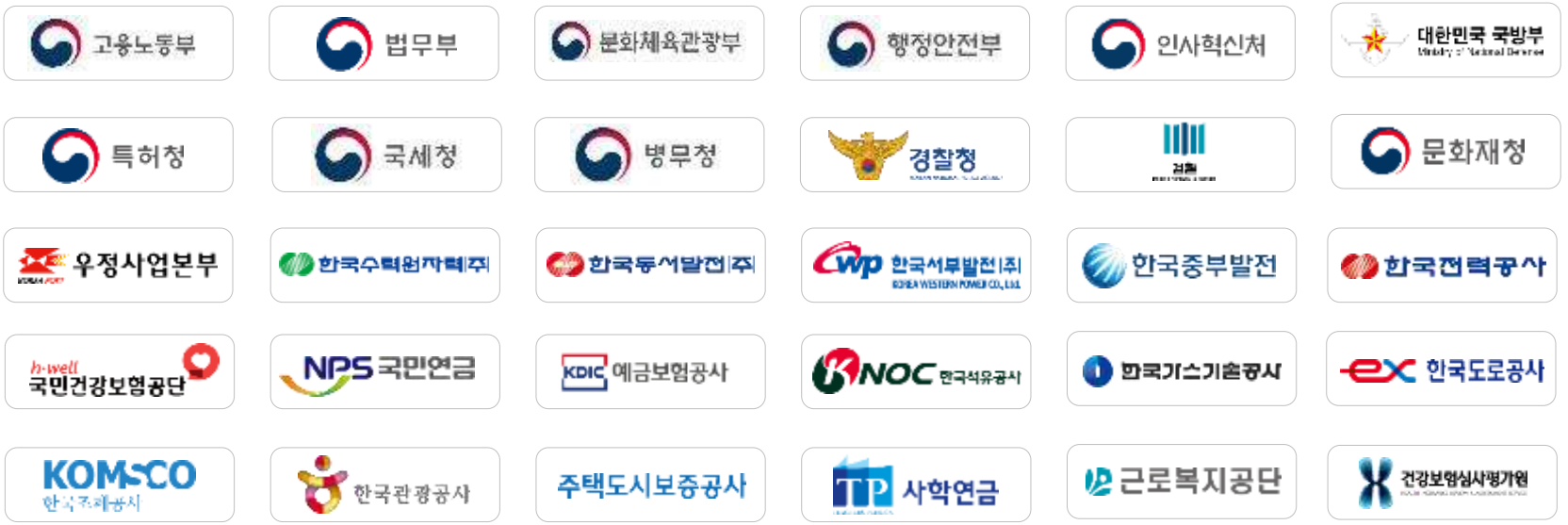
주기적 재검증
24시간
DB 최신화 작업수행

06. 레퍼런스

에이전트
도입 대수 1위

Privacy-i EDR은 엔드포인트 보안 솔루션 Privacy-i의 최신버전입니다
기존 Privacy-i 고객사는 순차적으로 Privacy-i EDR 업그레이드 예정입니다

중앙부처, 공기업 및 공공기관



* Privacy-i 엔드포인트 보안 솔루션 적용 사이트이며, 현재 EDR 버전으로 업그레이드 중

06. 레퍼런스

교육청 제품도입 1위

광역지방자치단체, 교육청, 병원 Privacy-i 도입

교육청 고객 50% 확보, Privacy-i 사용 중

지자체 및 교육청

서울특별시 | 경기도 | 대전광역시 | 대구광역시 | 행복충만 충청남도 | 휴먼시티 수원

안양시 | 고양시 | 경기도교육청 | 부산광역시교육청 | 인천광역시교육청 | 전라북도교육청

충청북도교육청 | 충청남도교육청 | 경상남도교육청 | 제주특별자치도교육청 | 서울시농수산식품공사 | 서울시설공단

병원

SAMSUNG 강북삼성병원 | SAMSUNG 삼성서울병원 | SAMSUNG 삼성창원병원 | 연세대학교 의료원 | 고려대학교안암병원 | 인제대학교 백병원

대전한방병원 DAEJEON UNIVERSITY | 경상대학교병원 | 국립목포병원 | 보건복지부 국립부곡병원 | 국립나주병원 | 국민건강보험 일산병원

* Privacy-i 엔드포인트 보안 솔루션 적용 사이트이며, 현재 EDR 버전으로 업그레이드 중

06. 레퍼런스

금융시장 1위

주요 금융사(은행, 생명, 화재, 카드, 증권 등)에서 Privacy-i 도입 및 운용 중
S사 등 외산 솔루션 윈백(Win-Back) 사례 다수 확보

금융

KB국민은행 | 하나은행 | 신한은행 | 수협 | DGB대구은행 | 전북은행
한국수출입은행 | KB생명보험 | 하나생명 | NH농협생명 | KYOBO 교보생명 | Heungkuk 흥국생명
한화생명 | MIRAE ASSET 미래에셋생명 | Cigna 라이나생명 | AIA 생명 | 수호천사동양생명 | KB손해보험
DB손해보험 | AIG 손해보험 | Heungkuk 흥국화재 | KB국민카드 | Hyundai Card | SAMSUNG 삼성카드
비씨카드 | KB증권 | 삼성증권 | 하나대투증권 | meritz 메리츠증권 | MG새마을금고중앙회
하나금융지주 | KB금융지주

* Privacy-i 엔드포인트 보안 솔루션 적용 사이트이며, 현재 EDR 버전으로 업그레이드 중

06. 레퍼런스

엔터프라이즈 1위

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

기업

삼성전자 · 삼성물산 · 삼성전자판매 · 삼성전자서비스 · 삼성웰스토리 · 삼성에버랜드
THE SHILLA · 삼성SDS · LG전자 · LG화학 · LG디스플레이 · LG유플러스
LG상사 · LG이노텍 · LG엔시스 · LG패션 · LG CNS · kt
kt skylife · SK하이닉스 · SK텔레콤 · SK이노베이션 · SK텔링크 · SK E&S
posco · posco 포스코ICT · posco 포스코건설 · posco 포스코에너지 · posco 포스코알텍 · LS
LS산전 · S-OIL · NCSOFT · DOOSAN · 금호아시아나

* Privacy-i 엔드포인트 보안 솔루션 적용 사이트이며, 현재 EDR 버전으로 업그레이드 중

2. 도입 필요성

01. 전통적인 엔드포인트 보안솔루션의 한계

02. 사후분석 무용론

03. 파일리스 공격(Fileless Attack)에
    가장 효과적인 방어방식

04. 랜섬웨어 공격에 가장 효과적인 방어방식

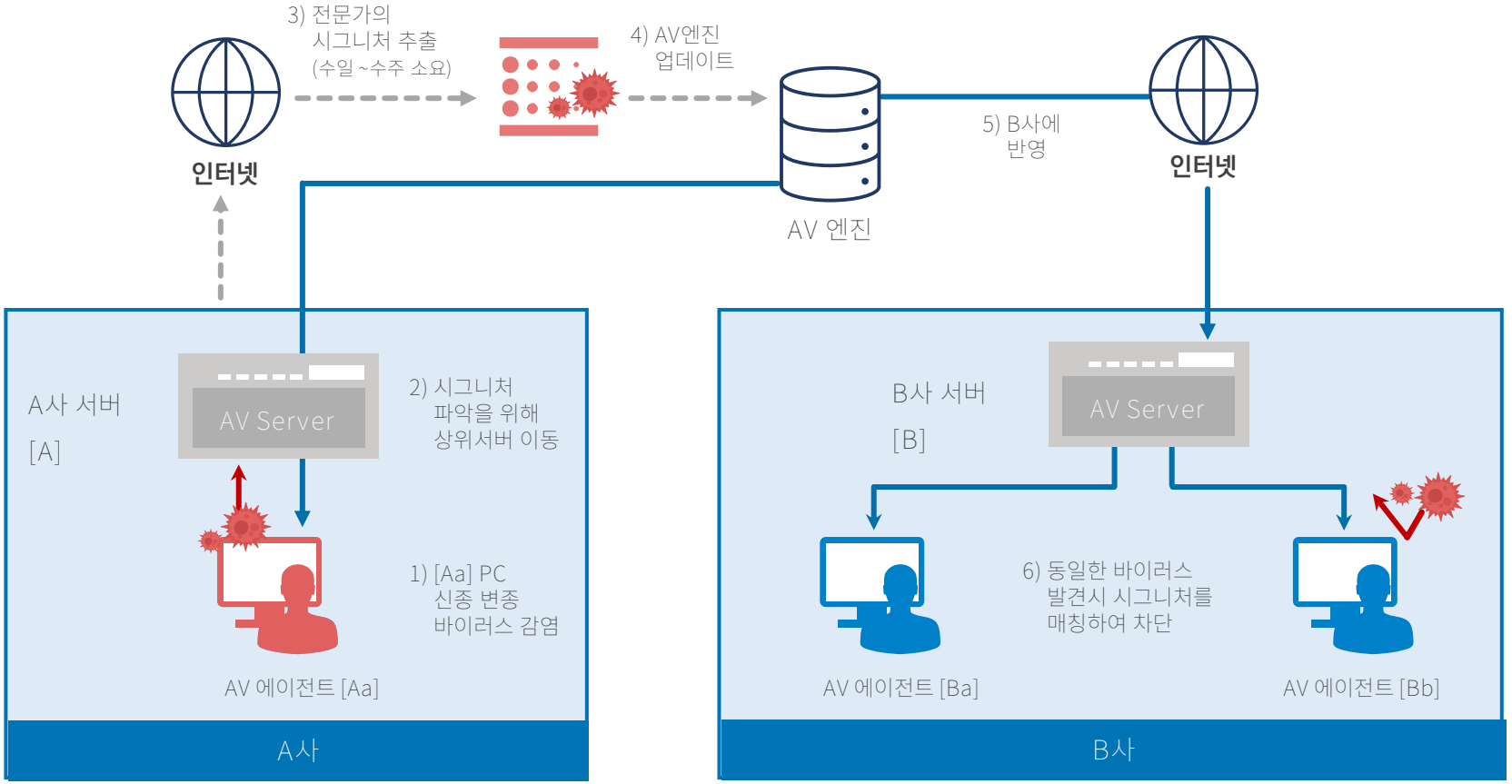
05. 경계선 보안 솔루션 역할 축소

06. 요약

01. 전통적인 엔드포인트 보안솔루션의 한계

안티바이러스

- 추출한 시그니처를 대조하여 악성여부를 판단하는 패턴매칭 방식 사용
- 안티바이러스 엔진 적용에 수일 ~ 수주 소요



02. 전통적인 엔드포인트 보안솔루션의 한계

전통적 안티바이러스 솔루션 한계점

- 가장 대중적인 보안 솔루션이나 패턴기반 차단방식 사용
- 제로데이 어택 및 신/변종 바이러스에 취약, 실시간 대응역량 부족

항목	안티 바이러스 엔진	비고
악성코드 식별	파일 내 패턴(시그니처) 기반	
변종 악성코드 대응	변종 악성코드의 파일 내 패턴식별 후 대응	패턴 추출에 Hour to Days 변종 악성코드는 하루에도 수만 여개 발생
제로데이 공격 대응	취약점 분석 후 패턴 업데이트	취약점 분석에 수 일 ~ 수 주가 소요될 수 있음 그 사이 감염 PC가 기하급수적으로 확산될 수 있음
신규 악성코드 발생시 대응	악성코드 샘플 수집 → (수작업) 패턴 추출 → 패턴 업데이트	악성코드 샘플수집, 분석, 배포의 자동화 측면에서 한계
오탐 가능성	패턴기반으로 차단 오탐 가능성 상대적으로 낮음	

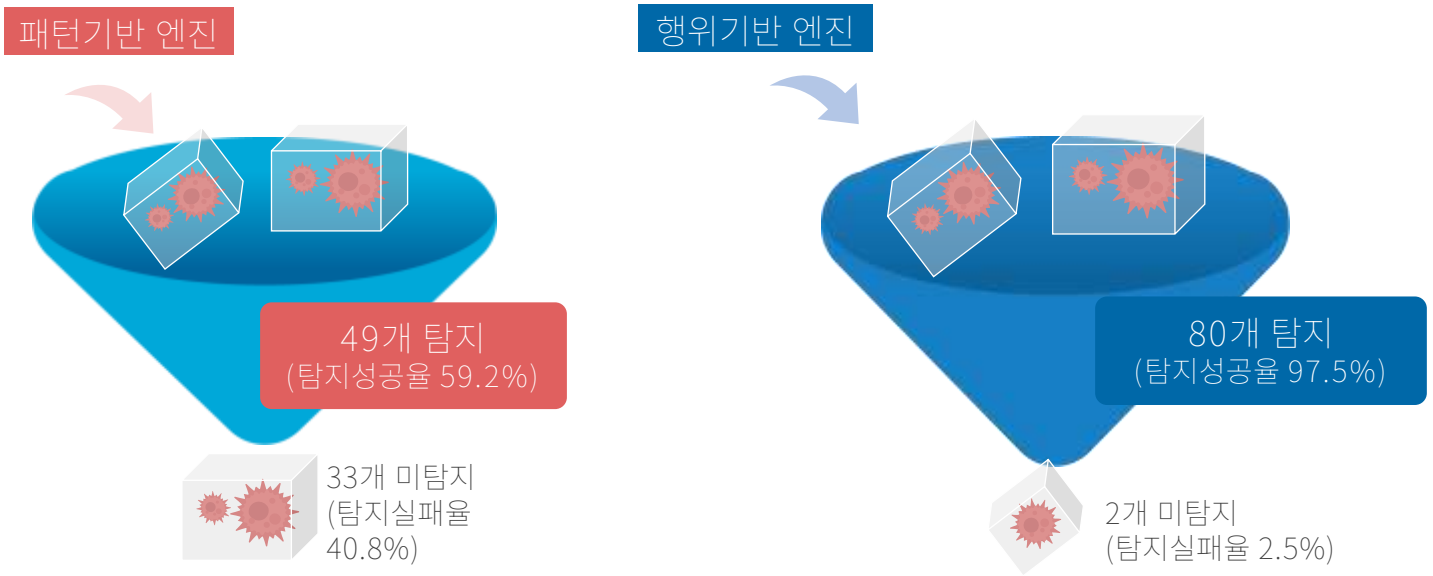
02. 전통적인 엔드포인트 보안솔루션의 한계

안티바이러스

랜섬웨어 변종(실행압축) 여부에 따른
패턴기반(안티바이러스) 및 행위기반 엔진 탐지율 테스트 시행

알려진 랜섬웨어는
패턴기반/행위기반 엔진 모두 100% 차단

변종 변환된 82개 랜섬웨어 대상 탐지 테스트
(2021.08)



변종에 취약한 패턴기반 엔진으로는 사내 데이터를 온전하게 보호할 수 없음

02. 사후분석 무용론

사후분석 무용론

Endpoint의 Event를 한 곳으로 모아서, 사후에 분석한다.

항목	이슈	비고
누가 분석을 할 것인가	일반 보안전문가가 아닌 악성코드 분석 전문가가 필요	대기업 이외에는 악성코드 분석 전문가가 내부에 없으며 채용으로 인력을 확보하는 것도 불가능
기존 보안관제 인력이 EDR로 분석이 가능한가	관제 전문가는 악성코드 분석 불가	
그런 사람을 유지하는데 얼마나 많은 비용이 소요되는가	2~3인팀으로 운영되어야 하며 인건비만 연간 3~5억 소요	운영 인력비용이 솔루션 도입 TCO를 압도함 대기업 이외는 불가능
이러한 사후분석이 어떤 의미가 있는가	사고를 막지 못하고 로그만 남으면 CISO에게는 로그가 없는 것보다 더 큰 문제	

EDR 또한 악성코드 선제적 차단 역할에 초점을 두어야 함

03. 파일리스 공격(Fileless Attack)에 가장 효과적인 방어방식

파일리스 공격

- 아래 파일리스 공격의 특징: 실행 3단계 모두 파일 생성없이 메모리에서 스크립트가 실행됨
- 파일이 생성되지 않으므로 시그니처도 없음. 안티바이러스 엔진은 탐지 불가

요즘 해커 무기는 '파일 없는' 공격

'파일리스' 수법 기승…로깅 강화·EDR 솔루션 활용 필요

김국배 기자 2020.10.26 16:36

2016년 미국 대선 당시 민주당 전국위원회 해킹부터 지난해 국내 400개 이상의 조직을 감염시킨 '클롭' 랜섬웨어, 국내 대기업을 감염시킨 '마이킹즈 봇넷' 공격까지.
이 사건들의 공통점은 바로 파일 없는 공격 '파일리스' 공격기법이 쓰였다는 것이다.
파일리스는 악의적인 기능을 수행하는 코드를 메모리에서만 실행시키며 시스템에 피해를 입히는 공격 유형이다. APT 공격이 이뤄진 침해 사고에서 파일리스 기법이 많이 발견되면서 '지능형 휘발성 위협(AVT)'라는 말까지 생겨났다. 2018년부터는 국내에서도 파일리스 기법이 쓰인 침해사고가 확인되기 시작했다.

스크립트가 악성코드 실행파일을
디스크에 남기지 않고,
신뢰할 수 있는 프로세스에 주입하여 실행/공격

2024.5, 모 스크린 스포츠 업체
랜섬웨어 감염 및 221만명 개인정보 유출
과징금 75억원 부과

2016.12, 미 민주당 전국위원회(DNC)
클린턴 후보 측근을 포함한
이메일 1만9천건 유출

공격 도중에 사용되는 파일이 없음

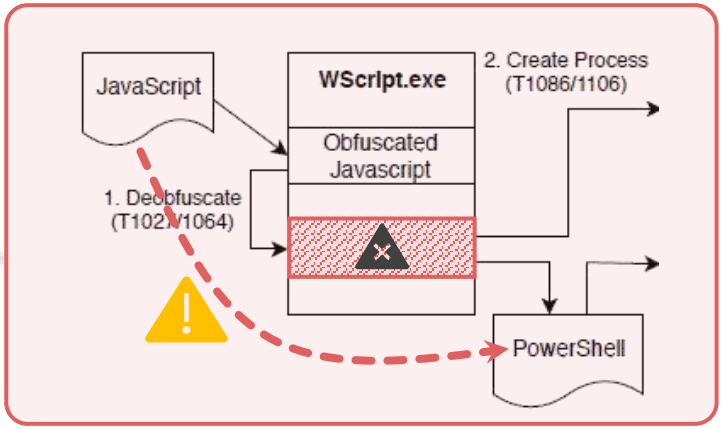
파일 내 시그니처를 기반으로 악성코드를 탐지하는 안티바이러스는 탐지불가

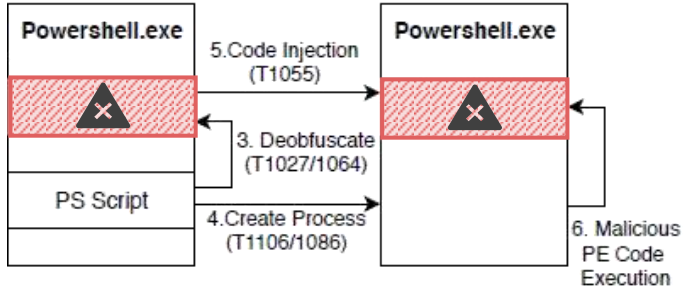
단, 행위기반 탐지방식의 Privacy-i EDR은 탐지가능

03. 파일리스 공격(Fileless Attack)에 가장 효과적인 방어방식

파일리스 공격

- 파일생성시 나타나는 시그니처가 없으므로 패턴기반 안티바이러스는 탐지불가
- 행동기반 탐지방식은 원인-결과를 중심으로 악성행위 판별차단





파일이 없어 스크립트를 읽을 수 없으므로
대신 행동으로 탐지

자바스크립트 실행 후, 파워쉘 실행

→ 이 행동 자체를 의심스럽게 보고 추적

악성행위로
판단,
실행 종료

실행 종료 후 가상환경에서 시뮬레이팅
프로세스 분석 후 TI 배포 업데이트

패턴기반 탐지방식으로는 불가능

오직 행위기반 탐지방식으로 대응할 수 있음

04. 랜섬웨어 공격에 가장 효과적인 방어방식

랜섬웨어 공격

- 랜섬웨어 감염은 주로 엔드포인트 PC 부터 시작
- 랜섬웨어는 끊임없는 변종을 통해 기관/기업을 공격, 오직 행위기반으로만 탐지 가능

미국 보험사 CNA, 랜섬웨어 감염 "1만5천대 기기 타격"

최근 금융업계 겨냥 랜섬웨어 공격 ↑

최은정 기자 2021.03.29 06:50

미국 대규모 보험사 CNA가 신규 랜섬웨어인 '피닉스 크립토락커' 공격으로 온라인 서비스가 중단되는 등 사업 운영에 차질을 빚은 것으로 나타났다.

CNA는 피닉스 크립토락커에 감염돼 약 1만5천개의 기기가 암호화 된 것으로 파악됐다. 감염된 기기에는 가상사설망(VPN)으로 접속한 원격근무 직원들의 PC도 포함됐다.

CNA는 같은 날 홈페이지를 통해 "정교한 사내 네트워크가 중단됐으며 회사 이메일 다"

몸값 40만달러 지불
(한화 약 5억원)

400여 개 병원 운영하는 UHS, 랜섬웨어 공격 받아 시스템 마비…한국도 주의

랜섬웨어 공격받아

길민권 기자 2020.10.04 12:31

병원/의료 서비스 업체 UHS가 9월 28일 네트워크에서 발생한 랜섬웨어 공격으로 인해 미국전역 의료시설 시스템을 중단시키는 사태가 발생했다.

캘리포니 컴퓨터와 전화 시스템에 접근할 수 없었다 C를 포함한 미국 UHS 병원에서 컴퓨터와 전화 시스템에 접근할 수 없었다고 밝혔다. 공격을 받은 병원은 구급차를 타 병원으로 연결하고 원으로 이송하고 있는 상황이다. 실험실, 어떠한 컴퓨터에도 액세스할 수 없었고 P 수 없게 된 것이다. 바로 랜섬웨어 공격에

몸값 지불 거부
시스템 및 인프라 복구비용
6,700만달러 예상
(한화 약 760억원)

엔드포인트에서 실시간으로 행위기반 탐지, 대응하는 EDR은

랜섬웨어 대응에 가장 최적화된 솔루션

05. 경계선 보안 솔루션 역할 축소

클라우드·모바일 컴퓨팅 환경 변화

업무환경 변화로 클라우드·모바일 컴퓨팅 기반 근무환경 보편화

사무실 밖 장소제한 없이 회사 시스템 접속 및 업무진행 가능

회사 내부망과 외부망의 경계가 희미해짐

경계선 보안(Perimeter Security) 개념 무력화

사무실을 벗어난 PC는
사내 네트워크 보안장비의 보호를 받을 수 없게 됨

결국 엔드포인트 단말의
보안기능을 강화하여 정보자산을 보호해야 함

차세대 안티바이러스 솔루션 EDR은

엔드포인트 단에서 실제 악성행위를 기반으로

스스로 판단하고 차단

06. 요약

항목	EDR	비고
악성코드 식별	행위기반 (동적 분석)	프로세스, 레지스트리, 파일 생성 등 행위 정보 수집
실시간 탐지여부	실시간 탐지	-
변종 식별능력	높음	-
제로데이 대응능력	높음	-
설치 위치	Endpoint	모든 PC에 에이전트 설치
행위 정보 수집 방식	실제 PC의 행위 정보	-

행위기반 악성코드 동적분석과 함께 패턴기반 정적분석이 동시에 진행 되어야 함

엔드포인트에서 동적분석& 정적분석을 동시에 수행할 수 있는 솔루션은

차세대 안티바이러스 EDR 하나 뿐

06. 요약

패턴기반
안티 바이러스 솔루션의
한계 극복

클라우드, 모바일 시대로 전환
경계선 보안(Perimeter)
필요성 약화

파일리스, 랜섬웨어 공격에
가장 효과적인
방어방식 구축

샌드박스 기반
APT 솔루션의
우회탐지 극복

EDR은 차세대 안티바이러스 솔루션 입니다

3. 기능

1. 차별화 기능
2. 기본기능
3. 제품 구성도

01. 차별화 기능 : 요약

01

악성코드 탐지
3대 요소 탑재
TI, AV, EDR, (AI)

패턴 및 행위기반엔진 모두 보유
다층 분석을 통한 정교한 탐지
(차단율 99.5%, 오탐율 0%)

02

악성코드 통제
3대 요소 탑재
프로세스킬, 파일격리, 단말격리

보안담당자 수작업 없이
보안위협 중 90%는
격리/종료를 통해 자동 대응

03

실시간
격리 및 복구
데이터 소실 최소화

이상행위를 빠르게 탐지하여
파일 암호화/위변조 직전
최신 변경점까지 복구

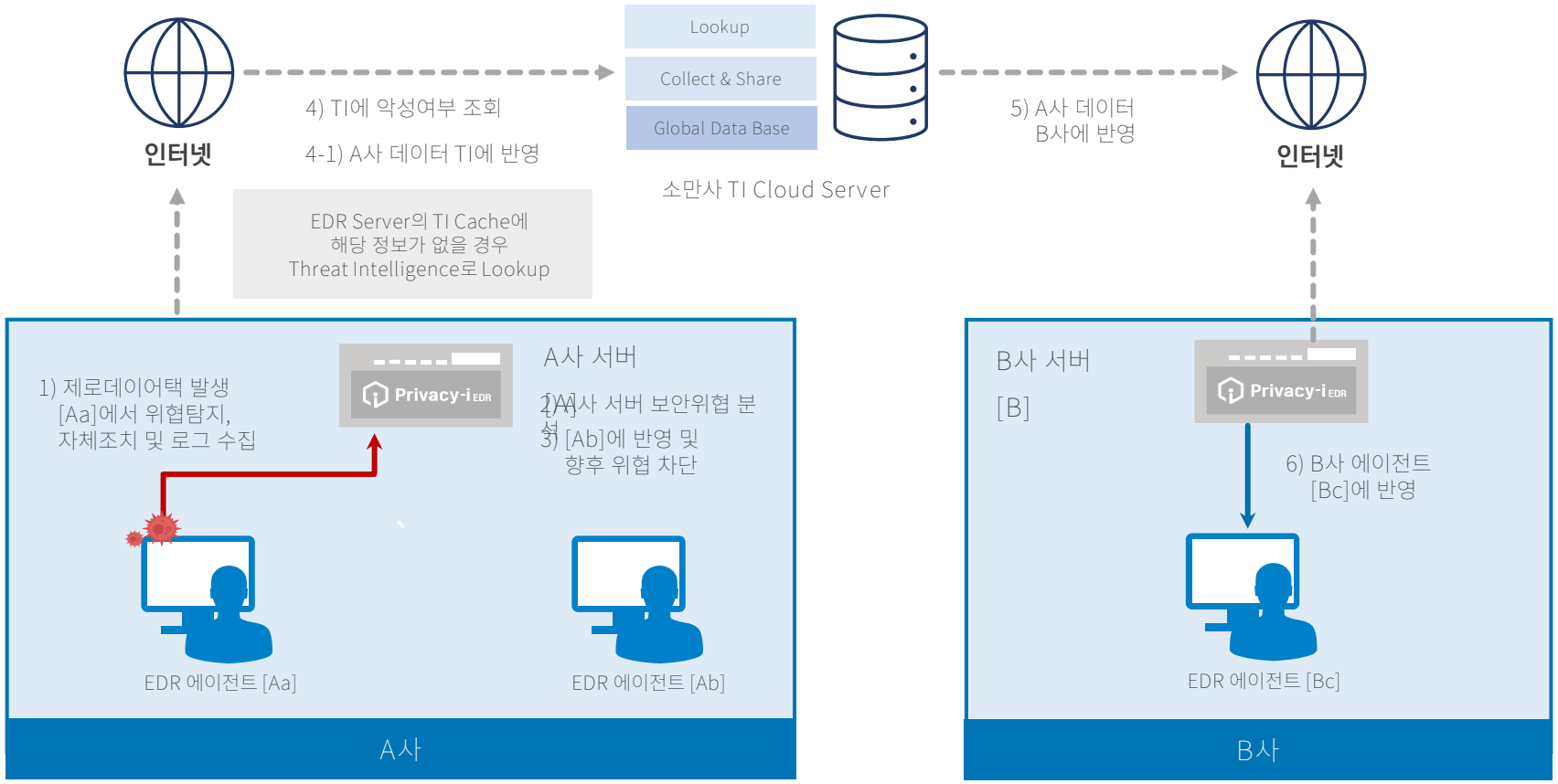
01. 차별화 기능

악성코드 탐지 3대 요소 탑재 : TI, AV, EDR, (AI)

- TI(Threat Intelligence)를 통해
  사내 EDR 서버에 없는 데이터를 주기적 업데이트
- 정적 탐지소스 YARA/IOC 규칙을 통해
  탐지 시간 단축/효율성 강화

01. 차별화 기능

악성코드 탐지 3대 요소 탑재 : TI, AV, EDR, (AI)



01. 차별화 기능

악성코드 탐지 3대 요소 탑재 : TI, AV, EDR, (AI)

항목	악성코드 검출 방식	분석성능	변종/제로데이 악성코드 대응력	비고
TI	해시기반 (Hash)	최상	낮음	단 1 Byte라도 달라질 경우 **검출 불가**
AV	시그니처 기반 (Signature)	높음	중간	변종 대응력 **낮음**
행위기반 엔진	악성코드 행위 기반 (Event)	중간	최상	변종 대응력 **높음**

01. 차별화 기능

악성코드 탐지 3대 요소 탑재 : TI, AV, EDR, (AI)

탐지/포착한 엔진명 | 탐지된 실행파일 | 공신력 있는 정보조회 출처

에이전트 아이피	탐지 종류	탐지 대상	파일 해시	정보 조회	대응 결과
172.16.2.56	위협 인텔리전스	C:\\Users\\hdkim\\Desktop\\Babuk(packed)\\Babuk(packed).exe	296df7094a387d4c9848e02a18bbcf7542e7e725810···		
172.16.2.56	위협 인텔리전스	C:\\Users\\hdkim\\Desktop\\test\\Babuk.exe	296df7094a387d4c9848e02a18bbcf7542e7e725810···		
172.16.2.56	위협 인텔리전스	C:\\Users\\hdkim\\Desktop\\Babuk(packed)\\Babuk(packed).exe	296df7094a387d4c9848e02a18bbcf7542e7e725810···		
172.16.2.56	위협 인텔리전스	C:\Users\2taewon\Desktop\Babuk(packed)\Babuk(packed).exe	296df7094a387d4c9848e02a18bbcf7542e7e725810···		
172.16.2.56	위협 인텔리전스	C:\\Users\\hdkim\\Desktop\\SomansaCrypto(Packed)\\Somans···	57494aec2b31e95e5be475bcb324d7abac732469a1f···		
10.0.2.15	안티 바이러스	C:\Users\somansa\Desktop\samples\medusa.exe	dde3c98b6a370fb8d1785f3134a76cb465cd663db20···		
10.0.2.15	안티 바이러스	C:\Users\somansa\Desktop\samples\medusa.exe	dde3c98b6a37(		
10.0.2.15	안티 바이러스	C:\Users\somansa\Desktop\samples\gandcrab.exe	ce8a3474f1be9		

Virus Total | Hybrid Analysis | Google

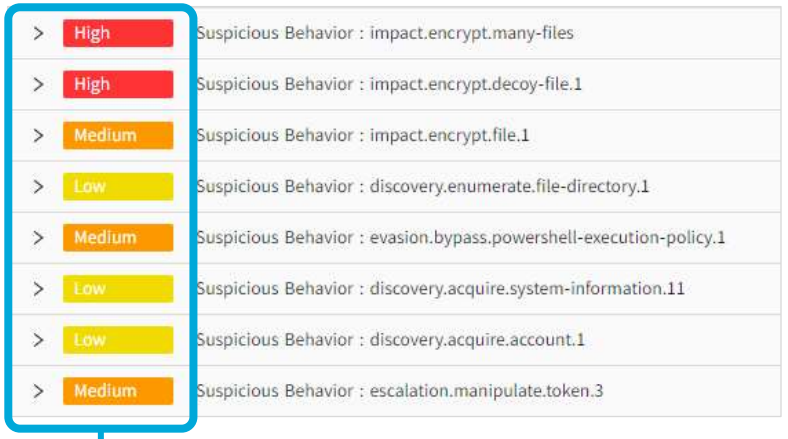
01. 차별화 기능

랜섬웨어 차단

Privacy-i EDR 패턴 & 행위기반 엔진 랜섬웨어 탐지율 테스트

- 테스트 랜섬웨어 100개
- 패턴기반 : 97/100 (97%)
- 행위기반 : 패턴기반이 탐지하지 못한 변종 3건을 모두 탐지

미 콜로니얼 파이프라인 송유관 마비사태 원인 Darkside 랜섬웨어 탐지차단 데이터



01. 차별화 기능

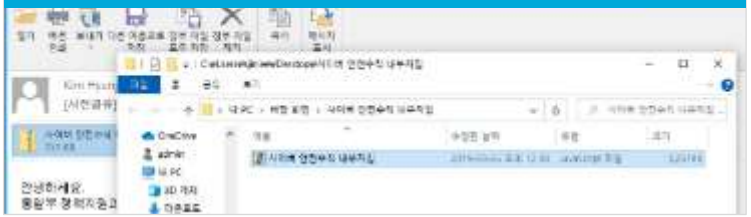
신종/변종 악성코드 차단

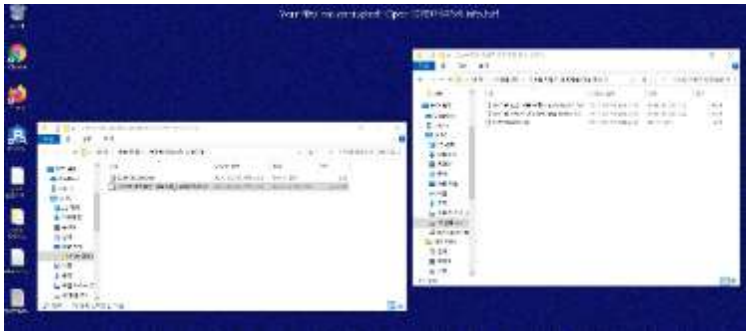
Privacy-i EDR 패턴 & 행위기반 엔진 변종 랜섬웨어 탐지율 테스트

- 변종 변환된 랜섬웨어 82개
- 패턴기반 : 49/82 (59.2%)
- 행위기반 : 80/82 (97.5%)

* 2021.8 소만사 자체 테스트 수행, Themida를 통해 압축 * 변환 후 크래시 발생 또는 미동작

패턴기반 엔진만 활성화 된 상태에서의 랜섬웨어 클릭





행위기반 엔진 활성화 후 랜섬웨어 클릭

랜섬웨어 프로세스 분석/저장

01. 차별화 기능

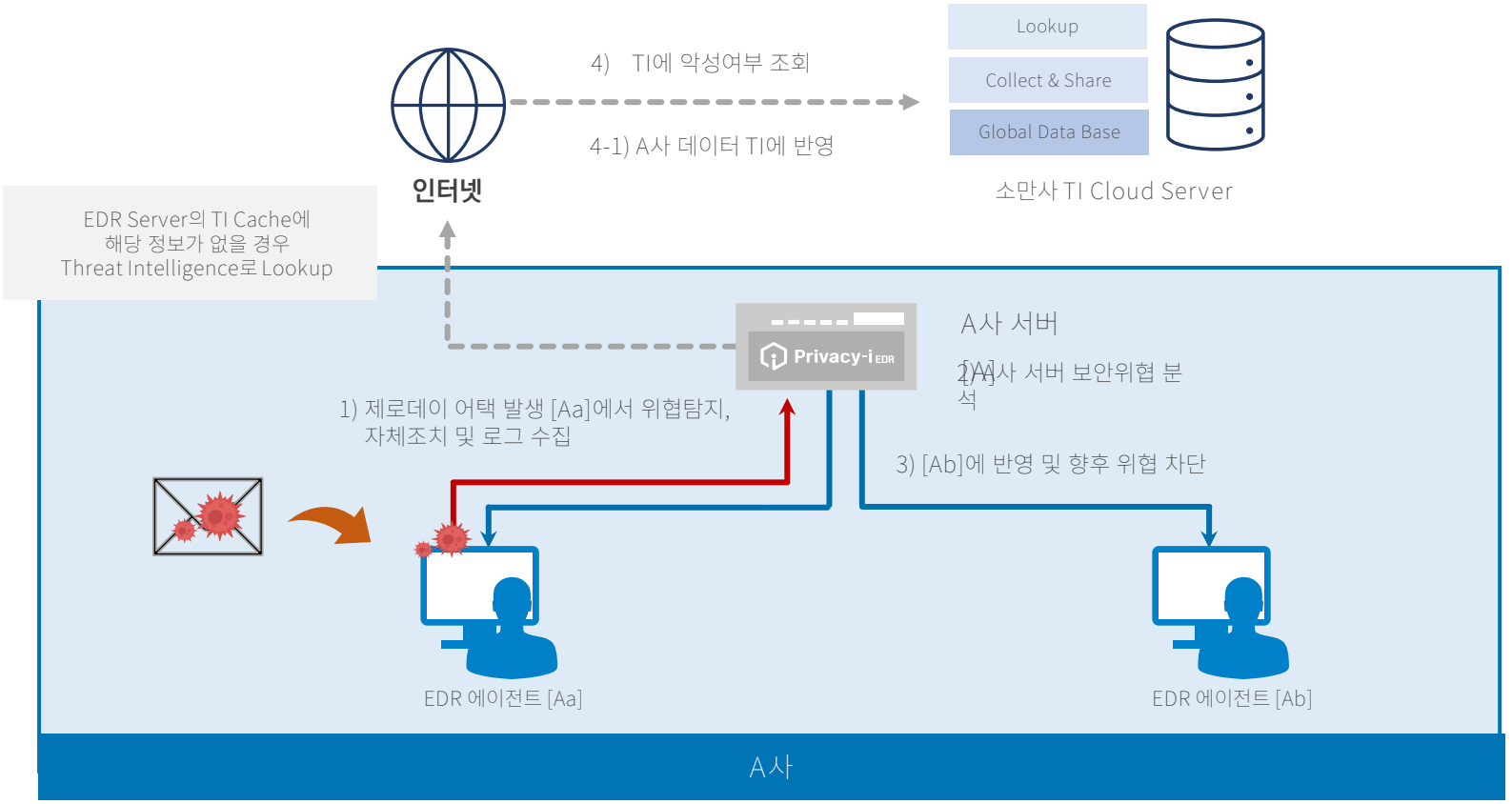
파일리스 공격 차단

악성코드 스크립트가 실행파일을 디스크에 남기지 않고,
신뢰할 수 있는 프로세스에 주입/실행한다면? 패턴기반 엔진은 대응불가

행위기반 엔진으로
행동에 따른 위험도 포착, 대응, 차단

01. 차별화 기능

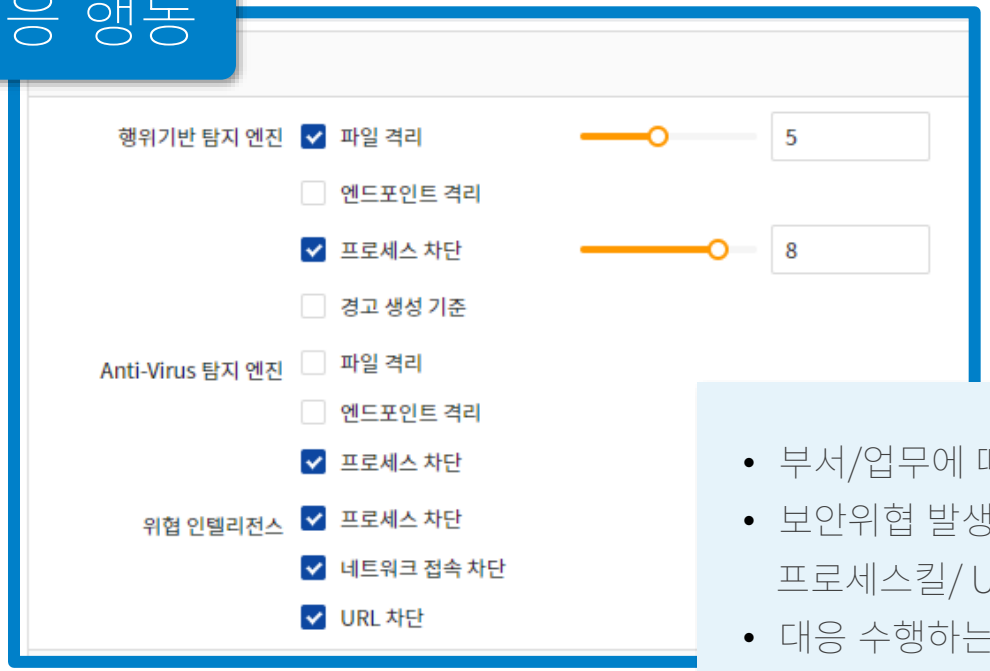
제로데이 공격 대응



01. 차별화 기능

악성코드 통제 3대 요소 탑재 : 프로세스킬, 파일격리, 단말격리

대응 행동



- 부서/업무에 따라 대응행동 세부설정
- 보안위협 발생시 파일격리/엔드포인트격리/ 프로세스킬/ URL 차단 /경고 등 대응행동 설정가능
- 대응 수행하는 악성행위 위험도 조정가능 (1~10 단계, 숫자가 높을 수록 강한 위협)

01. 차별화 기능

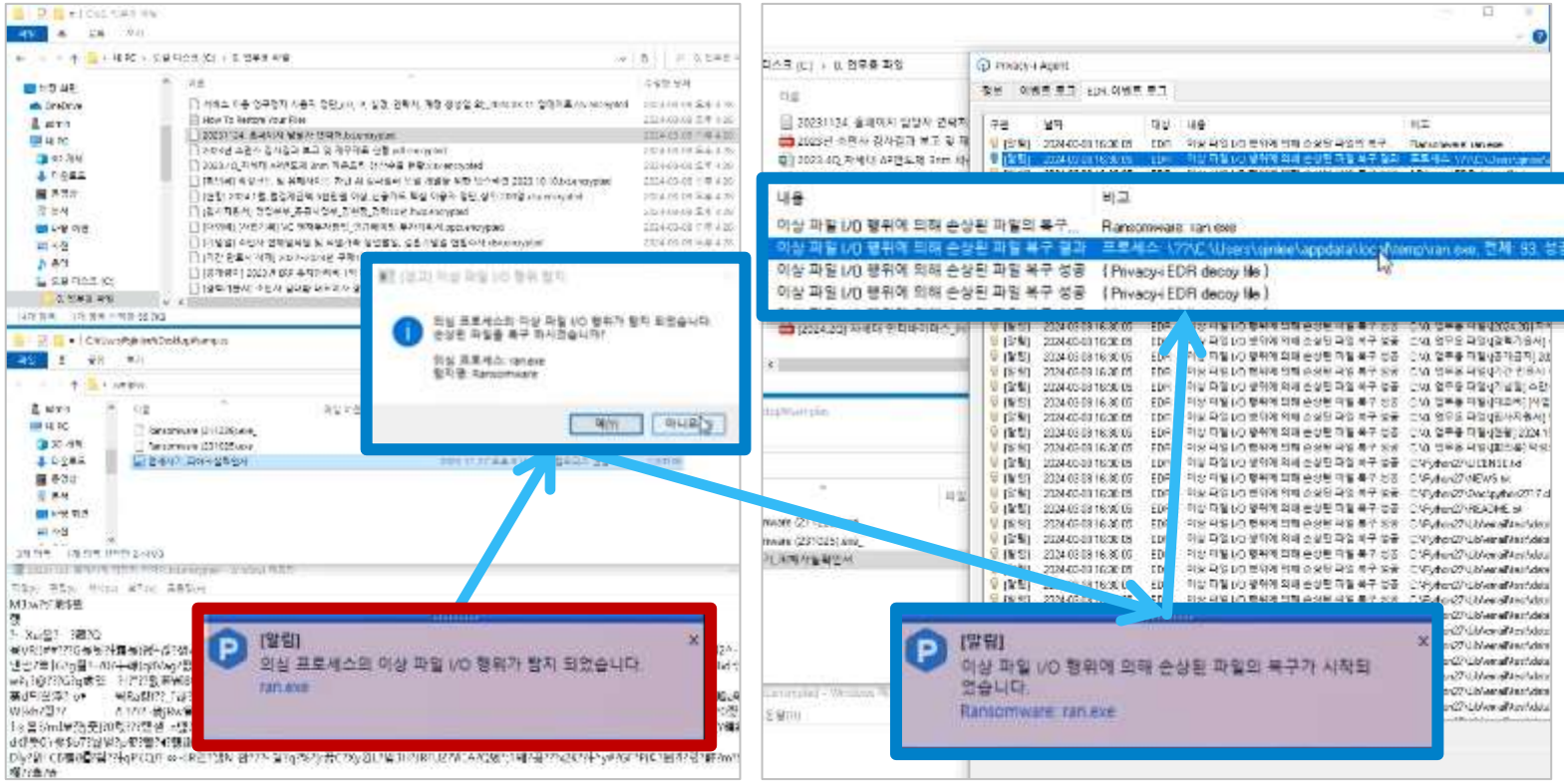
악성코드 통제 3대 요소 탑재 : 프로세스킬, 파일격리, 단말격리

- 보안 위협 중 90%는 자동으로 대응 (격리, 종료)
- 보안담당자의 수작업 없이 선제 대응하여 리소스 절감

01. 차별화 기능

실시간 격리 및 복구 : 데이터 소실 최소화

악성코드/랜섬웨어 위협으로 부터 100% 차단은 불가능
그럼에도 불구하고 감염 또는 데이터 위변조 발생시에는 실시간 파일백업 및 자동복원으로 데이터 복구



01. 차별화 기능

**싱글에이전트: 안티바이러스, EDR,
DLP, 개인정보보호, 내PC지키미 통합**

- 프로젝트 수행기간 절반이상 단축
- 솔루션 신규도입대비 구축비용 절감
- 에이전트 추가설치 불필요

기존 엔드포인트 DLP 솔루션
Privacy-i

PV-i 도입사는 에이전트 업데이트로 (100만여개)
EDR 및 엔드포인트 보안 솔루션 사용가능

- ⊕ DLP
- ⊕ EDR
- ⊕ 안티바이러스
- ⊕ 개인정보 보호
- ⊕ 내PC지키미

02. 기본 기능 : 요약

01

탐지 직후 즉각 대응
확산 차단

6개 대응 방안을 통해
악성행위 감염 및 확산을 차단

02

종합 통계
(위협 조사)

프로세스, 파일, IP, 엔드포인트 기준으로
사내에서 발생한 이벤트 모두 통합 및 통계

03

위젯방식
대시보드

대시보드 위젯 자유 배치, 다양한 위젯 및
레이아웃을 통한 데이터 분석/시각화 지원

04

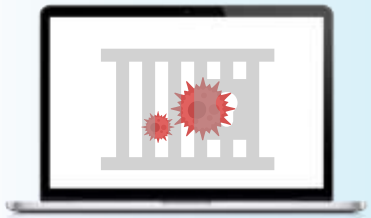
부서/업무 성향에 따른
세분화된 정책설정

취약점 공격방지 정책 제공
취약점 이용 악성코드/랜섬웨어 감염 통제

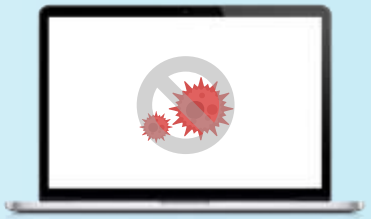
02. 기본 기능

01) 탐지 직후 즉각 대응, 확산 차단

6개 대응 방안을 통해
악성행위 감염 및 확산을 차단



격리 및 삭제
파일격리, 엔드포인트 격리
두 가지 방식 제공

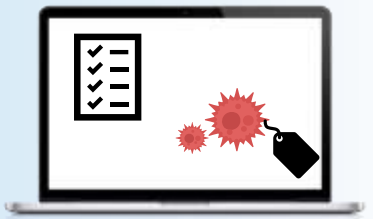


차단
위협발생 IP, C&C서버,
실행파일 등 차단

강제종료
프로세스 종료를 통해
엔드포인트 피해차단

경고 알림
관리자 및 사용자 대상
인적대응 가능하도록 조치

전체스캔
추가 악성행위 탐지를 위해
전사 엔드포인트 스캔



데이터 등록
타 단말 확산방지
동일위협 자동대응

02. 기본 기능

01) 탐지 직후 즉각 대응, 확산 차단

경고: 행위기반으로 탐지된 악성행위 현황조회

- 행위기반 탐지엔진으로 수집된 위협요소들을 발생 엔드포인트PC, 위험도, 분류, 경고이름에 따라 기록/검색
- 보안 위협 중 90%이상은 자동으로 대응(파일격리, 엔드포인트격리, 프로세스 종료)

02. 기본 기능

01) 탐지 직후 즉각 대응, 확산 차단

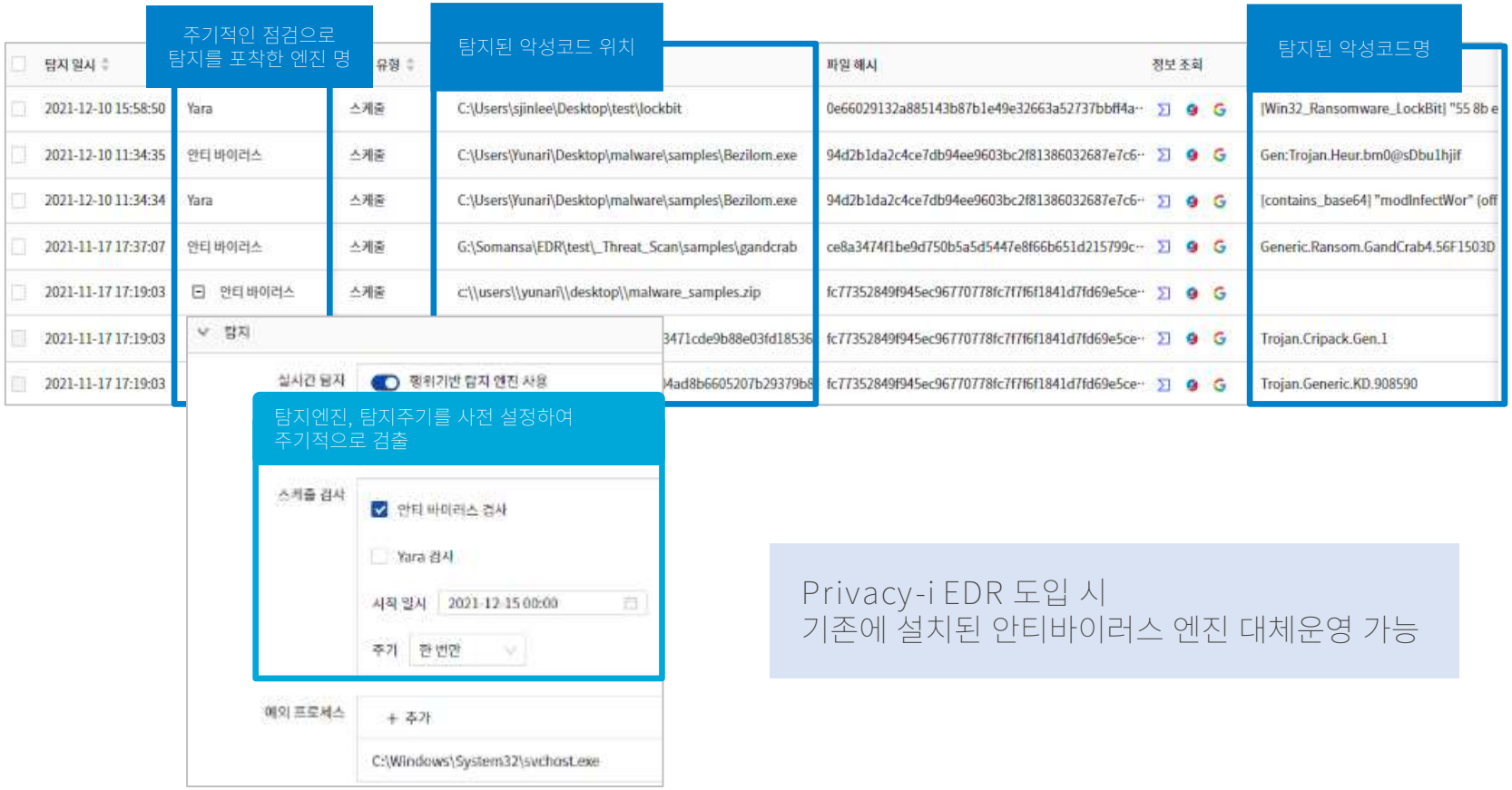
TI: 위협 인텔리전스, 안티바이러스로 실시간 탐지된 악성행위 현황 조회

- 행위기반 탐지엔진으로 수집된 위협요소들을 발생 엔드포인트PC, 위험도, 분류, 경고이름에 따라 기록
- 보안 위협 중 90%이상은 자동으로 대응(파일격리, 엔드포인트격리, 프로세스 종료)

02. 기본 기능

01) 탐지 직후 즉각 대응, 확산 차단

스캔: 패턴기반 엔진이 주기적으로 탐지



Privacy-i EDR 도입 시
기존에 설치된 안티바이러스 엔진 대체운영 가능

02. 기본 기능

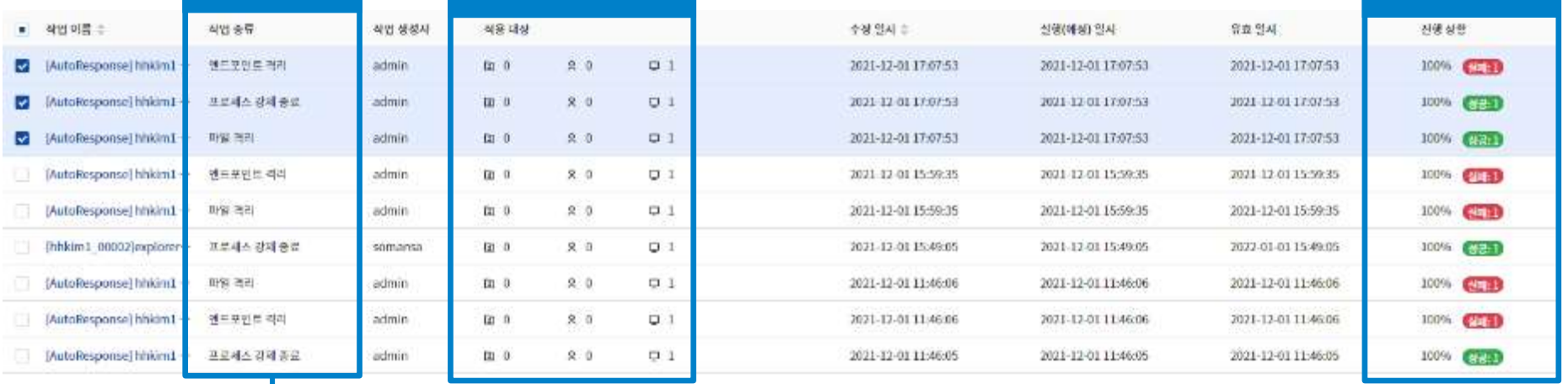
01) 탐지 직후 즉각 대응, 확산 차단

태스크: 발생한 위협과 관련하여
어떤 차단방식을 수행했는지 확인 및 현황조회

EDR이 실제로 대응처리한 방식 안내

탐지 이후 전체 스캔 추가 위협탐지시 동일하게 적용

대응여부 안내: 일부 위협은 관리자가 수동대응



파일 수집	파일 격리	엔드포인트 격리	프로세스 강제종료	위협스캔
엔드포인트 정보수집	파일 격리 해제	엔드포인트 격리해제	프로세스 덤프생성 및 수집	에이전트삭제

02. 기본 기능

01) 탐지 직후 즉각 대응, 확산 차단

격리: 현재 격리된 '파일' 현황 조회

- 부서, 사용자, 파일위치(경로), 파일크기 조회
- 공신력 있는 데이터베이스를 통해 2차 대조하여 격리사유 명확화
- 필요시 파일격리 해제 가능

격리해제 필요시 관리자 권한에 따라 해제가능

탐지된 실행파일 위치(경로)

공신력 있는 정보조회 출처

파일 격리 해제

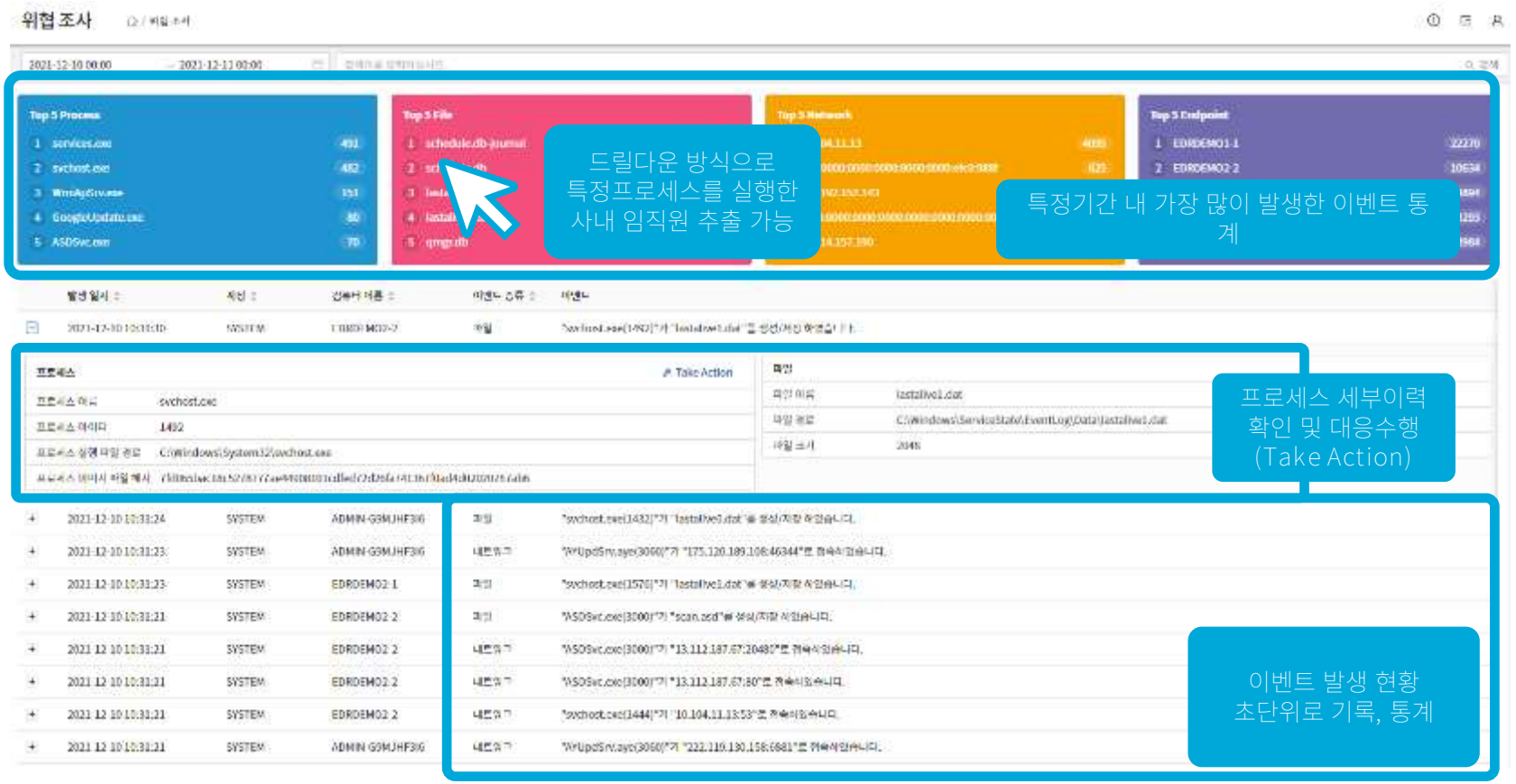
격리 일시	부서 이름	사용자 이름	사용자 아이디	에이전트 아이피	파일 경로	정보 조회	파일 크기(KB)
2021-12-10 10:11:17	영업본부	김현덕	hdkim	172.16.2.56	C:\Users\hdkim\Desktop\Babuk(packed)\Babuk(packed).exe		2620
2021-12-07 20:03:25	영업본부	김현덕	hdkim	172.16.2.56	C:\Users\2taewon\Desktop\test\Babuk.exe		2620
2021-12-06 17:22:15	영업본부	김현덕	hdkim	172.16.2.56	C:\Users\2taewon\Downloads\Babuk(packed)\Babuk(packed).exe		2620
2021-12-01 17:08:04	소만사	김현호	hhkim1	10.0.2.15	C:\Users\somansa\Desktop\samples\babuk.exe		30.5

Virus Total　Hybrid Analysis　Google

02. 기본 기능

02) 종합 통계 (위협조사)

프로세스, 파일, IP, 엔드포인트 기준으로
사내에서 발생한 이벤트 모두 통합 및 통계

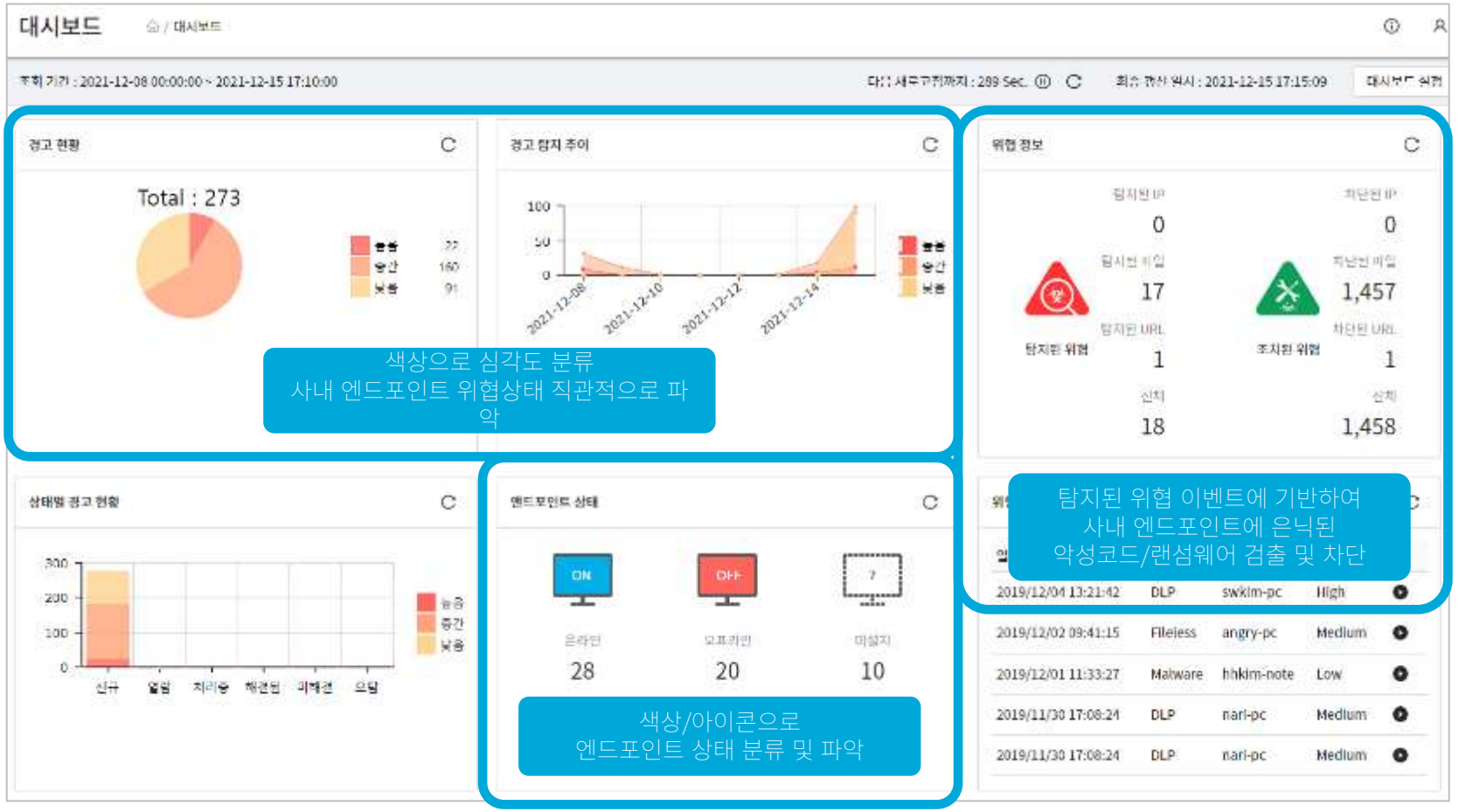


SOMANSA

02. 기본 기능

03) 위젯방식 대시보드

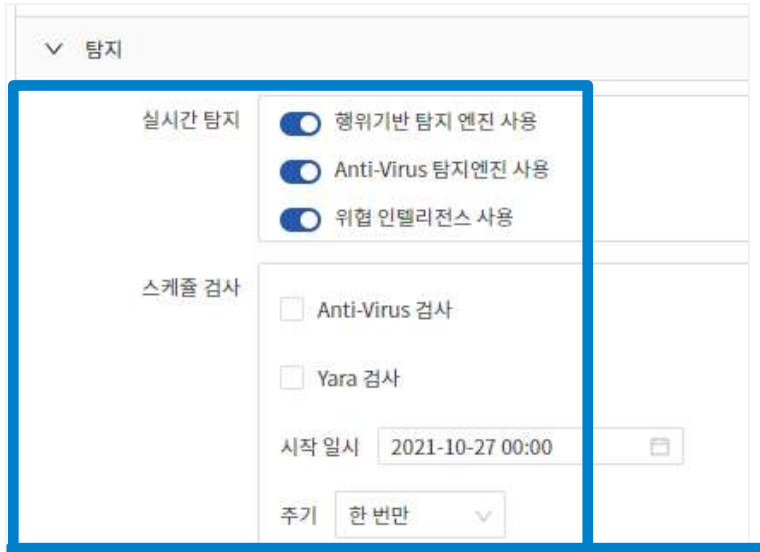
대시보드 위젯 자유 배치, 다양한 위젯 및 레이아웃을 통한 데이터 분석/시각화 지원, 다중 탭 지원



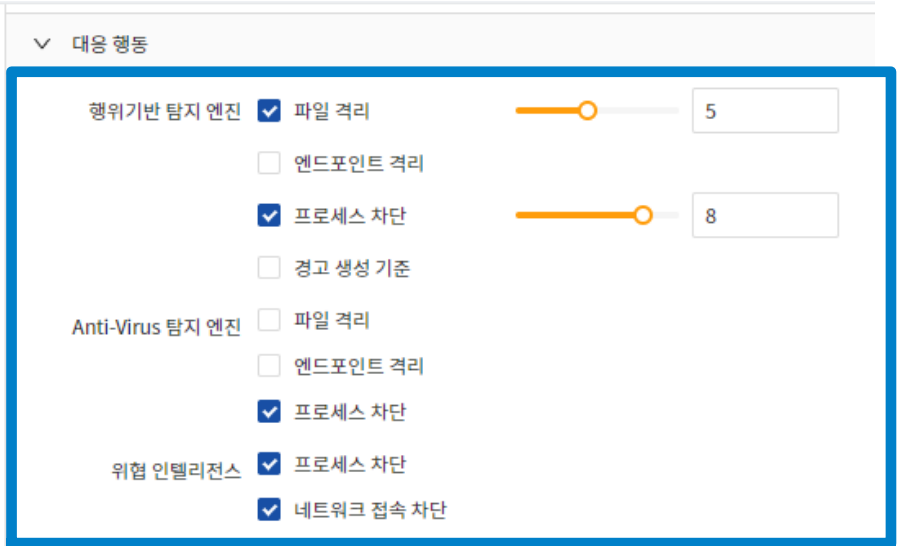
02. 기본 기능

04) 부서/업무 성향에 따른 세분화된 정책설정

성능부하 방지를 위해 행위기반, 안티바이러스, TI엔진 세부 설정
부서 업무 및 성향에 따라 대응강도 조정



· 소만사 자체 패턴기반 엔진 탐지
TI를 통해 사내 EDR 서버에 없는 데이터 주기적 업데이트
· 정적 탐지소스 YARA/IOC 규칙을 통해
탐지 시간 단축/효율성 강화

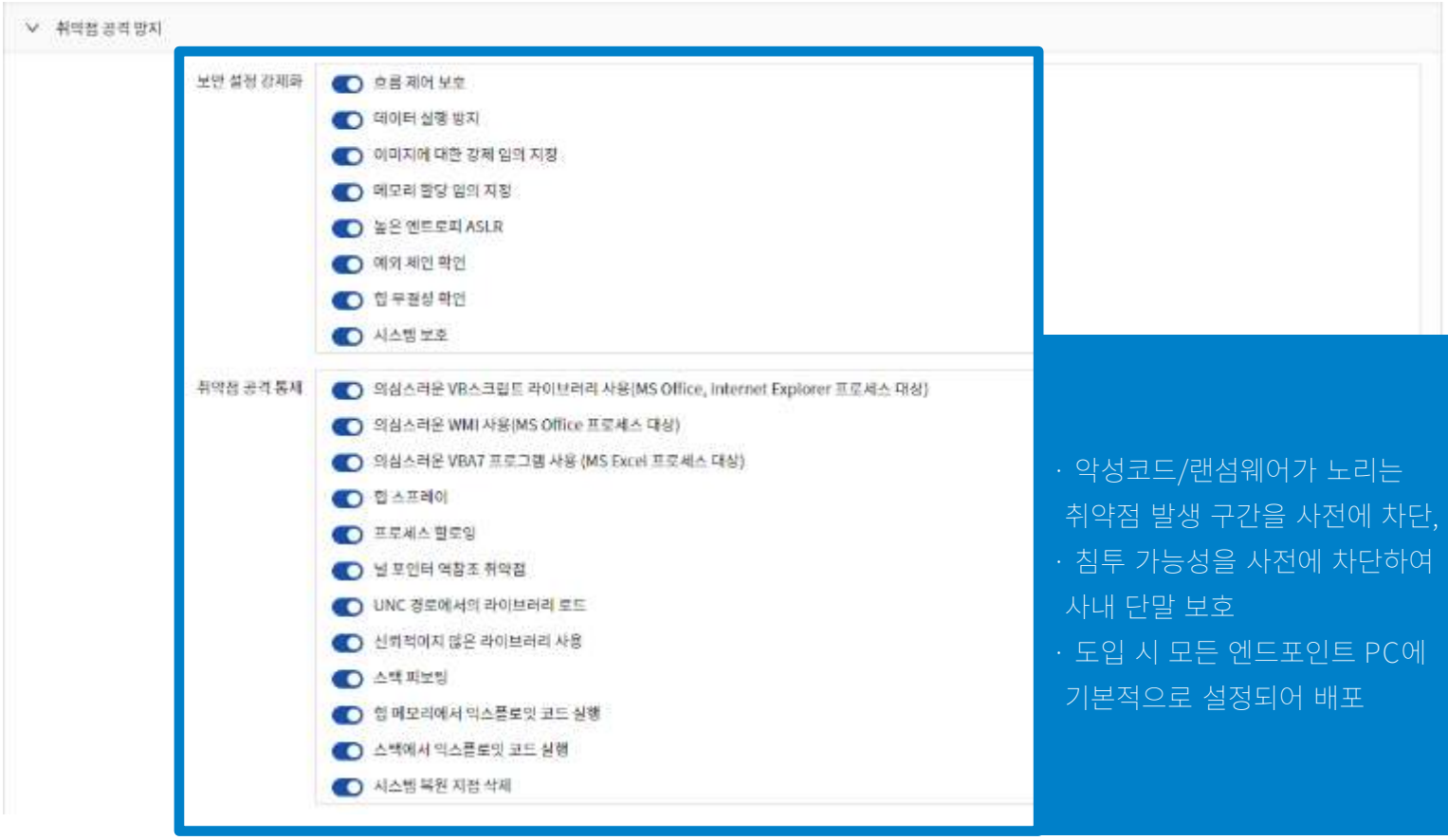


· 부서/업무에 따라 대응행동 세부설정 가능
· 보안위협 발생시 파일격리/엔드포인트격리/
프로세스 차단/ URL 차단 /경고 등 대응행동 설정가능
· 대응을 수행하는 악성행위 위험도 조정가능
(1~10 단계, 숫자가 높을 수록 강한 위협)

02. 기본 기능

04) 부서/업무 성향에 따른 세분화된 정책설정

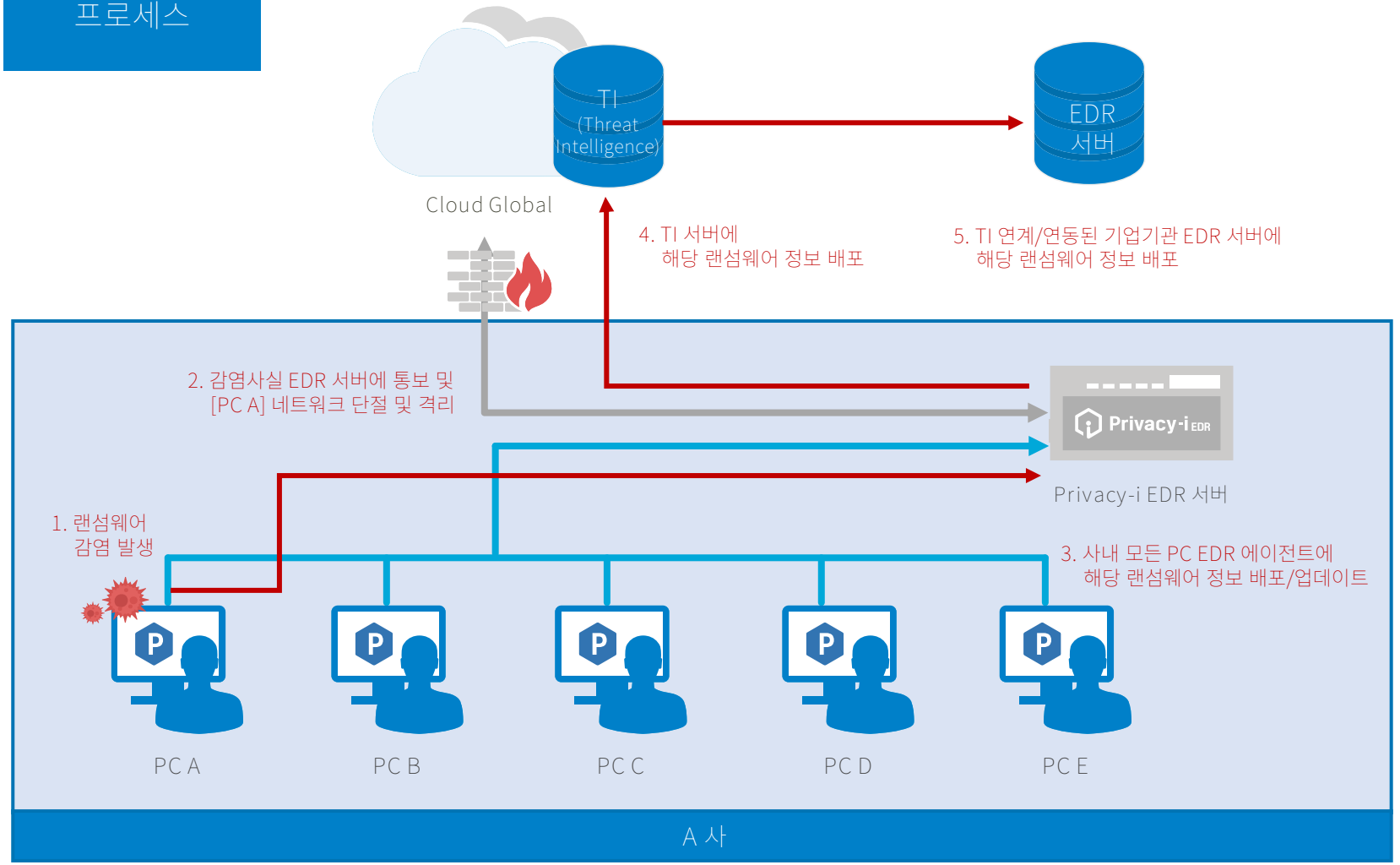
취약점 공격방지 정책 제공
취약점을 이용한 악성코드/랜섬웨어 감염 통제



- 악성코드/랜섬웨어가 노리는 취약점 발생 구간을 사전에 차단, 봉쇄
- 침투 가능성을 사전에 차단하여 사내 단말 보호
- 도입 시 모든 엔드포인트 PC에 기본적으로 설정되어 배포

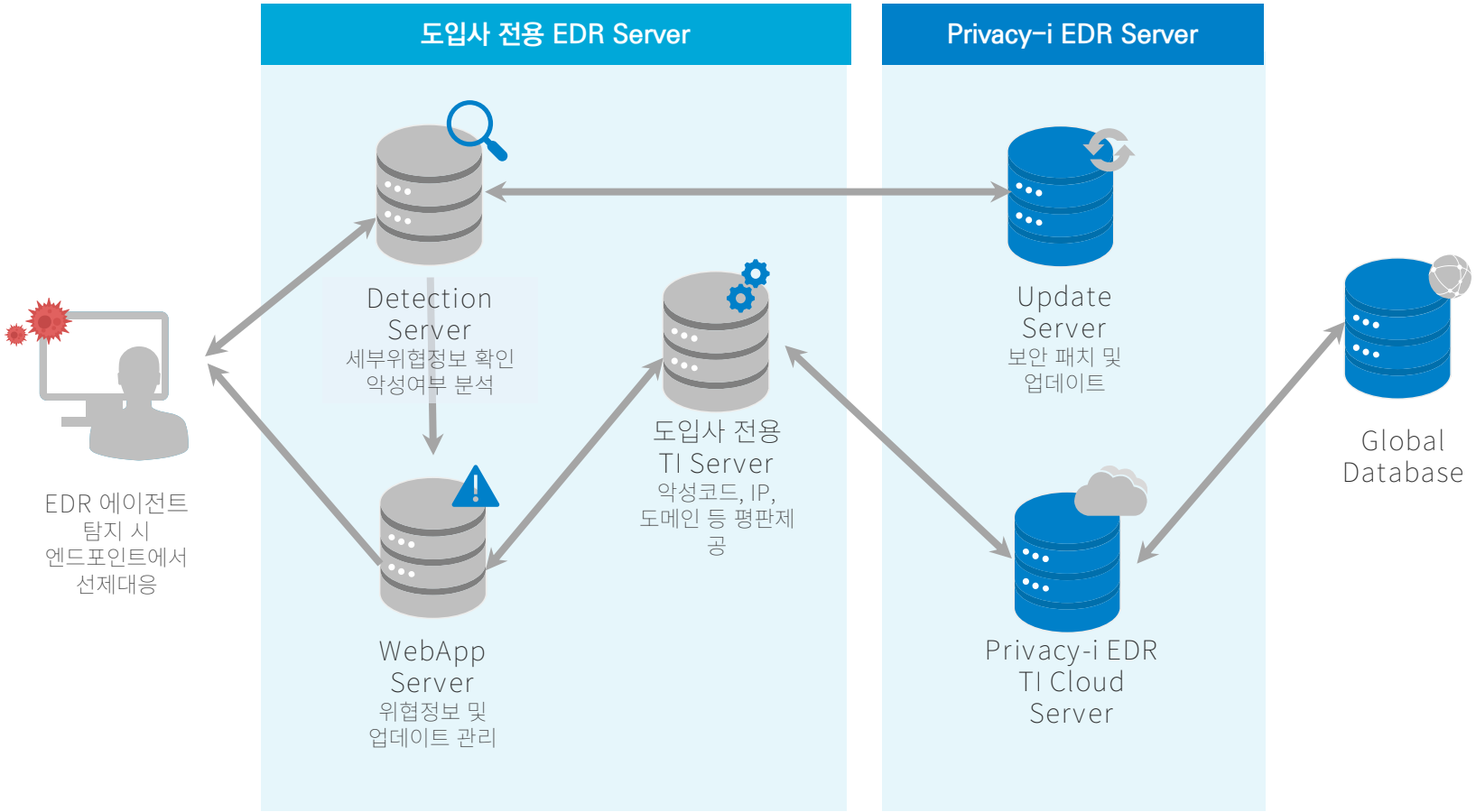
03. 제품 구성도

프로세스



03. 제품 구성도

플랫폼 아키텍쳐



4. 비교표 & 로드맵

01. 비교표

02. 로드맵

01. 비교표

구분	소만사 Privacy-i EDR	외산 C사 EDR 솔루션
에이전트 개수	싱글에이전트	EDR 이외 PC 에이전트 추가 설치
네트워크 차단과 연계 (XDR)	SWG 차단 연계	제한적
TI (Threat Intelligence: 위협 인텔리전스) 연계 차단	O	O
변종 악성코드 차단	O	O
제로데이 악성코드 차단	O	O
MITRE ATT&ACK 대응	O	O
실시간 데이터 복구	O	제한적
AV와 행위 엔진 동시 활용	O	제한적
악성코드 차단율	99%	94%

01. 비교표 : 악성코드 탐지성능

자체 탐지성능 테스트 수행
랜섬웨어 및 악성코드 샘플 1만개 차단 (자사에서 자체수집)

구분	소만사	국외 C사
EDR 탑재 패턴기반 탐지엔진	94.3%	90.3%
EDR 탑재 행위기반 탐지엔진	5.3%	3.7%
총 차단율	99.6%	94.0%

✓ 국산 EDR솔루션의 악성코드 탐지율은 글로벌 제품대비 떨어지지 않음

✓ 실시간 대응역량을 제외하면 글로벌 수준과 대등

02. 로드맵

싱글 에이전트

악성코드와 (EDR)와
정보유출차단(DLP)
통합 싱글 에이전트

XDR

EDR과
네트워크 보안장비와
연동 (SWG)

플랫폼 확장

OS를 windows 외
Mac, Linux
플랫폼으로 확장

딥러닝

인공지능
딥러닝 기법을 활용하여
악성코드 분석 역량강화

5. 프로젝트 관리 및 교육

01. 기술평가등급 T2

02. 프로젝트 수행

03. 기술지원 및 정기적 서비스

01. 기술평가등급 T2

- 기술평가등급 T2 → 기술력 상위 1% 이내
- 200여명 기술인력 보유
- 인프라 구축부터 유지관리까지 단일 벤더에서 일괄지원대응

기업체명	(주)소만사
대표자명	김대환
사업자등록번호	214-86-14882
법인등록번호	110111-1394115
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
산업분류	[J58222] 응용 소프트웨어 개발 및 공급업
유효기한	2024년 08월 08일
제출처 및 용도	적격심사 및 공공기관 제출용

기술평가등급

T2

평 가 일	2023년 08월 09일

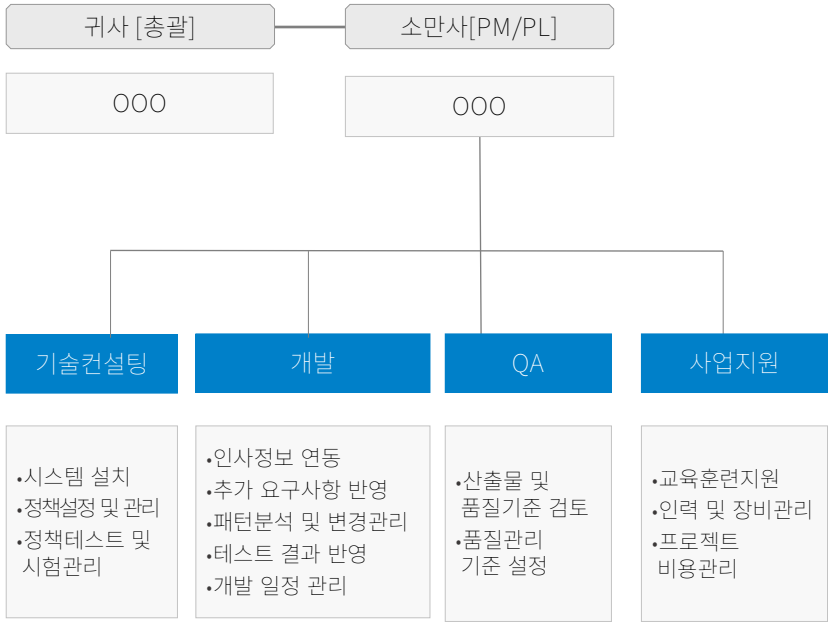
기술평가등급	매우취약	취약	미흡	보통이하	보통			보통이상			양호			우수			매우우수	최우수
	T10	T9	T8	T7	T6-	T6	T6+	T5-	T5	T5+	T4-	T4	T4+	T3-	T3	T3+	T2	T1
	기술력이 매우 우수한 수준으로 산업 및 시장환경의 급격한 변화에도 어느 정도 대응능력을 갖추고 있어 안정적임																	

02. 프로젝트 수행

㈜ 소만사는 Privacy-i EDR 구축사업의 성공적 수행을 위해 계약부터 완료까지 귀사와의 유기적 관계를 유지할 수 있는 조직을 구성합니다. 또한 완벽한 품질의 산출물이 생성되도록 독립적인 품질보증 팀의 지원을 받아 원활하고 효율적인 프로젝트 수행이 가능하도록 하며, 프로젝트 관리자가 전체 프로젝트 팀을 효율적으로 관리할 수 있도록 조직을 구성합니다.

인력확보 방안 및 인적 구성의 적정성

< 수행 조직 >



< 업무분장 >

조직	역할
귀사	▪ 계약체결, 사업관리 및 사업비 신청내역 확인 ▪ 검사 및 인수, 사후관리 ▪ OOO에서 담당할 필요가 있는 세부적인 업무
소만사 (PM)	▪ 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 품질보증, 투입인력, 자원 및 예산 관리 ▪ 주요 이해당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
소만사(PL)	▪ 기술적인 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 기술적인 품질보증, 투입인력, 자원 및 예산 관리 ▪ 기술 당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
기술컨설팅	▪ 시스템 설치 및 구축(하드웨어, 소프트웨어 – 운영체제, 로그서버 등) ▪ 정책설정, 관리 및 운영 지원 / 주요 산출물 작성
개발	▪ 추가요구사항 반영/ 패턴분석 및 변경관리/ 테스트 결과반영/ 개발일정관리
QA	▪ 산출물과 품질기준 검토 및 품질관리 기준 설정 ▪ 표준화가 필요한 업무에 대하여 프로세스 및 정보항목 도출 ▪ 표준화 추진방안 제시

03. 기술지원 및 정기적 서비스

교육지원 담당자의 책임아래 교육훈련을 진행합니다.

교육준비, 교육실시, 평가 및 분석 3단계로 나누어 시행하여 훈련효과를 극대화 합니다.

훈련 실시 후 교육내용 활용도를 조사, 부족한 부분을 추가 교육하여 대상 그룹의 시스템 적응력과 운용능력을 극대화 합니다.

교육훈련 일정

교육과정	주요내용	교육일정	교육대상	관련자료/장소
기초교육	▪ 솔루션사용법 - 사용자 환경설정 및 접속방법 - 로그조회 등 감사활동 방법 ▪ 솔루션 개념 및 구축 기법 ▪ 솔루션 시스템 운영 및 활용 방안 ▪ 집합교육	▪ 1일(2시간소요) (프로젝트 초기: M) - 계약 후 4개월이내	▪ 총괄 담당 직원	▪ 운영 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 기본 교육	▪ 솔루션의 운영관리 - 시스템 운영환경(H/W및 S/W)에 대한 이해 - 솔루션 운영교육 - 보안규칙 적용방법 - 모니터링 및 감사활동 방법 ▪ 운영 지침 ▪ 시스템 전반적인 이해 ▪ 각 모듈 별 요소 기술 ▪ 보안관리자 ▪ 매뉴얼 사용 방법 ▪ 집합교육 또는 쿠폰	▪ 1주일(일1시간) (솔루션 설치 완료시: M+1) - 계약 후 5개월이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 심화 교육	▪ 운영단계에서 실제 운영 시 상세 제품교육 ▪ 보고서 활용 관련 리포트 활용법 ▪ 집합교육 또는 쿠폰	▪ 1일(3시간) (시스템 안정화 단계 시: M+2) - 계약 후 6개월 이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정장소

03. 기술지원 및 정기적 서비스

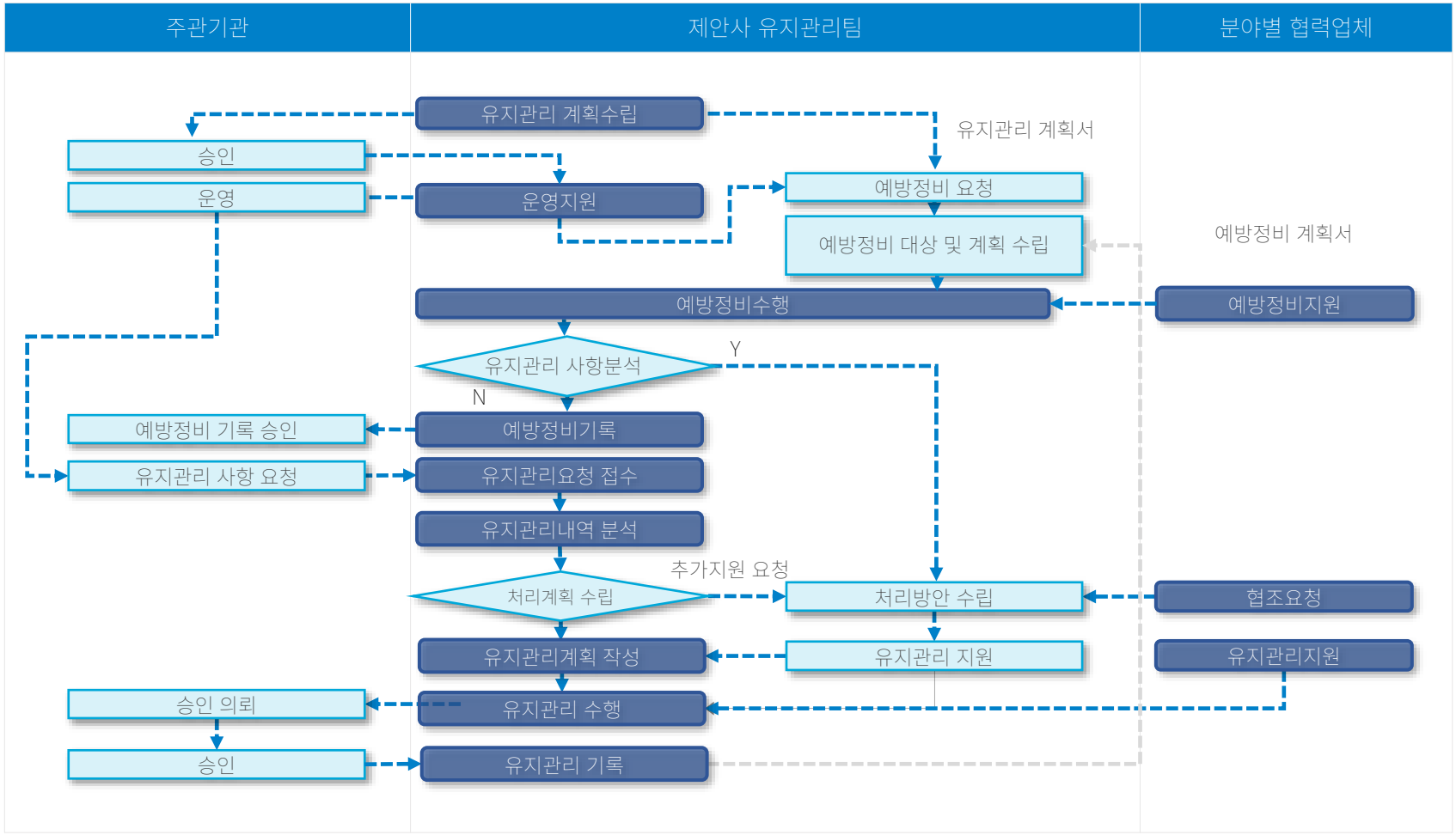
제안사의 운영기술 지원 서비스는 다음과 같이 5가지 영역으로 나뉘어 제공됩니다.
유지관리 정책은 검수 후 1년간 무상 지원되며, 이후 별도의 유지관리 계약을 통해서 지속적인 서비스를 제공합니다.

운영기술 지원 서비스

구 분	지원 방안	비고
예방정비 (PM)	• 전담 A/S 요원 정기점검 및 요청 시 방문 • 모듈 및 시스템 성능 검사 및 종합 테스트 • 정기적인 이론 실습 교육 • 전산 마인드 교육 • 업무시스템의 효율적인 사용을 위한 교육	• 전담 요원 확보 • 충분한 예비 시스템 확보
긴급정비 (EM)	• 유지관리를 위한 전담 엔지니어 확보 • Help Desk 운영을 통한 신속 정확한 장애 조치 • Diagnostic Program을 통한 정확한 고장부위 파악 및 조치	• 4시간 이내 착수하여 조치 이행함
서비스망 접수처리	• Help Desk를 구축 신속한 장애 접수 처리	• 상시 지원 체제 구축
기술지원	• Version Upgrade 관련 최신 기술정보 제공 • 대상 업무 검토 및 협의 • 시스템 성능향상을 위한 기술자문 및 신기술 세미나	• 유지관리 전담팀 활용
무상유지관리 기간	• 시스템 구축 후 1년	

03. 기술지원 및 정기적 서비스

1,000여개 유지관리 사이트 지원경험과 200여명의 전문가를 통한 대응체계를 고객에게 제공합니다

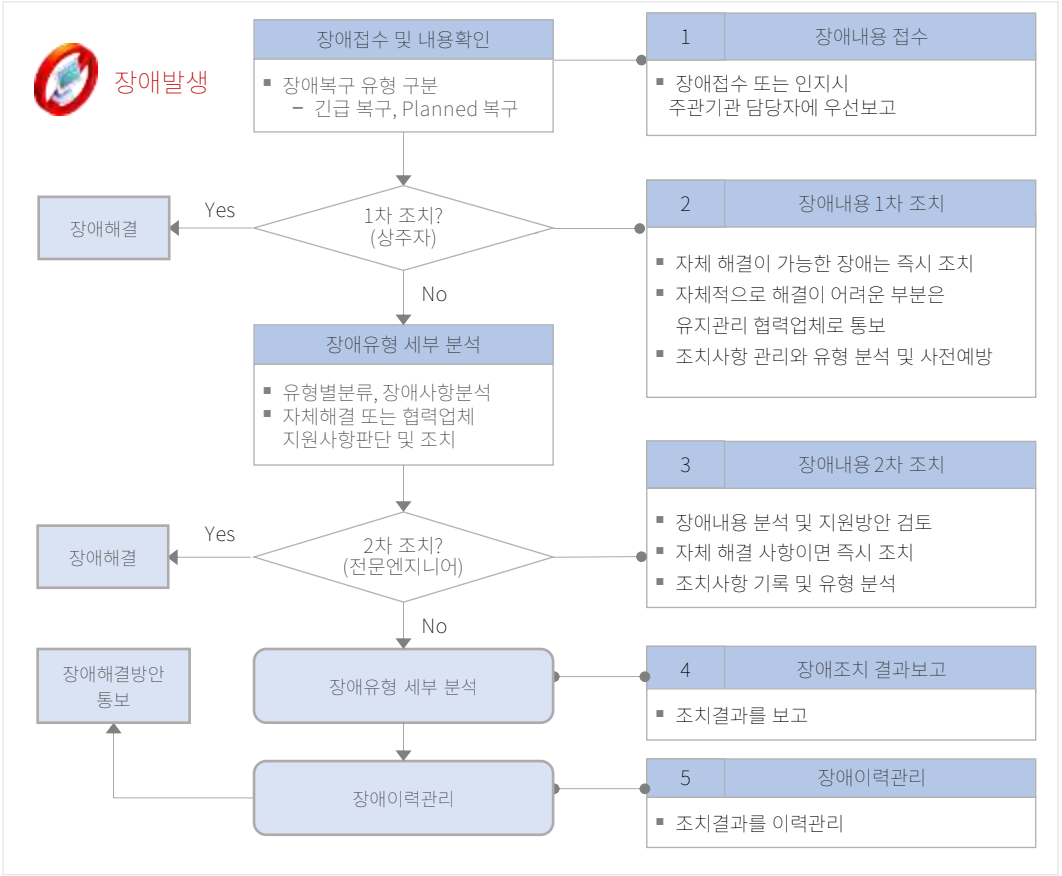


03. 기술지원 및 정기적 서비스

제안사 기술컨설팅 단일창구를 통해 장애접수 후

유지관리팀 및 주관기관 내 자체 운영조직에 의한 해결 또는 협력업체 현장방문으로 신속히 장애문제를 조치합니다

절차에 의한 체계적이고 신속한 장애처리



장애복구 유형별 조치방안

구분	내용	조치 담당자	비고
긴급 복구	장애요소제거 및 교체	유지관리 담당자	유지관리 수행팀은 전단계에 걸쳐 지속적인 지원
	시스템 (HW 및 SW) 가동	시스템 및 SW 운영자	
	서비스 가동 및 확인	업무담당자	
Planned 복구	복구작업 계획수립	관련자 전체	
	서비스 및 시스템 중지	업무담당자, 시스템 및 SW 운영자	
	장애요소 제거 및 교체	유지관리 담당자	
	시스템 및 서비스 가동, 확인	시스템 및 SW 운영자, 업무담당자	

차세대 안티바이러스 솔루션

Privacy-i EDR

성공적인 프로젝트로 보답하겠습니다

감사합니다

SOMANSA

서울특별시 영등포구 영신로220 KnK디지털타워 9층 소만사
대표번호 : 02-2636-8300 | 기술문의 : tech@somansa.com
제품구매 : 02-2655-4040 / sales@somansa.com

별첨: 소만사 악성코드차단통제 프레임워크

소만사는 데이터 보호 관점에 기반하여 내부자/해커 탈취에 의한 데이터유출 통제와 함께
악성코드, 랜섬웨어를 통한 데이터 파괴/변조행위를 차단하는 토탈 솔루션을 귀사에 제공합니다

별첨.

PC에 10여 개의 보안 에이전트가 설치되었을 때 문제점

항목	보안 Agents (개인정보보호, DLP, DRM, EDR, 안티바이러스, 내PC지키미, 매체제어, 출력물 통제 등)
부팅시간	지연
PC 성능	프로세스, MEM, CPU 점유
후킹장애 블루스크린	DLP, 안티바이러스, EDR, DRM, 매체제어, 출력물 통제 에이전트가 독립적으로 실행되므로 후킹 시 충돌가능성 높음
동일파일 다중스캔 부하	바이러스 악성코드 파일 스캔 / 개인정보 파일 스캔 / DRM 암호화 대상 파일 스캔
충돌회피	보안 에이전트간 충돌회피로 인한 보안 허점 발생
개인정보 패턴 일관성	동일파일에 대해서 매체제어, 출력물보안, PC개인정보보호, DLP 에이전트가 카운트한 개인정보 검출 횟수가 다름 USB 파일 복사 주민번호 150개 / 출력 주민번호 145개 / 웹메일 전송 주민번호 152개 / 개인정보 파일 검출 주민번호 151개
OS업그레이드시	OS 업그레이드시 모든 에이전트 업그레이드 프로젝트 수행

별첨.

Single Agent VS 10개 보안 에이전트

항목	Single	기존 보안 Agents
부팅시간	로딩타임 ½	지연
PC 성능	PC리소스 30%이상 절감	프로세스, MEM, CPU 점유
후킹장애	후킹 0%	DLP, 안티 바이러스, EDR, DRM, 매체제어, 출력물 솔루션이 동시 후킹
파일 스캔	단한 번의 파일스캔 1회	바이러스 악성코드 파일 스캔 / 개인정보 파일 스캔 / DRM 암호화 대상 파일 스캔
충돌회피	에이전트 간 충돌 0%	보안에이전트간 충돌회피 작업
개인정보 패턴 일관성	유지	동일 파일 USB 파일 복사 주민번호 150개 / 출력 주민번호 145개 / 웹메일 전송 주민번호 152개
OS업그레이드시	업그레이드 프로젝트 한번	OS 업그레이드시 모든 에이전트 업그레이드 프로젝트 동시 수행

SOMANSA

시장 1위
엔드포인트 내부정보유출방지(DLP) 솔루션

목차

1. 회사소개

01. 시장 1위 내부정보유출방지(DLP) 전문기업 소만사

02. 재무 안정성 상위 1%

03. 조직 및 기술력

04. 인증 및 지적 재산권

05. Privacy-i 레퍼런스

06. Best Practice

01. 시장 1위 내부정보유출방지(DLP) 전문기업 소만사

- 국내외 1,000여곳에서 28년 동안 축적 및 개발한 엔드포인트 보안 기술력을 보유하고 있습니다.
- 아시아 유일, '가트너 매직 쿼드런트' 엔터프라이즈 DLP분야 2년 연속 등재되었습니다 .

2024

하나은행 15,000명 규모 싱글 에이전트 구축

신한은행 10,000명 규모 싱글 에이전트 구축

2022

PC 취약점 점검 Privacy-i 지키미 출시

차세대 안티바이러스 Privacy-i EDR 출시

2021

Gartner Magic Quadrant 'Enterprise DLP' 보고서 2년 연속 등재

2020

가트너 Enterprise DLP분야 글로벌 Top10 아시아 기업 최초로 등재

Forrester Research 'Vender Landscape' 선정

2015

Privacy-i macOS 에이전트 출시

서버 DLP 솔루션 Server-i 출시

DB방식 대비 100배 빠른 초고속 로그 검색엔진 탑재

개인정보 유출방지 Privacy-i DLP(복사, 출력, 인터넷 업로드 통제) 출시

2007

국내최초 개인정보 검출·보호 솔루션 Privacy-i Discover 출시

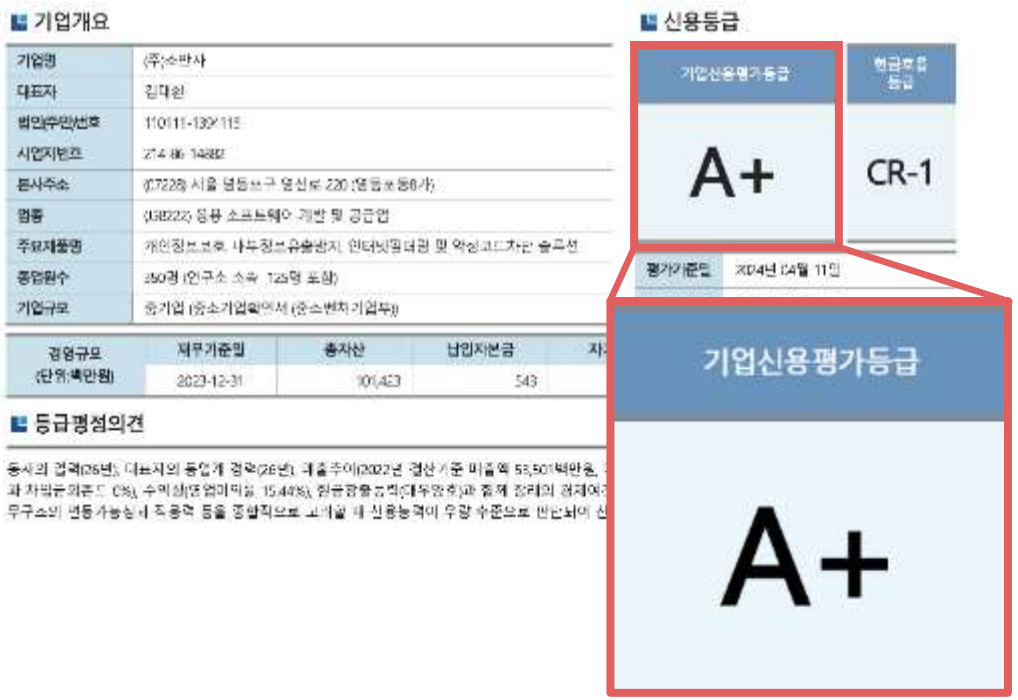
네트워크를 통한 내부정보 유출차단 DLP 솔루션 Mail-i 출시

1997

㈜소프트웨어를 만드는 사람들 설립

02. 재무안정성 상위 1%

- 중소기업 **재무안정성 상위 1%(A+), 유일한 무차입 기업**입니다.
- **신용평가 A+, 현금흐름등급 CR-1로 중소기업 상위 1%의 재무적 안정성**을 바탕으로
  소만사는 중장기 R&D 및 기술지원에 투자하고 있습니다.

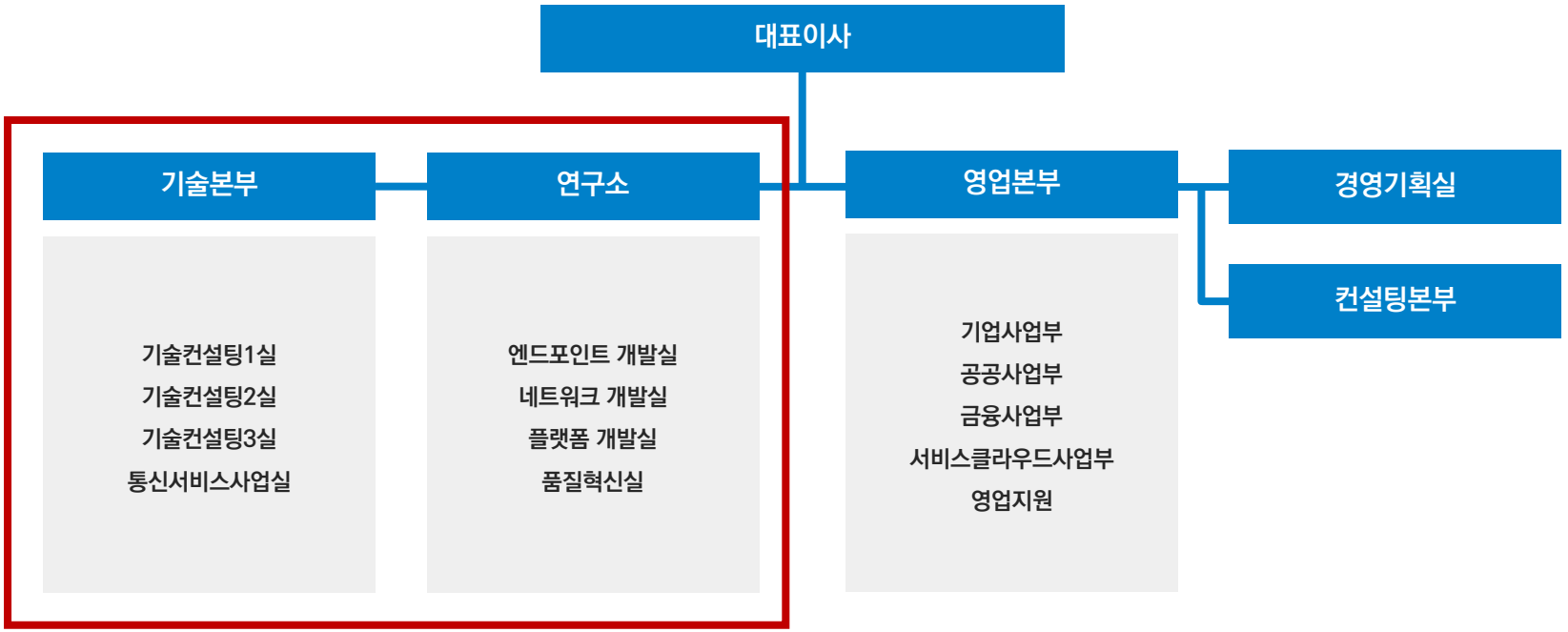


(단위: 억원)

구 분	2022년	2023년	2024년
매출액	535	577	653
영업이익	83	124	145
당기 순이익	88	140	161
차입금	0	0	0
총자산	847	1,014	1,221

03. 조직 및 기술지원능력

- 소만사 임직원 350명 중 240여명이 기술인력(약 70%)으로 재직 중입니다. (연구개발자 120여명, 기술엔지니어 120여명)
- 자사 연구소 내 엔드포인트 개발실(PC/서버 엔드포인트 보안)을 통한 엔드포인트 보안분야 핵심 원천 기술을 보유하고 있습니다.
- 경쟁사 대비 최소 3배 이상 기술지원 인력을 통한 국내 최고지원이 가능합니다.



04. 인증 및 지적재산권

- 자사 연구소 내 연구개발자를 통하여 지속적으로 핵심 원천기술 개발역량을 고도화 하였습니다.
- 이를 기반으로 CC인증, GS인증을 획득하였습니다 .
- 데이터유출방지, 개인정보 검출, 악성코드 차단 등 데이터 보호 분야에서 50건 이상 등록출원 하였습니다.

인증 수상

CC 인증

GS 인증

보안기능확인서

특허

- 엔드포인트의 트래픽에 대한 포워딩 시스템 및 방법
- 엔드포인트 정보유출방지 탐지 및 대응 기능 테스트 자동화 시스템 및 방법
- 디코이 개인정보 데이터를 이용한 정보유출방지 시스템 및 방법
- 엔드포인트 DLP를 위한 2계층 기반의 기밀 정보 검출 시스템 및 방법
- DLP(Data Loss Prevention) 시스템에서의 보다 정밀한 유출 탐지를 위한 다중 컬럼 키워드 패턴 매칭 장치 및 방법
- DLP시스템의 빅데이터 처리 시스템 및 방법
- 내용기반의 출력물 보안 시스템 및 방법

05. Privacy-i 레퍼런스

**1,000여곳에서 28년 동안 축적/개발한 엔드포인트 보안기술을 지속적으로 고도화하여
600여 유지관리 고객사에 업그레이드 하고 있습니다.**

경기도교육청	12만
서울특별시	1만
고용노동부	1만
kt	3만
하나은행	1만 5천
신한은행	1만

05. Privacy-i 레퍼런스

공공 시장 1위

- 1,000여개 고객사, 600여개 유지관리고객사에서 사용하고 있습니다.
- 주요 중앙행정기관, 공기업, 지방공기업, 준정부기관, 기타공공기관 200곳 이상 도입 제품입니다.

중앙부처

고용노동부 | 법무부 | 문화체육관광부 | 국민안전처 | 인사혁신처 | 대한민국 국방부

특허청 | 국세청 | 병무청 | 경찰청 | 검찰 | 문화재청

산림청 | 방위사업청 | 농촌진흥청 | 감사원 | 헌법재판소 | 공정거래위원회

광역시도청 및 교육청

서울특별시 | 경기도 | 대전광역시 | 대구광역시 | 울산광역시 | 경기도교육청

세종특별자치시교육청 | 대전광역시교육청 | 충청북도교육청 | 전라북도교육청 | 경상남도교육청 | 제주특별자치도교육청

05. Privacy-i 레퍼런스

공공 시장 1위

- 1,000여개 고객사, 600여개 유지관리고객사에서 사용하고 있습니다.
- 주요 중앙행정기관, 공기업, 지방공기업, 준정부기관, 기타공공기관 200곳 이상 도입 제품입니다.

중앙부처 산하기관 & 기타기관

우정사업본부 | 한국수력원자력(주) | 한국동서발전(주) | 한국서부발전(주) | KOMIPO 한국중부발전 | 한국전력기술
국민건강보험공단 | NPS 국민연금공단 | KDIC 예금보험공사 | KNOC 한국석유공사 | 한국가스공사 | ex 한국도로공사
KOMSCO 한국조폐공사 | 한국관광공사 | HUG 주택도시보증공사 | TP 사학연금 | 근로복지공단 | 건강보험심사평가원
공무원연금공단 | 한국보훈복지의료공단 Korea Veterans Health Service | 안전보건공단 | 한국장애인고용공단 | HRDK 한국산업인력공단

병원

SAMSUNG 강북삼성병원 | SAMSUNG 삼성서울병원 | SAMSUNG 삼성창원병원 | 연세대학교 의료원 YONSEI UNIVERSITY HEALTH SYSTEM | 고려대학교안암병원 KOREA UNIVERSITY ANAM HOSPITAL | 인제대학교백병원 INJE UNIVERSITY PAIK HOSPITAL
대전한방병원 DAEJEON UNIVERSITY | GNUH 경상대학교병원 | 국립목포병원 | 보건복지부 국립부곡병원 | 보건복지부 국립나주병원 | 국민건강보험 일산병원

05. Privacy-i 레퍼런스

금융 시장 1위

- 주요 금융사(은행, 생명, 화재, 카드, 증권 등)에서 사용하고 있습니다.
- S사 등 외산 솔루션 윈백(Win-Back) 사례를 다수 확보한 제품 입니다.

금융

하나은행 | 신한은행 | KB국민은행 | 수협 | DGB대구은행 | 광주은행
전북은행 | 한국수출입은행 | KB생명보험 | 하나생명 | NH농협생명 | KYOBO 교보생명
한화생명 | MIRAE ASSET 미래에셋생명 | Cigna 라이나생명 | AIA 생명 | 수호천사동양생명 | Heungkuk
KB손해보험 | DB손해보험 | AIG 손해보험 | Heungkuk | KB국민카드 | Hyundai Card
SAMSUNG 삼성카드 | 비씨카드 | SAMSUNG 삼성화재 | KB증권 | create with you 삼성증권 SAMSUNG | 하나대투증권
meritz 메리츠증권 | MG새마을금고중앙회 | 하나금융지주 | KB금융지주 | KB신용정보 | SBI 저축은행

05. Privacy-i 레퍼런스

엔터프라이즈 시장 1위

- 메이저 제조, 통신, 서비스 기업 고객사를 보유한 제품입니다.
- 산하 계열사, 뿐만 아니라 유럽/미국/중국 등 해외법인에서도 운영하고 있습니다.

기업

삼성전자, 삼성물산, 삼성전자판매, 삼성전자서비스, 삼성헬스토리, 삼성에버랜드, THE SHILLA, 삼성SDS, LG전자, LG화학, LG디스플레이, LG유플러스, LG상사, LG이노텍, LG엔시스, LG패션, LG CNS, kt, kt skylife, SK하이닉스, SK이노베이션, SK텔링크, SK E&S, DOOSAN, posco, posco 포스코ICT, posco 포스코건설, posco 포스코에너지, posco 포스코알텍, LS, LS산전, S-OIL, NCSOFT, 금호아시아나

06. Best Practice

5여개 엔드포인트 보안솔루션을 하나의 에이전트로 구축 전환 완료

신한은행

항목	내용
배경	기존 외산제품(S사)의 기술지원 역량 부족으로 소만사 Privacy-i 싱글 에이전트로 교체
유저 수	10,000 유저
경쟁사	외산 S사 외
선정기준	❶ 기존 보안 에이전트 개수 단축 (출력물, 매체제어, PC보안, 개인정보 검색, DLP) ❷ Mac 에이전트 지원
결과	❶ 시스템 부팅시간 단축 ❷ 개인정보 검색시간 2배 이상 단축
비고	10년 이상 외산 S사 제품 사용 후 원백

하나은행

항목	내용
배경	엔드포인트 보안솔루션 개수 줄이기 기존 PC보안/개인정보보호 솔루션 단종
유저 수	15,000명 유저
경쟁사	외산 S사 외
선정기준	❶ 기존 보안 에이전트 개수 단축 ❷ 개인정보 검색기능 개선 (기존 대비 2배 이상) ❸ Mac 에이전트 지원
결과	❶ 서버 내 파일검색, 출력물 개인정보 포함여부 탐지, PC 개인정보 검색관련 개인정보 패턴 일치화 ❷ 개인정보 검색시간 2배 이상 단축
비고	10년간 국내 S사제품 사용했으나 단종되어 원백

2. 도입 필요성

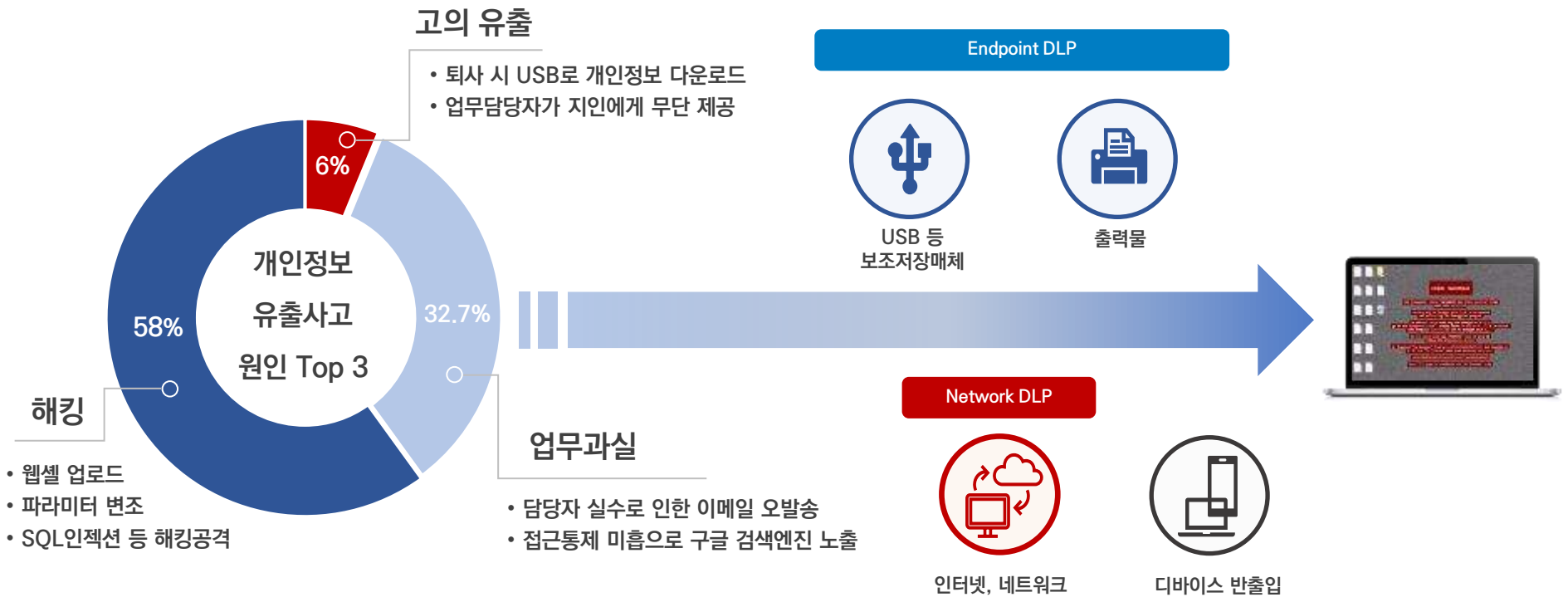
01. 4대 개인정보 유출채널별 DLP 솔루션

02. 데이터 유출사고 재발방지

03. 개인정보 컴플라이언스 준수

01. 4대 개인정보 유출채널별 DLP 솔루션

개인정보 데이터가 반출되는 대표적인 4대 채널은 보조저장매체, 출력물, 인터넷/네트워크 입니다.
해당 4대 유출채널에 보호조치를 구축하지 않을 경우 해커 또는 내부자에 의해 개인정보가 유출될 수 있으며
형사처벌, 손해배상소송, 기업가치 하락 등 피해규모는 걷잡을 수 없이 커지게 됩니다.



02. 내부 임직원 데이터 유출시 통제/차단

고의, 실수 여부와 상관없이 내부 임직원에 의한 개인정보 유출사고는 끊임없이 발생합니다.

Privacy-i는 업무상 발생할 수 있는 위험요소를 사전에 통제/차단함으로써
임직원들에게 안전한 보안환경을 제공합니다.

01

PC에 개인정보 천만 건 저장 후 매체에 복사

Privacy-i Copy Prevent +
① 저장매체로 개인정보 복사 시 검출
② USB 복사 결재 · 차단 · 경보 · 로그

02

고객정보 5만 건 PC에 보유, 신용정보회사에 판매

Privacy-i Discover
① PC내 개인정보 검출
② 보유현황 파악 · 암호화 · 파기 등

03

개인정보를 프린터로 출력 및 유출

Privacy-i Print Prevent +
① 개인정보 검출 · 결재 · 차단 · 경보 ·
② 워터마크 · 로그기록

직원의 실수에 의한 유출사고 사전 차단
처벌/소송 위험으로부터 직원 보호

업무관련 데이터 외부반출 시
실시간으로 탐지/기록하여 추후 소명가능

03. 개인정보 컴플라이언스 준수

기술적 조치를 취하지 않은 상태에서 **개인정보 유출시 〈관련매출 3%이하 과징금 부과〉**

Privacy-i는 데이터 유출방지 **법규정 준수를 위한 〈기술적 보호조치〉 100% 충족**합니다.

개인정보보호법 (개인정보보호위원회 법률 제19234호, 2023. 3. 14., 일부개정)

구분	조문내용	Privacy-i 법규충족/제공기능
21조 파기	① 개인정보 유효기간 만료, 처리목적 달성시 지체없이 파기 ② 복구/재생되지 않도록 파기조치 → 미조치시 3천만원 이하의 과태료 부과 (제 75조 제2항 제4호)	맥OS, 윈도우 기반 PC에서 개인정보 검출→파기
23조 민감정보 처리제한	① "민감정보"처리금지 (동의와 법에 따른 경우 제외) → 위반시 5년 징역 5천만원 벌금 (제71조 제4호) → 위반시 전체 매출 100분의 3을 초과하지 않는 범위 과징금 부과(제64조의2 제1항) ② 민감정보에 〈안전성 확보에 필요한 조치〉를 해야 함 → 미조치시 3천만원 이하 과태료 부과 (제75조 제2항 제5호)	빅데이터 검색엔진을 통한 민감정보 키워드 검색
64조의2 제9호 과징금의 부과	① 개인정보의 기술적, 관리적, 물리적 조치를 취하지 않은 상태에서 개인정보가 분실,도난,유출, 위조,변조,훼손된 경우 전체 매출액의 100분의 3을 초과하지 않는 범위의 과징금 부과	개인정보 파일 암호화, 유출방지기능을 통해 과징금부과, 손해배상소송 위험 예방
75조 제2항 과태료	② 3천만원 이하 과태료 4. 개인정보의 파기 등 필요한 조치를 하지 않은 자 5. 민감정보에 관한 안전성 확보 조치를 취하지 않은 자 13. 가명정보 처리 시 개인을 식별할 수 있는 정보가 생성되었음에도 이를 파기하지 않은 자	맥OS, 윈도우 기반 PC에서 개인정보 검출→파기/암호화 개인정보 파일 암호화, 유출방지기능을 통해 개인정보보호법고시 준수

03. 개인정보 컴플라이언스 준수

공공기관 개인정보파일 전수검사 대응 솔루션

Privacy-i를 통해 전직원 PC내 개인정보파일 전수검사 및 후속조치 일괄 수행할 수 있습니다.

개인정보보호법 제32조

① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다.

③ 보호위원회는 필요하면 제1항에 따른 개인정보파일의 등록여부와 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.

기관별 개인정보 전수조사 절차

기관별 세부 정비계획 수립

PC
개인정보파일 전수조사 실시
(Privacy-i 검사)

서버 (DB 포함)
서버/DB 전수조사 실시
(Server-i 검사)

내부 검토회의

〈주요 검토내용〉
- 지속운용 필요성
- 최소수집원칙 준수여부
- 등록항목의 적정성 등

후속조치 (등록, 암호화, 파기 등)

〈주의사항〉
- 보유근거, 보유기간 정보주체 수 확인 철저
- 암호화/파기 절차 파기방법 준수 등

Privacy-i 전수검사 대응기능

모든 PC 내 다양한 패턴의 개인정보 검색 및 조사를 원클릭으로 가능

보유한 개인정보 패턴 분류 및 예외처리

보유기간 설정
복구 불가한 방식으로 파기
파일 암호화 등

3. 기능소개

01. 강점

02. 기능

03. 구성도

01. 강점

01

★★★

통합 엔터프라이즈
DLP
기술력

데이터보호 관점에 기반
서버, PC, 네트워크까지 유출통제
데이터가 오가는 모든 채널 보호/통제

02

윈도우
맥 OS
모두 보안

99대 윈도우 PC, 1대의 Mac PC
단 1대의 PC로도 모든 정보는 유출됨
매체제어 및 Discover 기능 제공

03

엔드포인트
싱글 에이전트
통합보안

단 하나의 싱글 에이전트로
데이터 유출 차단 통제대응,
개인정보 자산식별, 매체제어 수행

01. 강점

통합 엔터프라이즈 DLP 기술력

데이터 보호 관점에 기반하여
서버, PC, 네트워크까지 탐지/통제/보호

기능	Mail-i	Privacy-i	Server-i
Discover	-	O	O
Prevent	O	O	-
매체제어	-	O	O
취약점탐지	-	O	O

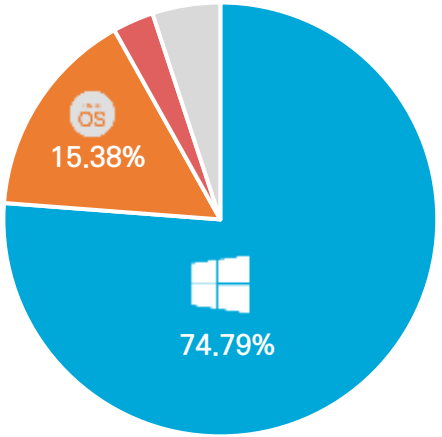
자체 개발한 '엔터프라이즈 DLP' 전문 기술력을 통해 데이터가 오가는 모든 채널 보호/통제

01. 강점

윈도우·맥OS 모두 보안

Discover (자산식별),
매체제어 (USB 등 보조저장매체, 블루투스 등 근거리 통신 통제) 기능 제공

세계 PC 운영체제 점유율



100대의 PC 중 99대는 Windows, 1대는 macOS일 때
OS 지원문제로 Windows만 보안한다면?

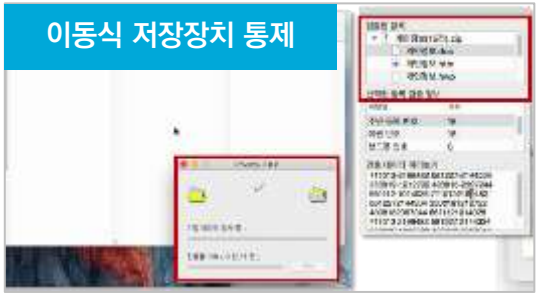
해커 또는 악의를 품은 내부임직원
정보유출 통제조치가 구축되어 있지 않은 macOS 기반 PC로 내부정보 유출

mac OS 시장은
Windows 대비 1/5 수준
그러나 R&D 투입비용은
Windows과 동일함

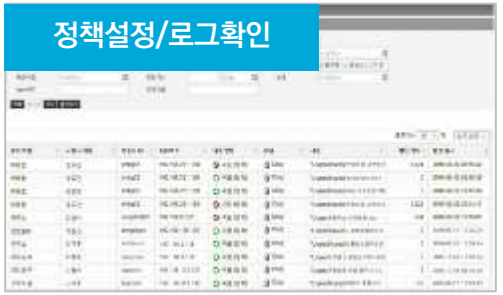
투자대비 수익에서
큰 매출을 기대할 수 없어
보안업체의
시장진출이 전무한 상황

개인정보 검출

이동식 저장장치 통제



정책설정/로그확인



Statcounter: Desktop Operating System Market Share Worldwide (2022)

01. 강점

엔드포인트 싱글 에이전트 통합보안

데이터 보호 관점에 기반하여
서버, PC, 네트워크까지 탐지/통제/보호

단 하나의 엔드포인트 싱글에이전트로

데이터 유출 차단 통제대응 뿐만 아니라 개인정보 자산식별, 매체제어까지 수행

02. 기능

Discover

데이터 분석
- 고유식별정보를 포함한 13종 이상의 [개인정보]패턴 검색 · 분석 가능
- 사용자 정의 패턴검출

자가검출 및 분류
- 유휴시간대 검사 (업무지장 최소화)
- 검출된 파일 암호화 또는 파기
- 파일 예외처리, 보유기간 설정 등

원격 검사/보호조치
- 개인정보 파일 원격 검사/암호화/파기
- 문서 승인/결재 정책 설정
- 검사 요약/보유기간 만료 알림 등

Prevent

보조저장매체 개인정보 유출차단 (Copy Prevent+)
- USB 복사시 개인정보 검출/차단
- 복사된 파일 원본저장 및 로깅
- 미등록 저장매체 사용 차단

출력물 통한 개인정보 유출차단 (Print Prevent+)
- 출력물에 개인정보 포함시 차단
- 출력 파일은 Text/JPG 로깅
- 워터마크 삽입

네트워크 통한 개인정보 유출차단 (Upload Prevent+)
- 웹메일 통한 개인정보 전송통제
- 클라우드, 메신저, 블로그, 페이스북 등 업로드 통제

클립보드 통제 (Clipboard Prevent+)

어플리케이션 통제 (Application Control)

미디어 통제 (Media Control)
악성 Rootkit 통제

Bigdata Search & Report

- 요약 및 상세 분석 가능한
- 드릴다운 검색 기능

- DB검색 대비 1,000배 빠른
- 빅데이터 검색 기능

- 침해사고 대응을 위해
- 원본파일, 유출내역 상세 로깅

- 사용자, 부서별
- 접속자 리포팅 등

02. 기능

Discover

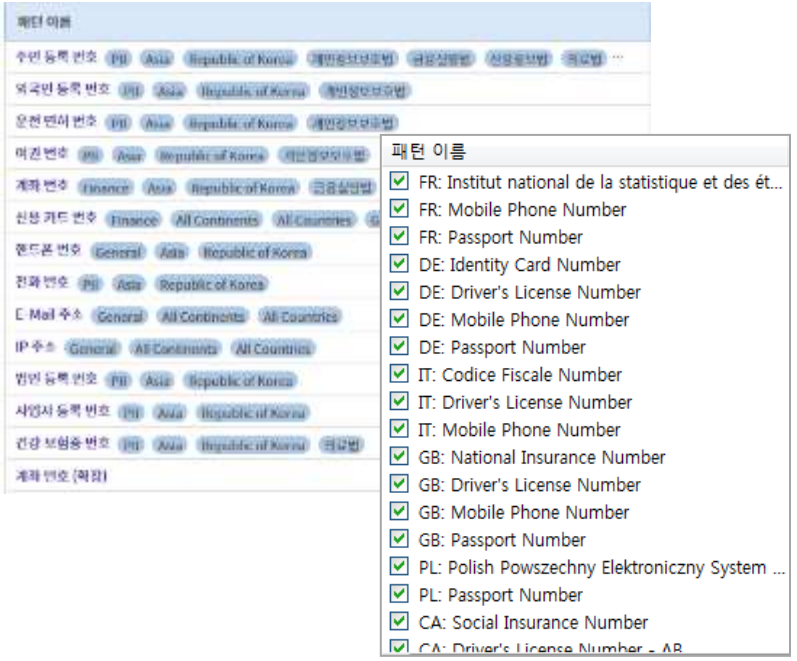
개인정보 패턴분석
13종이상 개인정보 패턴 분석/통제

네트워크를 통해 반출되는 개인정보패턴 정확하게 탐지

- 국내 주요 개인정보 모두 지원, 유효성체크

  주민등록번호, 외국인등록번호,
  유일 체크섬
  운전면허번호, 여권번호, 핸드폰번호,
  계좌번호, 신용카드번호 등

- 건강보험번호 등 추가 개인정보 패턴 등록
- 사용자 정의 패턴(정규표현식/키워드) 등록
- EU(GDPR준수), 북미, 중남미 국가 개인정보 패턴보유
  → 글로벌 컴플라이언스 대응



국가/국적 구별없이 네트워크로 반출되는 모든 개인정보패턴 분석 통제

02. 기능

Discover

MS오피스, 아래 한글, PDF, 구글 워크스페이스 등 50여 문서포맷 분석
다단계 압축파일, 확장자 변조파일 등 변칙을 사용해도 구분 및 분석

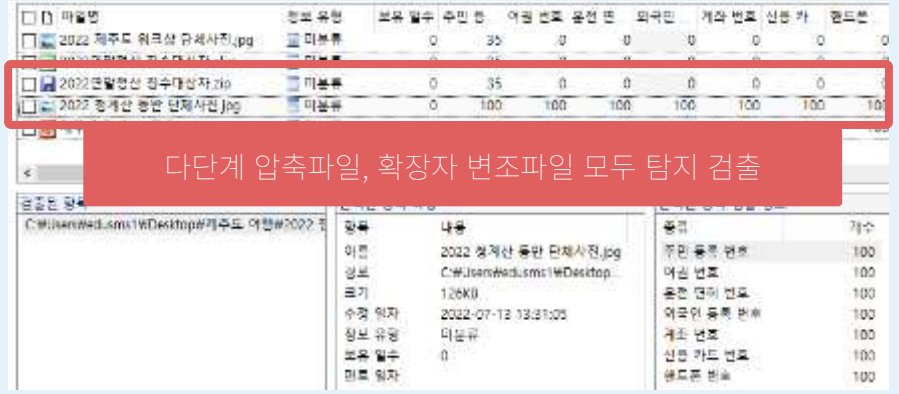
바이너리 파일

파일 포맷을 탐지하고
해당 파일 내 텍스트를 추출하여
개인정보 패턴을 탐지할 수 있어야 함

- ✓ 상용화된 문서 포맷 50여개 탐지 및 내용 검출
- ✓ CAD/CAM, VDI 등 전문 소프트웨어 포맷 탐지가능

압축 파일

DRM, 다단계 압축파일, 확장자 변조탐지 파일을
구분하고 분석할 수 있어야 함

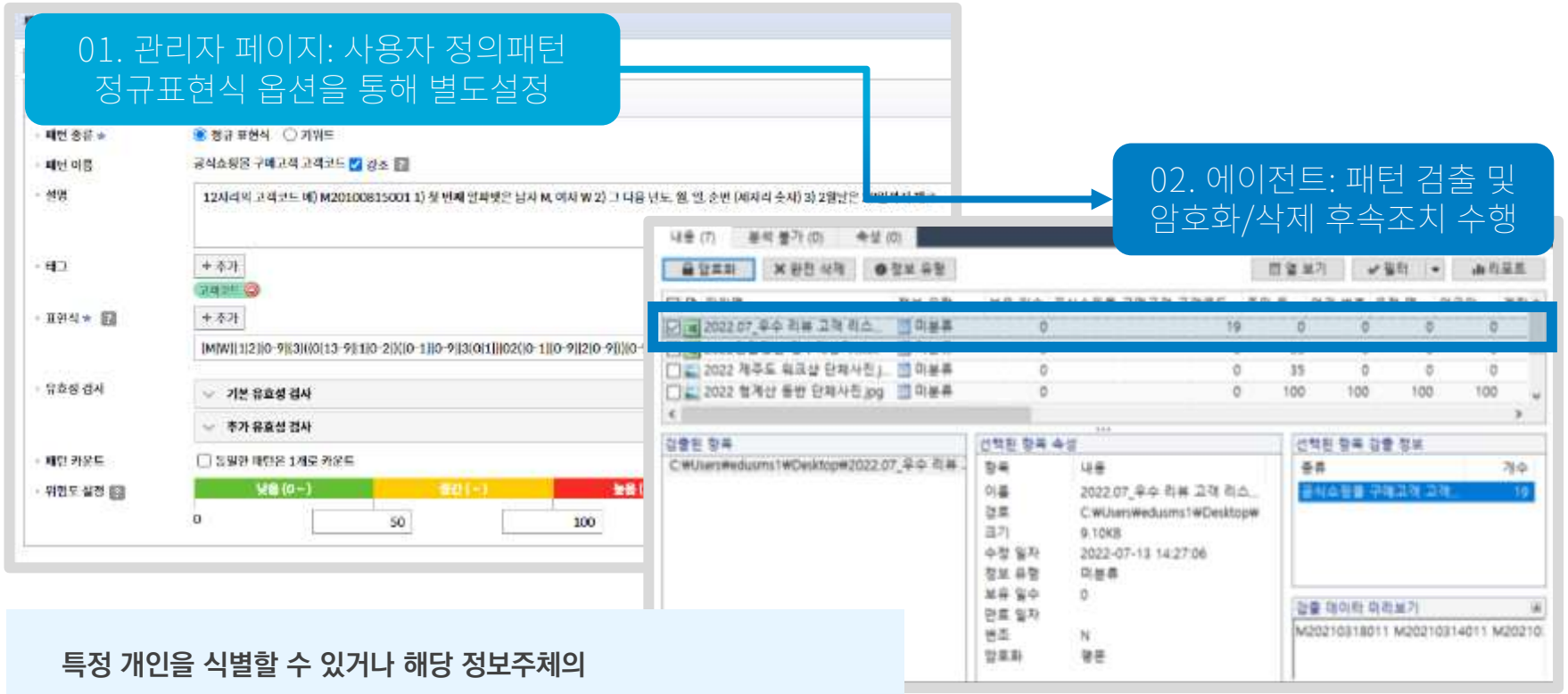


- ✓ ZIP, JAR, RAR 등 알려진 압축/아카이브 파일 포맷 탐지 및 내용 검출
- ✓ 5회 이상 다단계 압축해도 실제 콘텐츠를 확인하기 때문에 100% 탐지
- ✓ 이미지파일로 확장자 변조한 문서파일도 탐지

02. 기능

Discover

사번 · 고객코드 · 구매코드 등 소속기관에서만
사용하는 패턴도 사용자 정의패턴으로 추가등록 및 탐지가능



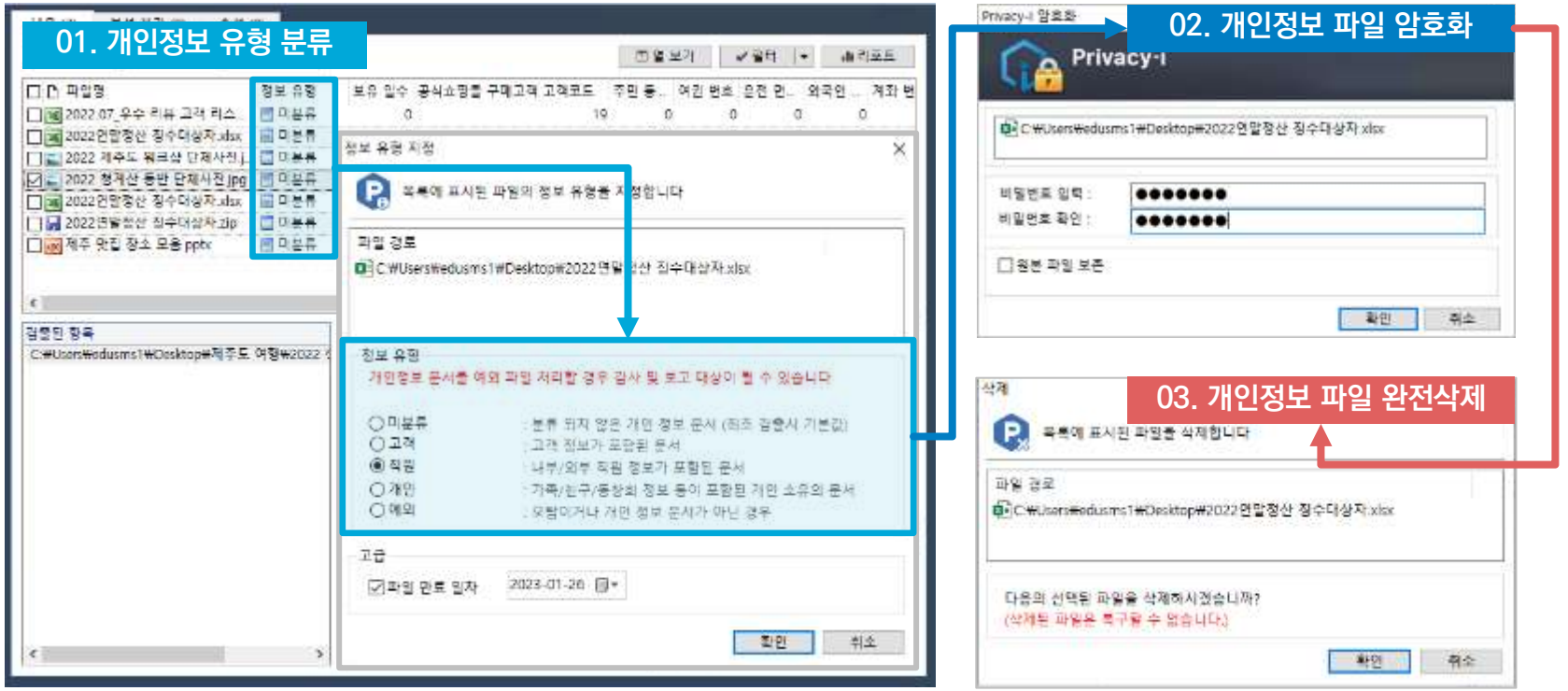
특정 개인을 식별할 수 있거나 해당 정보주체의
평판, 재정상황, 사생활과 연관된 개인정보는
표현식 또는 키워드를 기준으로 검출, 삭제, 암호화하여 보호 가능

02. 기능

Discover

직원이 직접 자가검출, 자가분류, 보유기간지정, 파기, 암호화 수행
보안팀 리소스절감 및 내부직원 마찰 감소

- 검출된 파일 암호화 또는 파기
- 파일 예외처리, 보유기간 설정 등
- 유휴시간대 검사 (업무지장 최소화)



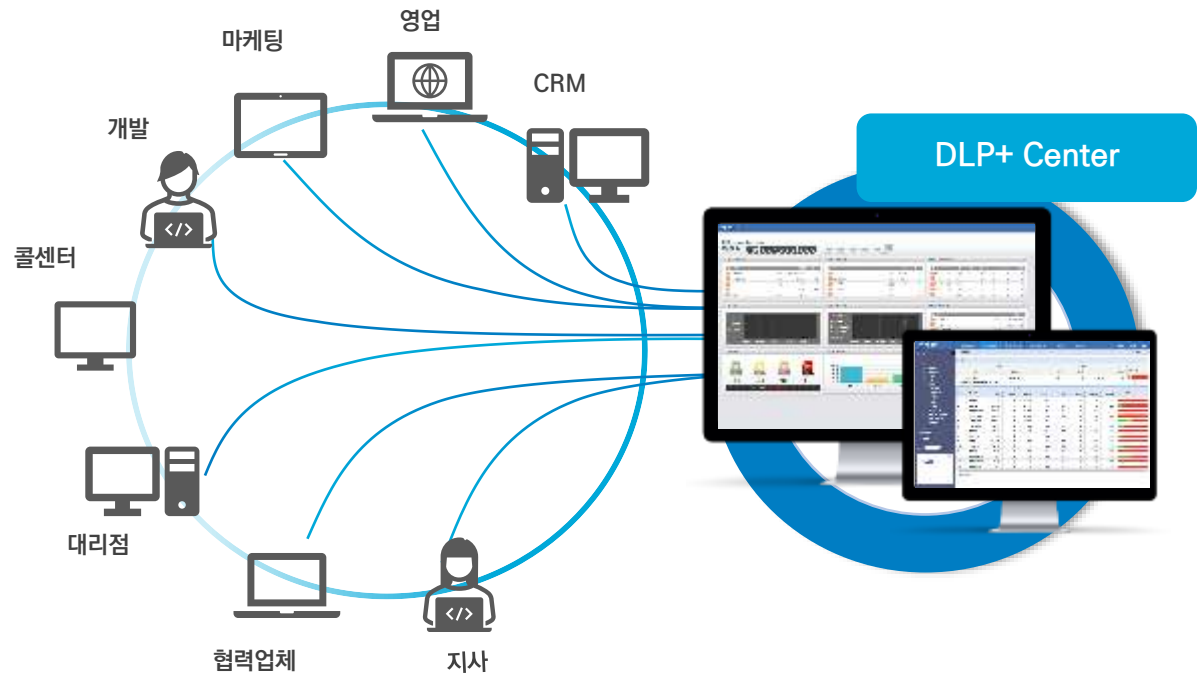
02. 기능

Discover

웹콘솔 DLP+Center에서 원격 검사/보호조치 수행
사내 중요정보, 파일, 에이전트 일괄관리 가능

정책 설정, 원격 보호 조치 가능

- 개인/부서/업무성향 별 세부정책 설정 후 실시간 원격 적용
- 특정직원 PC 내 저장된 개인정보, 민감정보의 실시간 보호조치가 필요할 경우 원격으로 삭제 또는 암호화 수행



02. 기능

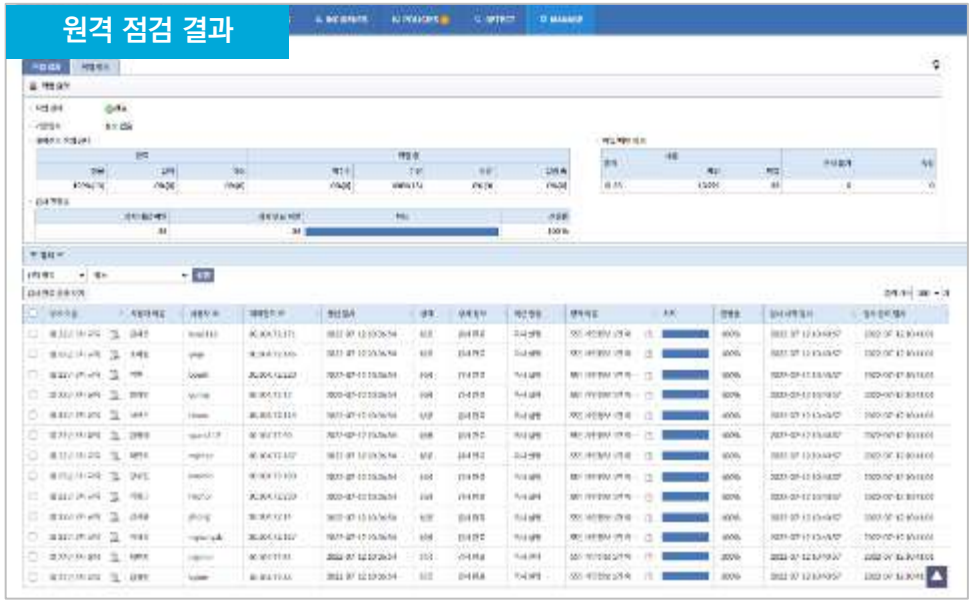
Discover

웹콘솔 DLP+Center에서 원격 검사/보호조치 수행
사내 중요정보, 파일, 에이전트 일괄관리 가능

직원 PC 원격 점검 후

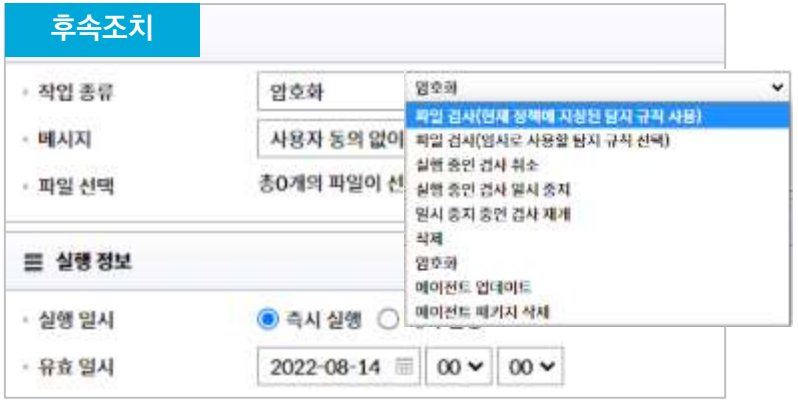
- 후속조치가 필요한 직원들을 선택하여 원격에서 〈재검사, 삭제, 암호화, 에이전트 업데이트〉 수행 가능
- 파일 삭제, 암호화의 경우 〈삭제, 암호화 대상〉 파일만 선택하여 처리가능

원격 점검 결과



직원 업무용PC내 개인정보파일 현황

후속조치



02. 기능

Prevent

이동식 저장매체 개인정보 유출차단 (Copy Prevent+)

시나리오:
주민번호 5건 이상 USB 복사

Privacy-i 웹콘솔 DLP+ Center

정책 설정/적용

결재 요청/승인

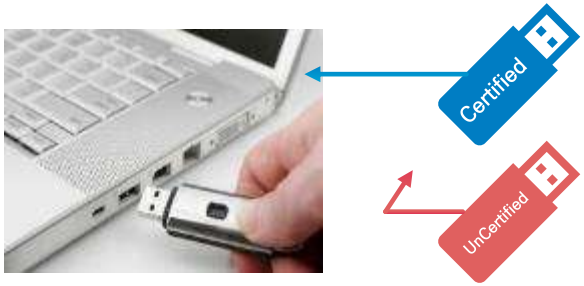
로그 및 파일원본

Privacy-i PC 에이전트

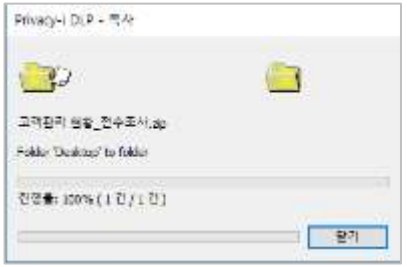
3 로그저장 및 탐지 개인정보 분석

4 날짜, 키워드, 패턴 초고속 검색

1 등록된 저장장치만 허용



2 개인정보 검사 후 정책에 따라 차단 · 결재 · 전송



02. 기능

Prevent

출력물을 통한 개인정보 유출차단(Print Prevent+)

시나리오:
주민번호 5건 이상 프린트 출력

Privacy-i 웹콘솔 DLP+ Center

정책 설정/적용

결재 요청/승인

로그 및 파일원본

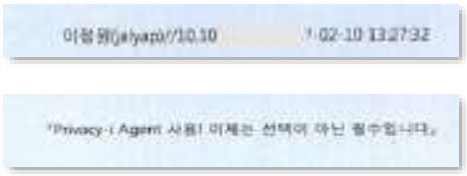
Privacy-i PC 에이전트

3 로그저장 및 탐지 개인정보 분석

4 날짜, 키워드, 패턴 초고속 검색

1 개인정보 검사 후 정책에 따라 차단 · 결재 · 출력

2 출력시 프린트 워터마크



일련번호 삽입, 출력문서 추적용이

02. 기능

Prevent

네트워크를 통한 개인정보 유출차단 (Upload Prevent+)

웹메일, 클라우드, SNS, 웹게시판 등

시나리오: 주민번호 1건 이상 포함된 파일 메일 발송시 차단

상용 웹메일로 개인정보파일 전송 시 내용기반 통제

1 상용 웹메일에 개인정보 파일 첨부, 전송 시도

2 Privacy-i 개인정보 패턴 탐지 및 차단

3 네트워크 업로드 로그 및 파일 원본 저장

Privacy-i 업로드 통제 대상 (일부)

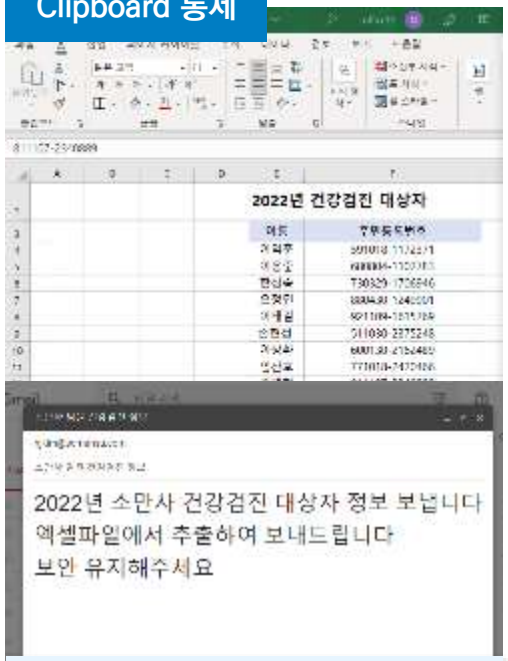
kakaomail nate MYBOX Gmail Google Drive amazondrive

02. 기능

Prevent

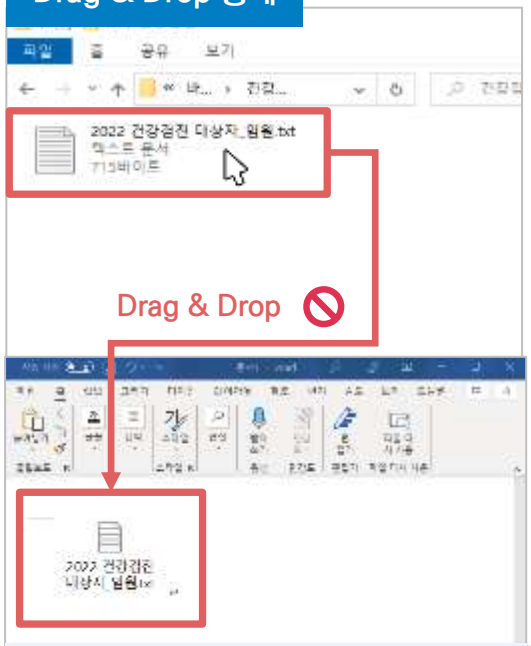
개인정보 복사& 붙여넣기 또는
파일 Drag& Drop 통제 (Clipboard Prevent+)

Clipboard 통제



복사시 Clipboard에 저장되는
텍스트 정보 및
개인정보 파일에 대해
내용기반 통제

Drag & Drop 통제



MS Office와 같이 문서 본문에
파일 Drag & Drop을
지원하는 경우
내용기반 통제

통제대상 응용프로그램

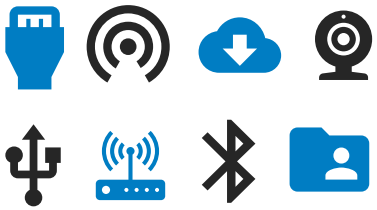
보안솔루션을 무력화하거나
악용될 소지가 있는
RootKit, Sysinternals,
모니터링 프로그램은 사전 차단

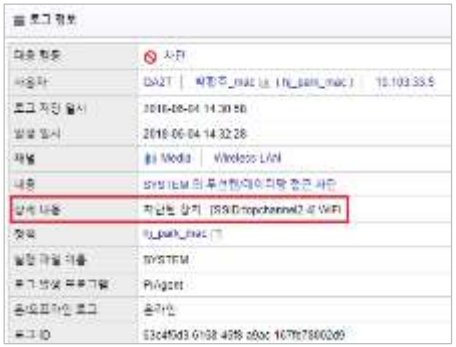
02. 기능

Prevent

기타 DLP 및 에이전트 보호:
불필요 or 정보유출 가능성 있는 인터페이스/앱 실행차단 및 로깅

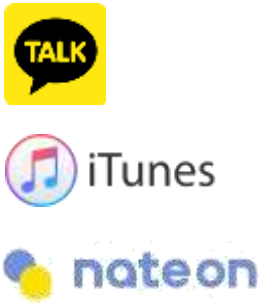
Media Control

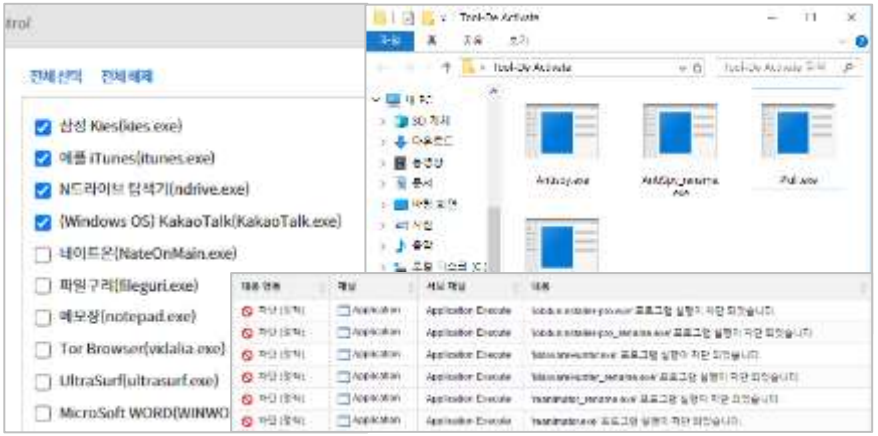




- 불필요한 주변기기 접근 통제
- 정보유출에 악용될 수 있는 인터페이스 비활성화 (허용 / 차단 / 읽기 전용 등)
- 차단 로그 저장

Application Control





- 카카오톡, 아이튠즈 등 정보 유출에 악용 가능성이 있는 어플리케이션 실행 차단
- 에이전트를 우회할 수 있는 악성 어플리케이션 차단 (에이전트 보호)

02. 기능

Prevent

기타 DLP 및 에이전트 보호: PC Security, 에이전트 보호

제29조(안전조치의무)

개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.

PC Security

- 공유폴더 사용 허용여부, 기본공유 허용여부 선택을 통해 개인정보보호법고시 준수가능
- 화면보호기, 화면 캡쳐기능 사내지침에 따라 통제가능
- 사용 차단로그는 저장하여 사후감사용도로 활용가능

에이전트 보호

Agent 모듈 숨김

- 프로세스 강제종료 or 삭제 방지목적
- 에이전트 주요 실행모듈 숨김처리
- 작업관리자 실행 프로세스, 레지스트리 등록정보, 윈도우 탐색기의 설치 폴더 숨김처리

언-인스톨 (Uninstall)방지

- 사용자에 의한 에이전트 임의삭제 방지

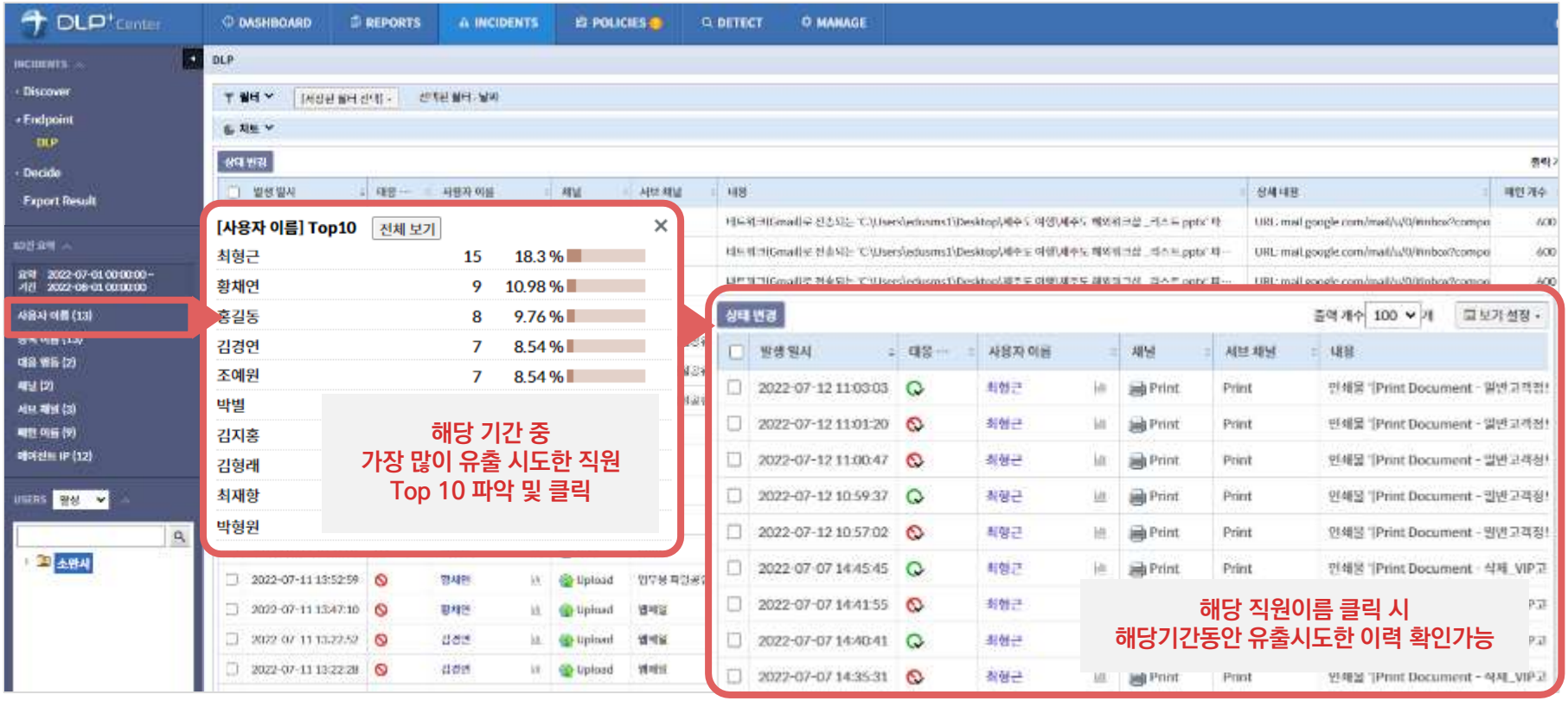
서비스/드라이버 종료방지

- 서비스 설정 변경방지 등

02. 기능

Search & Report 요약 및 상세 분석 가능 드릴다운 검색 기능

시나리오 202X.7월 '개인정보 유출시도'를 가장 많이 수행한 직원 찾기



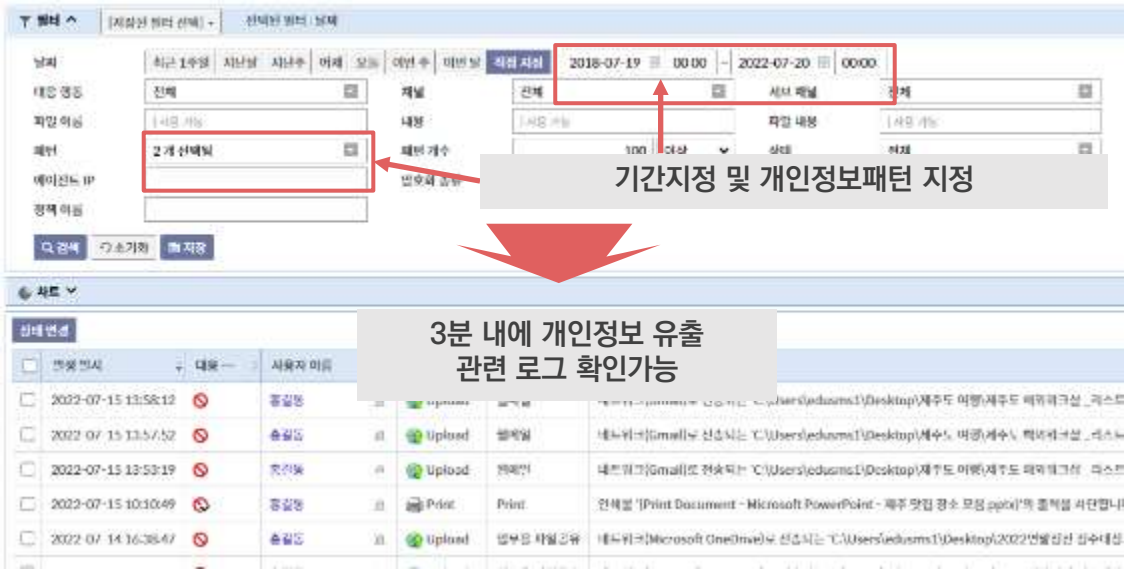
02. 기능

Search & Report

3년 대용량 로그 3분내 초고속 '빅데이터 검색'
DB검색 대비 단축시간 1,000배 단축

- 수년간 축적한 수백만 건 로그 속에서 원하는 정보를 3분 이내 검색 가능
- 고속 검색 시스템을 통해 보안 담당자가 정보유출 또는 이상징후에 신속 대응할 수 있음
- 복합(통합) 조건검색(채널, 파일명, 허용/차단, 패턴, 패턴 개수 등)으로 재검사 없이 원하는 로그 즉시 확인
- 개인정보/민감정보 관련 30개 키워드 동시 검색 가능

3년치 주민번호/여권번호 유출시도 기록 검색결과



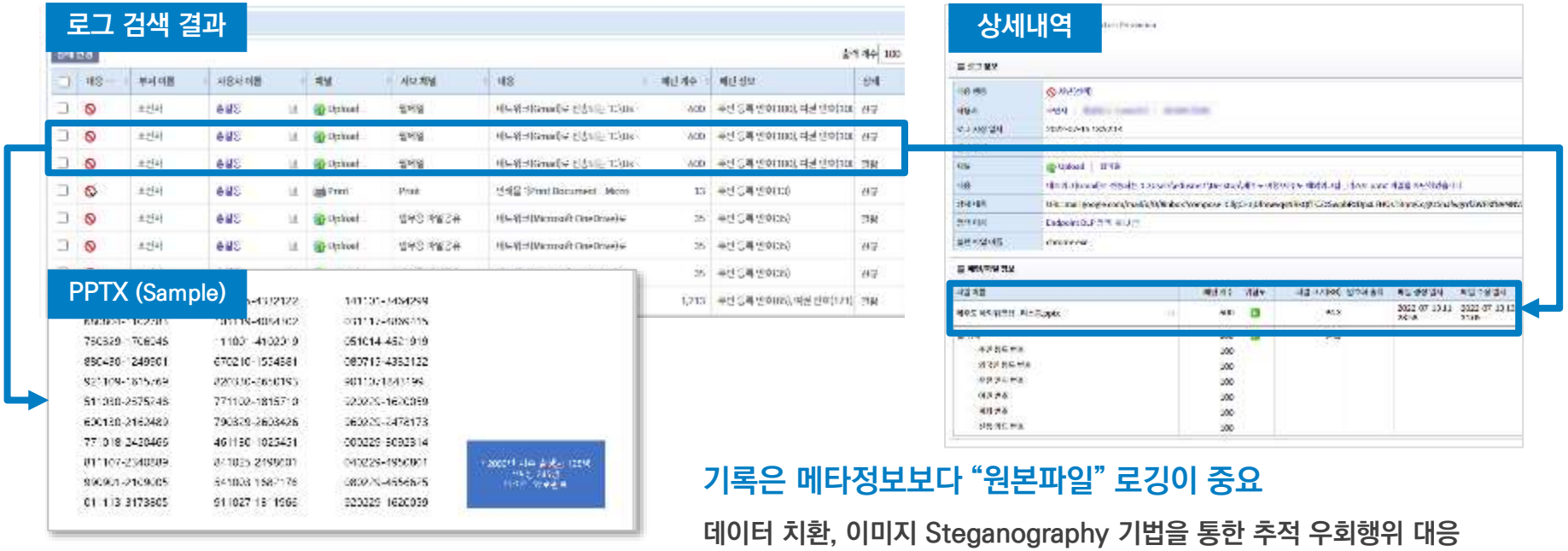
3년치
개인정보 유출내역
3분 내 검색

02. 기능

Search & Report

침해사고 대응을 위해 원본파일, 유출내역 상세 로깅

- 침해사고에 실시간으로 대응할 수 있도록 원본 파일, 유출 내역 등 상세하게 기록/저장
- 수백만 건의 로그에서도 확인하고자 하는 인시던츠를 초고속 검색을 통해 즉시 검출
- 포렌식 관점에서 유출경로 및 유출된 데이터를 100% 재구성하여 사후감사자료로 활용 가능



기록은 메타정보보다 “원본파일” 로깅이 중요

데이터 치환, 이미지 Steganography 기법을 통한 추적 우회행위 대응

➡ 법적 증거자료 확보, 책임소재 추적, 감사자료 활용 필수

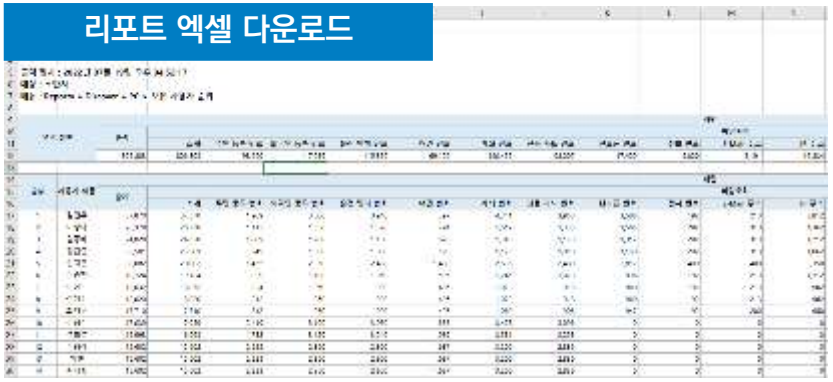
02. 기능

Search & Report 사용자, 부서별 접속자 리포팅 등

- 기본 리포트 및 대시보드 기능 이외에도 사용자 및 파일 관점에서 데이터 가시성을 확보할 수 있는 툴 제공

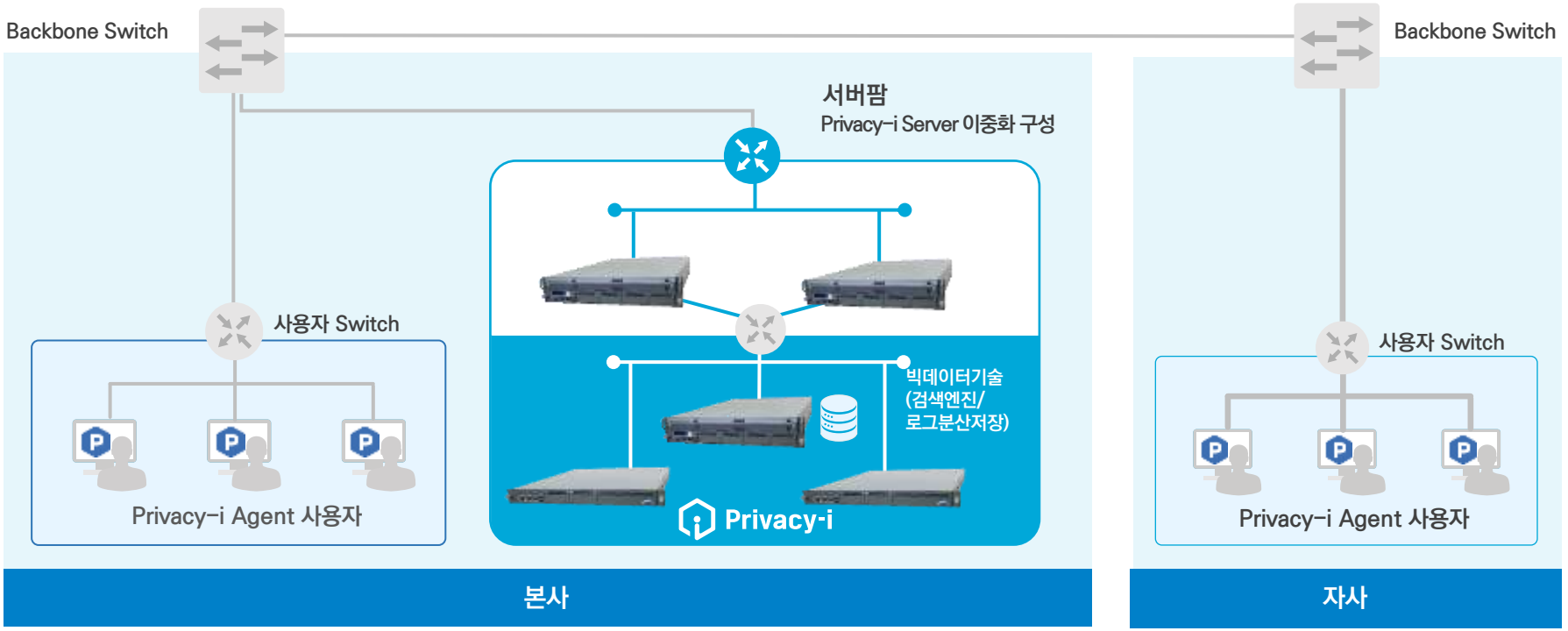
부서/사용자/패턴별 리포트

리포트 엑셀 다운로드



웹/사용자/에이전트 대시보드

03. 구성도



Privacy-i Server 이중화 구조 제안

- 이중화 서버는 중앙에 위치
- 로드밸런싱/서버장애 시 Fail over 수행
  [대당 수천 명의 로그인 및 데이터전송 처리 검증]
- 빅데이터 기술기반 검색엔진 및 로그 분산저장

구성요소

Privacy-i Agent	사용자PC에 설치, 개인정보 검출·암호화·삭제 등 보호조치 수행
Privacy-i Server	통합 정책 관리 및 제어, 리포팅
로그관리	대용량 로그처리 기술(검색엔진, 로그 분산저장), 로그 위변조 방지

03. 구성도

어플라이언스

DLP 전용 패킷처리 엔진 탑재
프라이버시 슈퍼엔진 자체 개발로 패킷 처리능력 외산대비 4배 개선

제품	BG500	EF1000	EF2000
사양	· Xeon E-2234, 3.8G/4C · HDD 1TB over · 전원 이중화(Dual)	· Xeon Silver 4410Y, 2.1G/8C · HDD 1TB over · 전원 이중화(Dual)	· Xeon Silver 4410Y, 2.1G/8C * 2 · HDD 1TB over · 전원 이중화(Dual)
유저	~300유저	~ 4,000유저	4,000유저 이상
외형			

* 본 사양은 사전 예고없이 변경될 수 있습니다.
처리 성능은 해당사이트의 네트워크의 특성에 따라서 변동될 수 있습니다.

4. 제품 비교표

제품비교표

항목		소만사	국내 A사
DISCOVER (중요 정보 검출)	Windows, macOS 개인정보 검출 모두 지원	O	X
	개인정보 패턴 지원범위 (국내 13종 및 미국, 일본, 중국, GDPR 등)	O	O
	사용자 정의 패턴/키워드 설정 및 검출	O	O
	검출된 파일 유형 분류, 파일 만기일 지정	O	O
	파일 암호화 또는 파기	O	O
DLP (정보 유출 방지)	미등록 USB/외장하드 등록/차단	O	O
	이동식 저장매체, 출력물을 통한 유출 차단	O	O
	반출된 파일 원본저장	O	X
	클립보드 / Drag & Drop 통제	O	X
	Media(인터페이스) 통제	O	X
	어플리케이션/에이전트 우회 프로그램 통제	O	X
검색/리포팅 (초고속 검색/리포팅)	대량로그에서 복합(통합)조건 3분 이내 초고속 검색(보고, 사고 대응시 필수)	O	X
	부서별, 개인별, 패턴별 보유현황 리포트(리포트 Export 포함)	O	O
	특정 사용자/파일의 현황 확인을 위한 파일뷰/사용자뷰	O	X

5. 프로젝트 관리 및 교육

01. 기술평가등급 T2

02. 프로젝트 수행

03. 기술지원 및 정기적 서비스

01. 기술평가등급 T2

- 기술평가등급 T2 → **기술력 상위 1% 이내**
- 200여명 기술인력 보유
- 인프라 구축부터 유지관리까지 단일 벤더에서 일괄지원대응

기업체명	(주)소만사
대표자명	김대환
사업자등록번호	214-86-14882
법인등록번호	110111-1394115
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
산업분류	[J58222] 응용 소프트웨어 개발 및 공급업
유효기한	2024년 08월 08일
제출처 및 용도	적격심사 및 공공기관 제출용

기술평가등급

T2

평 가 일	2023년 08월 09일

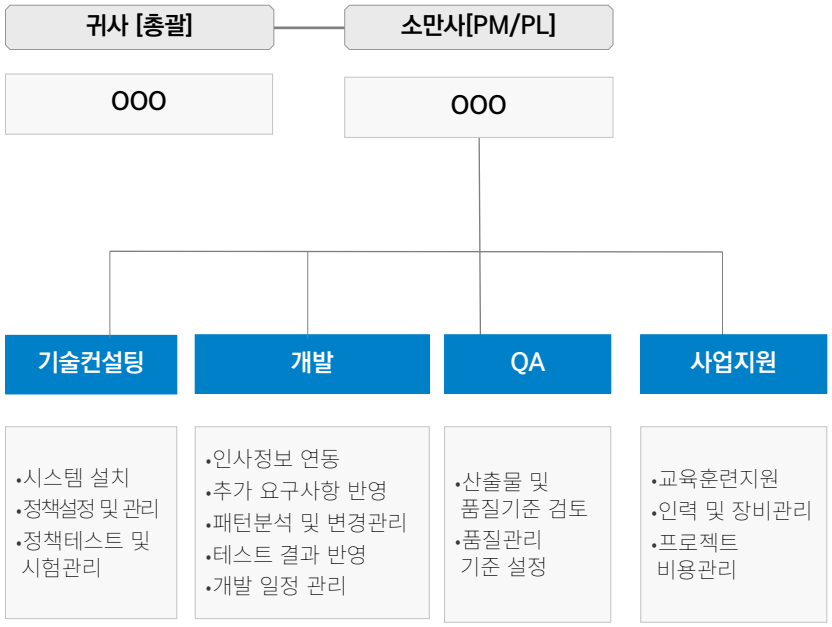
기술평가등급	매우취약	취약	미흡	보통이하	보통			보통이상			양호			우수			매우우수	최우수
	T10	T9	T8	T7	T6-	T6	T6+	T5-	T5	T5+	T4-	T4	T4+	T3-	T3	T3+	T2	T1
	기술력이 매우 우수한 수준으로 산업 및 시장환경의 급격한 변화에도 어느 정도 대응능력을 갖추고 있어 안정적임																	

02. 프로젝트 수행

㈜ 소만사는 Privacy-i 구축사업의 성공적 수행을 위해 계약부터 완료까지 귀사와의 유기적 관계를 유지할 수 있는 조직을 구성합니다. 또한 완벽한 품질의 산출물이 생성되도록 독립적인 품질보증 팀의 지원을 받아 원활하고 효율적인 프로젝트 수행이 가능하도록 하며, 프로젝트 관리자가 전체 프로젝트 팀을 효율적으로 관리할 수 있도록 조직을 구성합니다.

인력확보 방안 및 인적 구성의 적정성

〈 수행 조직 〉



〈 업무분장 〉

조직	역할
귀사	▪ 계약체결, 사업관리 및 사업비 신청내역 확인 ▪ 검사 및 인수, 사후관리 ▪ OOO에서 담당할 필요가 있는 세부적인 업무
소만사 (PM)	▪ 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 품질보증, 투입인력, 자원 및 예산 관리 ▪ 주요 이해당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
소만사(PL)	▪ 기술적인 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 기술적인 품질보증, 투입인력, 자원 및 예산 관리 ▪ 기술 당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
기술컨설팅	▪ 시스템 설치 및 구축(하드웨어, 소프트웨어 – 운영체제, 로그서버 등) ▪ 정책설정, 관리 및 운영 지원 / 주요 산출물 작성
개발	▪ 추가요구사항 반영/ 패턴분석 및 변경관리/ 테스트 결과반영/ 개발일정관리
QA	▪ 산출물과 품질기준 검토 및 품질관리 기준 설정 ▪ 표준화가 필요한 업무에 대하여 프로세스 및 정보항목 도출 ▪ 표준화 추진방안 제시

03. 기술지원 및 정기적 서비스

교육지원 담당자의 책임아래 교육훈련을 진행합니다.

교육준비, 교육실시, 평가 및 분석 3단계로 나누어 시행하여 훈련효과를 극대화 합니다.

훈련 실시 후 교육내용 활용도를 조사, 부족한 부분을 추가 교육하여 대상 그룹의 시스템 적응력과 운용능력을 극대화 합니다.

교육훈련 일정

교육과정	주요내용	교육일정	교육대상	관련자료/장소
기초교육	▪ 솔루션사용법 – 사용자 환경설정 및 접속방법 – 로그조회 등 감사활동 방법 ▪ 솔루션 개념 및 구축 기법 ▪ 솔루션 시스템 운영 및 활용 방안 ▪ 집합교육	▪ 1일(2시간소요) (프로젝트 초기: M) – 계약 후 4개월이내	▪ 총괄 담당 직원	▪ 운영 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 기본 교육	▪ 솔루션의 운영관리 – 시스템 운영환경(H/W및 S/W)에 대한 이해 – 솔루션 운영교육 – 보안규칙 적용방법 – 모니터링 및 감사활동 방법 ▪ 운영 지침 ▪ 시스템 전반적인 이해 ▪ 각 모듈 별 요소 기술 ▪ 보안관리자 ▪ 매뉴얼 사용 방법 ▪ 집합교육 또는 쿠폰	▪ 1주일(일1시간) (솔루션 설치 완료시: M+1) – 계약 후 5개월이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 심화 교육	▪ 운영단계에서 실제 운영 시 상세 제품교육 ▪ 보고서 활용 관련 리포트 활용법 ▪ 집합교육 또는 쿠폰	▪ 1일(3시간) (시스템 안정화 단계 시: M+2) – 계약 후 6개월 이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정장소

03. 기술지원 및 정기적 서비스

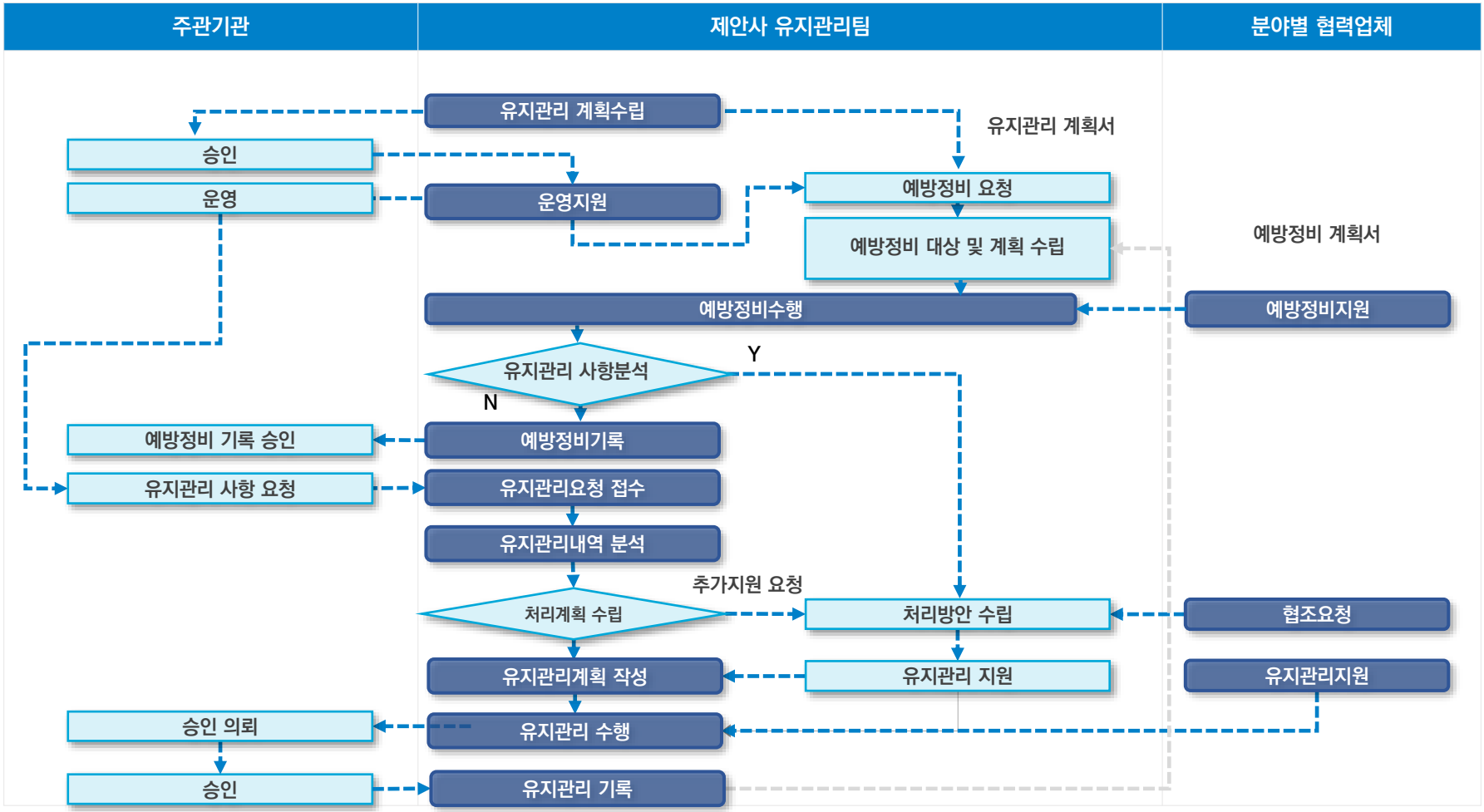
제안사의 운영기술 지원 서비스는 다음과 같이 5가지 영역으로 나뉘어 제공됩니다.
유지관리 정책은 검수 후 1년간 무상 지원되며,
이후 별도의 유지관리 계약을 통해서 지속적인 서비스를 제공합니다.

운영기술 지원 서비스

구 분	지원 방안	비고
예방정비 (PM)	• 전담 A/S 요원 정기점검 및 요청 시 방문 • 모듈 및 시스템 성능 검사 및 종합 테스트 • 정기적인 이론 실습 교육 • 전산 마인드 교육 • 업무시스템의 효율적인 사용을 위한 교육	• 전담 요원 확보 • 충분한 예비 시스템 확보
긴급정비 (EM)	• 유지관리를 위한 전담 엔지니어 확보 • Help Desk 운영을 통한 신속 정확한 장애 조치 • Diagnostic Program을 통한 정확한 고장부위 파악 및 조치	• 4시간 이내 착수하여 조치 이행함
서비스망 접수처리	• Help Desk를 구축 신속한 장애 접수 처리	• 상시 지원 체제 구축
기술지원	• Version Upgrade 관련 최신 기술정보 제공 • 대상 업무 검토 및 협의 • 시스템 성능향상을 위한 기술자문 및 신기술 세미나	• 유지관리 전담팀 활용
무상유지관리 기간	• 시스템 구축 후 1년	

03. 기술지원 및 정기적 서비스

1,000여개 유지관리 사이트 지원경험과 200여명의 전문가를 통한 대응체계를 고객에게 제공합니다

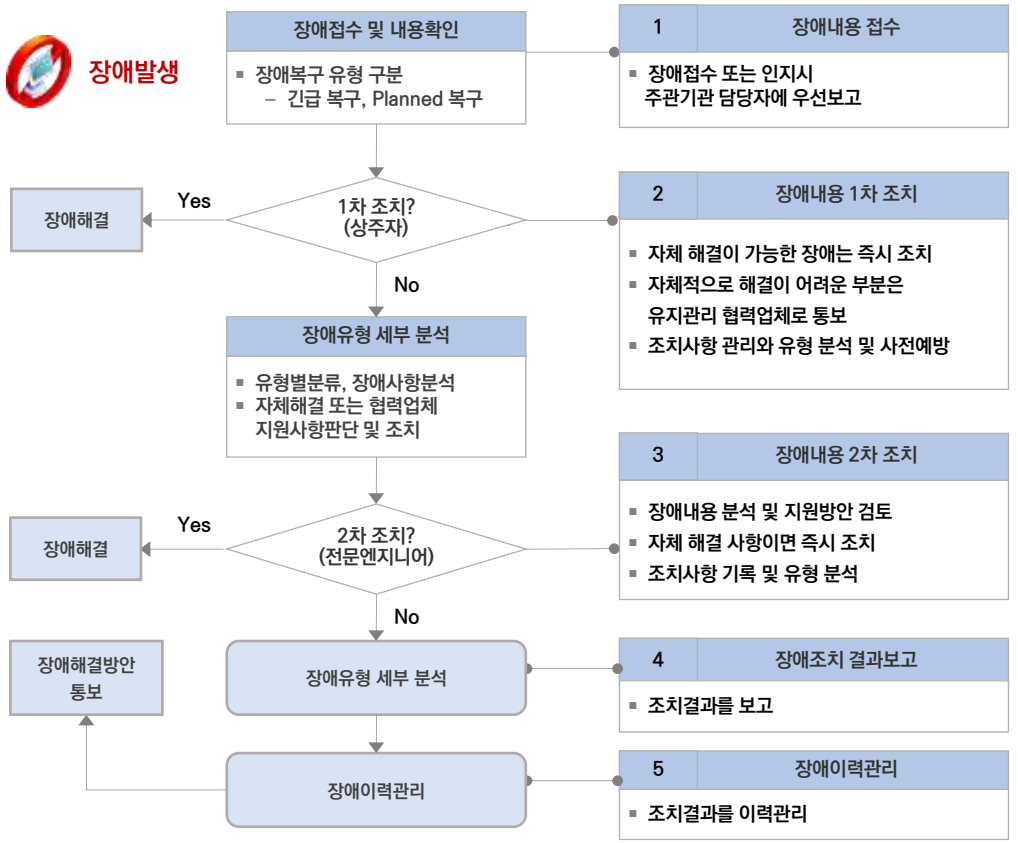


03. 기술지원 및 정기적 서비스

제안사 기술컨설팅 단일창구를 통해 장애접수 후

유지관리팀 및 주관기관 내 자체 운영조직에 의한 해결 또는 협력업체 현장방문으로 신속히 장애문제를 조치합니다

절차에 의한 체계적이고 신속한 장애처리



장애복구 유형별 조치방안

구분	내용	조치 담당자	비고
긴급 복구	장애요소제거 및 교체	유지관리 담당자	유지관리 수행팀은 전단계에 걸쳐 지속적인 지원
	시스템 (HW 및 SW) 가동	시스템 및 SW 운영자	
	서비스 가동 및 확인	업무담당자	
Planned 복구	복구작업 계획수립	관련자 전체	
	서비스 및 시스템 중지	업무담당자, 시스템 및 SW 운영자	
	장애요소 제거 및 교체	유지관리 담당자	
	시스템 및 서비스 가동, 확인	시스템 및 SW 운영자, 업무담당자	

시장 1위
엔드포인트 내부정보유출방지
(DLP) 솔루션

Privacy-i

성공적인 프로젝트로 보답하겠습니다

감사합니다

SOMANSA

서울특별시 영등포구 영신로220 KnK디지털타워 9층 소만사
대표번호 : 02-2636-8300 | 기술문의 : tech@somansa.com
제품구매 : 02-2655-4040 / sales@somansa.com

별첨

내용검출 포맷

Privacy-i 탐지가능 파일 포맷 리스트

유형	포맷이름	확장자명
워드프로세서	한글과 컴퓨터 아래아 한글	hwp
	Microsoft word	doc; docx
	핸디소프트 아리랑	hwd
	훈민정음/정음Global	gul
	iWork Pages	pages
	JustSystems Ichitaro	jtd
	OpenOffice Writer	odt; sxw
프레젠테이션	Microsoft PowerPoint	ppt; pptx; pps; potm; potx; ppam; ppsm; psx; pptm; thmx
	한컴오피스 한쇼	show
	iWork Keynote	key
	OpenOffice Impression	odp; sxi
스프레드시트	Microsoft Excel	xls; xlsx; xlsm
	넥스소프트 넥셀	nxl
	한컴오피스 한셀	cell
	iWork Numbers	numbers
	OpenOffice Calc	ods; sxc

유형	포맷이름	확장자명
텍스트	일반 텍스트	txt
	쉼표로 분리된 텍스트	csv
	Copy of Print Document	pvi
	Extensible Markup Language	xml
	Hypertext Markup Language	Html; htm
	Microsoft Hypertext Archive	mht
	Rich Text Format	rtf
이미지	Bitmap	bmp; dib
	Graphic Interchange Format	gif
	Joint Photographic Experts Group	jpg; jpe; jpeg
	Tag image file format	tif; tiff
데이터베이스	Microsoft Access	mdb; accdb
	Microsoft Outlook	msg;oft
	Microsoft Outlook Express	eml; mht
Autodesk Auto CAD		dwg

유형	포맷이름	확장자명
ARCHIVE	7z	7z
	ALZip	alz
	bzip2	bz2;tbz
	Gzip	gz; tgz
	JAR	jar
	LHA	Lzh; lha
	RAR	rar
	Tape archive	tar
	ZIP	zip; zipx
기타	Adobe Flash	swf
	Adobe portable Document Format	pdf
	핸디소프트 Bizflow Groupware	hwn; hwx
	Microsoft Compiled HTML	Microsoft Compiled HTML
	Microsoft Document Imaging	mdi
	XML paper Specification	xps

SOMANSA

유해 & 악성코드 배포사이트 차단

WebKeeper SG

SECURE WEB GATEWAY

SOMANSA

왜 WebKeeper인가?

업계 최장 25년간 공공/기업/금융 시장점유율 1위

업계 최다 1천 여 고객사 대상으로 고품질 차단DB 제공, 경쟁사 대비 3배 이상 업데이트

업계 최대 경쟁사 대비 기술인력 3배 이상 '240여 명' 전문 기술인력 보유

업계 최고 NDR과 EDR 동시대응 XDR 로드맵 보유, 자사 솔루션 통합하여 시너지 효과 보장

업계 최장

유해/악성코드 차단 및 데이터 보호 기술개발

25년간 시장점유율 1위

- **공공/기업/금융 시장 1위, 보안 기술력 1위, 유해차단 기술력 1위**
- **유해사이트 및 악성코드/랜섬웨어 차단, ChatGPT 통제** 등 웹서비스를 통한 데이터 유출차단까지 확대한 통합 보안 전문기업

업계 최다

1천 여 고객사 대상으로 고품질 차단DB 제공

경쟁사 대비 3배 이상 업데이트

- **1천개 고객사**를 통한 **국내 최대 DB 인프라 확보**
- **AI 인공지능기반 데이터 자동분류 기술** 적용 (국내 최초) **분석/업데이트 속도 향상 및 보안담당자 업무부담 해소, 보안위협 실시간 차단 고도화**
- 10여년 간 매일, 매월, 매년 업데이트 리포트 발행

업계 최대

국내최대 유해차단 전문 개발자/엔지니어 보유

경쟁사 대비 3배 기술인력 보유

- **소만사 임직원 3명 중 2명은 기술인력 (전체인원의 70%)**
- **경쟁사 대비 3배 이상 확보**
- 제품기획 및 기술개발에 참여한 전문인력을 통해 갑작스러운 인력 변동에도 원활한 기술지원 수행

업계 최고

NDR과 EDR 동시대응 XDR 로드맵

자사 솔루션 통합하여 4배 시너지 효과 보장

- **네트워크를 통해 유입되는 악성코드/랜섬웨어는 웹키퍼가 차단**
- 엔드포인트에서 탐지되는 악성위협은 자사 Privacy-i EDR로 차단
- 자사 솔루션을 통해 엔드포인트 부터 네트워크 단 까지 발생하는 보안위협 전방위 차단

SOMANSA

목차

1. 회사소개

01. 시장 1위 악성코드 차단 전문기업 소만사

02. 재무 안정성 상위 1%

03. 조직 및 기술력

04. 악성코드 분석 로드맵

05. 인증 및 지적 재산권

06. WebKeeper 레퍼런스

01. 시장 1위 악성코드 차단 전문기업 소만사

- 국내외 1천 여 고객사에서 도입 및 운용 중
- 연간 2천만 건 유해 · 악성코드 · 비업무 사이트 DB 업데이트 및 공유

2023

ChatGPT를 통한 개인정보 유출통제(로깅 및 차단) 개발 및 적용

2021

생성형 AI 기반 유해사이트(음란, 도박, 비업무사이트 등) 자동분류 시스템 국내최초 개발 및 적용

세계3대 악성코드 평가기관 바이러스 불러틴 VB100 A+ 인증 획득

2015

S그룹 표준 유해사이트 차단 시스템 선정 (국내제품 유일)

연간 1천만 건 이상 DB업데이트 (국내 경쟁사 대비 3배 이상)

WebKeeper SG 프락시 일체형 출시

빅데이터 검색기능 탑재 1천명 규모 3년 누적 접속 데이터 3분 내 검색완료

2010

1,000여개 고객사 달성 확보

국내최초 10G 트래픽처리 고성능 패킷처리엔진 개발

1998

국내최초 유해사이트 차단솔루션 국정원 CC인증 획득

유해사이트 차단 솔루션 WebKeeper 출시

1997

㈜소프트웨어를 만드는 사람들 설립

02. 재무안정성 상위 1%

- 중소기업 **재무안정성 상위 1%(A+), 유일한 무차입 기업**입니다
- **신용평가등급 A+, 현금흐름등급 CR-1로 중소기업 상위 1%의 재무적 안정성**을 바탕으로 소만사는 중장기 R&D 및 기술지원에 투자하고 있습니다


Korea Rating & Data

Ⅰ. 기업신용등급

회사명 : (주)소만사 대표자명 : 김대환 사업자번호 : 214-86-14882

■ 기업개요

기업명	(주)소만사
대표자	김대환
법인(주민)번호	110111-1394115
사업자번호	214-86-14882
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
업종	(J58222) 응용 소프트웨어 개발 및 공급업
주요제품명	개인정보보호, 내부정보유출방지, 안티랜섬웨어 및 악성코드차단 솔루션
종업원수	338명 (연구소 소속 117명 포함)
기업규모	중기업 (중소기업확인서 (중소벤처기업부))

■ 신용등급

기업신용평가등급	현금흐름등급
A+	CR-1
평가기준일	2023년 04월 14일
재무기준일	2022년 12월 31일

경영규모 (단위:백만원)	재무기준일	총자산	납입자본금	자기자본	매출액	순이익
	2022-12-31	84729	543			

■ 신용등급이력

평가기준일	재무기준일	신용등급	변동
2023-04-14	2022-12-31	A+	-
2022-04-15	2021-12-31	A+	
2021-04-19	2020-12-31	A	

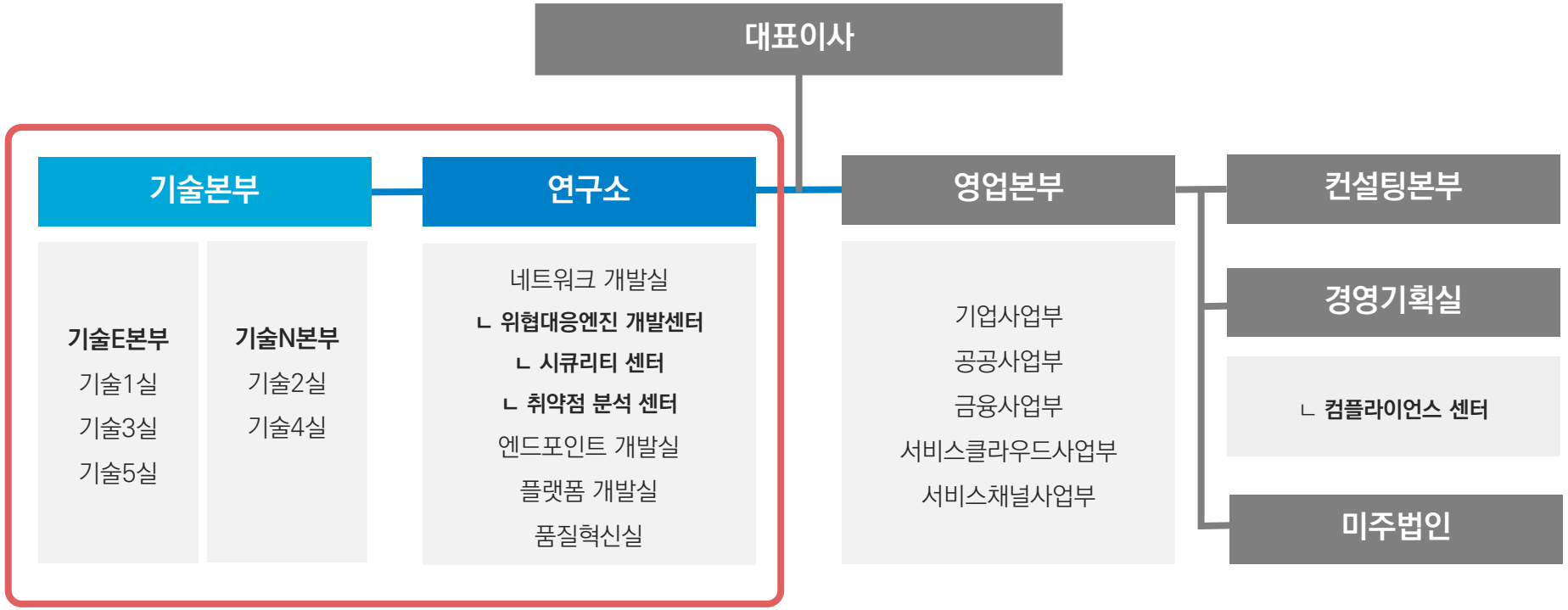
AA A BB CC D 2021-04 2022-04 2023-04

(단위: 억원)

구 분	2022년	2023년	2024년
매출액	535	577	653
영업이익	83	124	145
당기 순이익	88	140	161
차입금	0	0	0
총자산	847	1,014	1,221

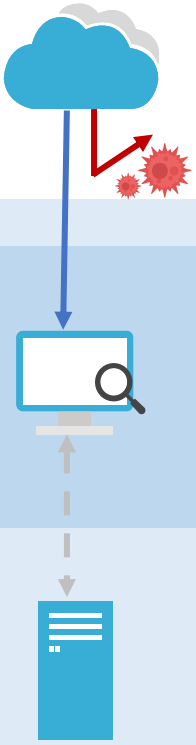
03. 조직 및 기술지원능력

- **소만사는 전체 임직원 350명 중 240여 명이 기술인력(70%)으로 재직 중입니다.**
- **데이터보호업계 최대 수준인 연구개발자 120여명, 기술엔지니어 120여명**을 바탕으로 지속적인 R&D와 서비스를 제공합니다.
- **위협대응엔진 개발센터(악성코드 분석), 시큐리티 센터(유해사이트 DB 고도화 및 업데이트), 취약점 분석센터**를 보유하고 있어 신속한 제품구축과 안정적인 기술지원을 약속 드립니다.



04. 악성코드 분석 로드맵

- 소만사는 **악성코드/랜섬웨어 차단통제(XDR)** 로드맵을 보유한 기업입니다
- 국내기업 중에는 단 두 곳만이 네트워크(NDR)부터 엔드포인트(EDR)까지 악성코드/랜섬웨어가 유입되는 모든 구간을 실시간으로 탐지/차단하고 있습니다.



WebKeeper

악성코드배포 및 유해사이트 차단

웹응답값에 포함된 악성코드, 바이러스 차단

네트워크

Privacy-i

패턴기반	행위기반	취약점 탐지대응	개인정보보호	DLP
안티 바이러스	악성코드 위협탐지 및 대응	PC 취약점 점검 탐지 대응	개인/기밀정보 자산식별 및 암호화	출력물, 매체제어 개인정보 유출차단

엔드포인트

Server-i

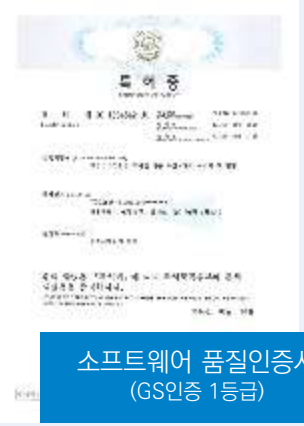
취약점 탐지대응	안티 바이러스	DLP
서버 취약점 점검 탐지 대응	서버전용 악성코드, 바이러스 차단 백신	서버 내 개인/기밀정보 유출통제

서버

05. 인증 및 지적재산권

- 국정원 CC인증, 과학기술정보통신부 GS인증을 획득한 제품입니다.
- 유해 & 악성코드 배포사이트 통제분야 핵심특허를 15건 이상 등록한 제품입니다.

보안기능확인서



소프트웨어 품질인증서
(GS인증 1등급)

CC인증
(보증등급 EAL3)

SSL,TLS 도메인 이름 수집
관리 시스템 및 방법

미러링 및 인라인 방식 부하분산
이중화 지원 어플라이언스 시스템 및 방법

P2P 및 인스턴트 메신저 네트워크
트래픽 제어방법 및 시스템

네트워크기반 고성능 유해사이트
차단 시스템 및 방법

네트워크 기반 고성능 콘텐츠
보안 시스템 및 방법

06. WebKeeper 레퍼런스

공공 시장 1위

- 1,000여개 고객사, 600여개 유지관리고객사 보유

중앙부처

지자체

06. WebKeeper 레퍼런스

공공 시장 1위

- 1,000여개 고객사, 600여개 유지관리고객사 보유

중앙부처 산하기관 & 기타기관

06. WebKeeper 레퍼런스

금융 시장 1위

- 제1금융권 및 카드, 보험, 증권사에서 구축 운용, 시장점유율 60%이상

금융기관

KB국민은행 | 신한은행 | 우리은행 | 하나은행 | Standard Chartered SC제일은행 | Sh 수협은행
광주은행 | 전북은행 | BNK 경남은행 | DGB대구은행 | 제주은행 | kakaobank
K bank | 한국은행 BANK OF KOREA | KRX 한국거래소 | 금융결제원 | SBI 저축은행 | NH저축은행
true friend 한국투자 저축은행 | NH농협생명 | 삼성카드 SAMSUNG | KB생명보험 | 한화생명 | 한화손해보험
NH농협손해보험 | 신한생명 | 롯데손해보험 | KB국민카드 | 신한카드 | 하나카드
LOTTE CARD | 비씨카드 | Hyundai Card | 신한금융지주회사 | 하나금융지주 | 농협중앙회
수협중앙회 | KB증권 | IBK기업은행 금융그룹 IBK투자증권 | 대신증권 Daishin Securities

06. WebKeeper 레퍼런스

엔터프라이즈 시장 1위

- 메이저 제조, 통신, 서비스 기업 고객사를 보유
- 산하 계열사, 해외법인에서도 운용, 지속적인 유지관리를 통한 안전웹환경 보장

엔터프라이즈

2. 도입 필요성

01. 비업무 사이트 접속 통제

02. 악성코드 배포사이트 차단

03. 암호화 웹트래픽 통제

04. 법률준수

01. 비업무사이트 접속통제

직장인 80%
업무와 무관한 인터넷 사용
일 평균 30분

업무생산성 저해 5대 소셜미디어 서비스

가상화폐/주식 거래 사이트	5,000여개
국내 주요 홈트레이딩앱	30개+
주요 도박사이트	1,000여개
게임관련 사이트	1,500여개
게임앱	30개+
네트워크 대역폭에 영향을 주는 P2P, 영상 스트리밍 사이트	70,000여개

대기업 S사 도입사례

웹키퍼 도입효과 비업무 사이트 접속차단으로 업무생산성 강화, 투자회수율 ROI 연간 300%

직원 1,000명,
월 평균 500만원 급여,
월 20일, 하루 8시간 근무 기업에서
직원 1명당 10분씩
비업무 사이트 접속시간을 줄인다면?

- 임직원 1인당 연125만원 절감
- 연간 기대 ROI 300%
- 연 생산성 12억원 향상 (월1억)
- 투자금액 4억, 생산성 강화효과 12억

02. 악성코드 배포사이트 차단

악성코드/랜섬웨어의 주 감염경로는
신뢰할 수 없는 웹사이트 접속과 E-메일내 웹 링크 클릭

국내외 랜섬웨어 감염사례

01
미 '콜로니얼 파이프라인' 송유관 마비
랜섬웨어에 감염된 PC 1대를 통해
사내 모든 네트워크에 침투하여 발생
기업 주요데이터 100GB탈취 및 남동부 지역 연료수급 중단
연방정부 지역 비상사태 선포

02
국내 웹호스팅 업체 랜섬웨어 감염
변종 에레버스(Erebus) 랜섬웨어에 서버 153대 감염
웹페이지 5천5백 여 곳 마비, 복호화 비용 약13억원 지불
기계적 문제로 2대는 복구 실패

03
악성코드 배포사이트는
국내 검색엔진에서 쉽게 접속가능한
여행사, 커뮤니티, 언론, 병원, P2P/웹하드 사이트로 구성

웹키퍼 악성코드 차단

01
연간 1천만 건 이상 악성코드 배포사이트 DB 갱신
➡ **1천 여 고객사에 설치된 사이트 리포터를 통해 클라우드 기반으로 수집**
➡ **구글, KISA를 포함한 공신력 있는 DB로 종합분석**

02
국내 유저를 타겟으로 한
악성코드 배포사이트 집중차단
➡ **음란, 도박, P2P 등 유해사이트를 통한 악성코드 유입증가로 유해사이트 분류·차단**
➡ **국내 검색엔진에서 쉽게 노출되는 악성코드 배포 웹사이트 (여행, 병원, 교육, 웹하드 등) 집중분석 및 차단**

03
30분내 수집→분석→배포 완료

03. 암호화 웹트래픽 통제

보안 사각지대

기존 미러기반 장비는 **SSL/TLS 트래픽 복호화 불가능**
유해사이트/악성코드 배포사이트 **차단정책 우회**

SSL/TLS 적용 서비스

주요 상용웹메일	Gmail, Outlook, NAVER, kakao, yahoo!
웹하드/ 클라우드	Google Drive, iCloud, MYBOX, OneDrive, Dropbox
SNS/ 엔터테인먼트	facebook, NAVER 블로그, Instagram, twitter, kakaotalk, YouTube

SSL/TLS 악용사례

facebook
twitter
Instagram

- 비공개/불법계정 (음란물, 도박, 불법공유 사이트) 접속
- 사내 개인정보/기밀정보 유출

Google

- 구글번역 우회기능을 악용한 음란물/불법사이트 접속
- 출처 불분명 메일 읽기 및 링크, 첨부파일 클릭

[단일장비에서 SSL/TLS 복호화&유해사이트 차단] **웹키퍼 가시성 확보 장비로 일반/암호화 트래픽 통제**

04. 법률준수

컴플라이언스 준수

웹키퍼는 **국정원 소관 〈국가정보보안 기본지침〉** 내
인터넷 접속통제, 비공개 업무자료 보호, 공격정보 탐지처리 준수를 위한 **〈기술적 보호조치〉 100% 충족**

국가정보보안 기본지침 (국가정보원 2023.01.31 개정)

구분	조문내용	웹키퍼 법규충족/제공기능
제47조 (인터넷 사용제한)	② 기관 인터넷망의 효율적인 운영 관리 및 **악성코드 유입 차단을 위하여 게임 · 음란 · 도박 등 업무와 관련이 없는 인터넷 이용을 차단**하여야 하며, 악성코드 유입 차단을 위하여 필요할 경우 제66조제4항에 따른 상용 정보통신서비스 접속 제한 가능	• 비업무 사이트/어플리케이션 차단 • 임직원 인터넷 접속기록 보관/검색
제66조 (비공개 업무자료 처리)	④ **정보통신서비스(전자우편 · 메신저 포함)** 또는 국외제공 유사 서비스를 이용하여 **비공개 업무자료를 작성, 저장, 수 · 발신하여서는 안됨**	• 웹메일/메신저 등 웹서비스 접속차단 • 웹메일 수신 확인 허용 / 쓰기 차단
제134조 (공격정보 탐지 · 처리)	② **사이버공격에 관한 정보를 실시간 탐지하는 장비** **[암호화된 사이버공격 패킷을 가시화(可視化)하는 장비**를 포함한다]를 보안관제 대상기관의 정보통신망에 **설치 · 운용**하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 처리	• SSL/TLS 가시성 확보 장비를 통한 유해 및 악성코드 배포사이트 탐지 통제

04. 법률준수

컴플라이언스 준수

웹키퍼는 '전자금융감독규정', '보안업무규정' 등에서 요구하는
인터넷 접속통제 **법규정 준수를 위한 〈기술적 보호조치〉 100% 충족**

전자금융감독규정 (금융위원회 2019.12.10 시행)

구분	조문내용	웹키퍼 법규충족/제공기능
제16조 (악성코드 감염 방지대책)	① 악성코드 감염을 방지하기 위하여 다음 대책을 수립·운용 1. 응용프로그램 사용시 악성코드 검색프로그램 등으로 진단/치료 후 사용 2. 악성코드 검색 및 치료프로그램은 최신상태로 유지	• 악성코드 배포사이트 및 유해사이트 DB 업데이트 체계 구축 • 유해사이트 차단 접속 차단
제17조 (홈페이지 등 공개용 웹서버 관리대책)	⑤ 금융회사 또는 전자금융업자는 **단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련**	• 비업무 사이트/어플리케이션 차단 • 임직원 인터넷 접속기록 보관/검색
제18조 (IP주소 관리대책)	3. 내부 IP주소 및 외부 IP주소의 **인터넷 접속내용을 1년 이상 별도로 기록·보관**	• 임직원 인터넷 접속기록 보관/검색

개인정보 보호조치 안내서 (보호위 2020.12 발행)

구분	조문내용	웹키퍼 법규충족/제공기능
5. 개인정보 안전조치 의무 개인정보 접근통제 조치	업무상 **P2P, 공유설정, 상용 웹메일, 웹하드, 메신저, SNS** 등은 원칙적으로 사용하지 않도록 해야 하며 반드시 필요한 경우라도 개인정보가 유노출되지 않도록 안전조치	• 웹메일 수신 확인 허용 / 쓰기 차단 • 비업무 사이트/어플리케이션 차단

3. 기능소개

01. 강점

명시적 프록시 인라인 프록시 모두 지원

대규모 엔터프라이즈
네트워크에서는
명시적 프록시 방식
우선 적용

국내 최대 DB 수집 분석 배포 인프라

AI인공지능 자동화 분석 및
1천 여 웹키퍼 고객사를 통해
실시간 축적되는
데이터 인프라

성능과 안정성 입증

외산 SWG와의 BMT 4회 승리
기술력을 인정받아
국내 4대 대기업에서
모두 운영 중 (국내유일)

ChatGPT 생성형 AI서비스 차단

보안성(개인정보유출),
윤리성(저작권위반)을 저해하는
생성형 AI 서비스
카테고리 분류 및 접속차단

01. 강점

명시적/인라인 2개 방식 구축지원

Secure web gateway 네트워크 구성도 및 특징

명시적 프록시 (Explicit Proxy)

명시적 프록시

- ✓ 사용자 요청이 Proxy로 전달되도록 브라우저에서 명시적 설정(PAC)
- ✓ 방화벽에서 Proxy를 거치지 않은 웹트래픽은 차단 설정

장점

- ✓ 웹프락시 장애발생시에도 네트워크 전체 단절 없음
- ✓ SPOF(Single Point Of Failure) 네트워크 장애 위험요소 낮음

단점

- ✓ 웹Proxy 설정이 불가능한 특정개발 App의 경우, 통신중계 불가

인라인 프록시 (In-Line Proxy)

인라인 프록시

- ✓ OS레지스트리에 CA목록에 추가작업 필요 , 모든 트래픽 처리 가능

장점

- ✓ PC 브라우저 프록시 설정 불필요
- ✓ 방화벽 설정 불필요

단점

- ✓ SPOF(Single Point Of Failure) 네트워크 장애위험요소 높음

01. 강점

명시적 프록시
인라인 프록시

네트워크 구성안 및 특징

항목	명시적 프록시	인라인 프록시
장애 발생시 네트워크 전체 중단 위험	낮음	상대적으로 높음
장애 발생시 네트워크 전체 지연 위험	낮음	상대적으로 높음
이중화, 비대칭 등 복잡한 네트워크 환경에서의 설치운영 편리성	높음	상대적으로 복잡
정책에 따른 유해사이트 접속차단	○	○
정책에 따른 악성코드 접속차단	○	○
브라우저 Proxy 설정	필요	불필요
방화벽에서 Proxy 이외 트래픽 차단설정	필요	불필요

대규모 엔터프라이즈 네트워크에서는 명시적 프록시 방식 우선 적용
네트워크 트래픽 양이 적은 중소규모 네트워크에서는 인라인 프록시 방식 적용 용이

01. 강점

국내 최대 DB 수집, 분석, 배포 인프라

1천 여 웹키퍼 고객사를 통해 방대하게 축적되는 웹 데이터, AI 분석기술로 실시간 업데이트되는 국내 최대 DB인프라

수집

사이트 리포터
1,000여개 국내 고객사에서
미분류 접속 사이트 자동수집

시큐랩닷컴
보안담당자 미분류 사이트 직접신고

키사이트 콜렉터
검색엔진 키워드별 검색결과 자동분류

분석

AI 인공지능기반 자동 분석센터
웹사이트 내 이미지, 텍스트를 추출하여
비업무, 유해, 불법, 음란사이트 여부를 자동 판단

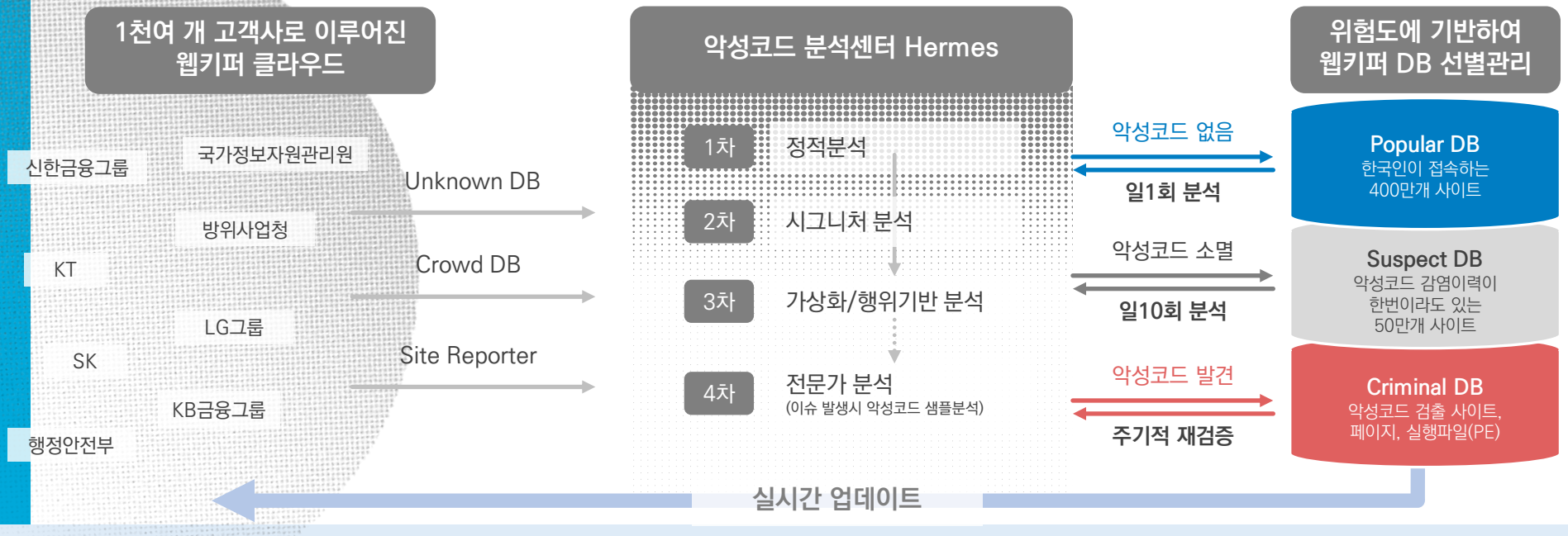
Google, KISA 등 DB 분석
공신력 있는 기관 제공 악성코드DB 3종 이상 보유

전문가로 구성된 자체 분석센터
1~4차 분석프로세스 제공,
피해규모가 큰 악성코드/랜섬웨어는 상세리포트 제공

배포

30분 이내 배포
수집-분석-배포까지
30분 이내

주기적 재검증
24시간
DB 최신화 작업수행



01. 강점

국내 최대 DB 수집, 분석, 배포 인프라

유해사이트 차단분야
14년 연속 보안성 지속 서비스 제공

일간, 월간, 연간 업데이트 내역 공시 및 자료 발간 (국내유일)

웹키퍼의 정교하고 신속한 DB 수집, 분석, 배포 인프라를 증빙하는 연간 리포트 매년 발행

DB 업데이트

데일리 카톡

월간 리포트

연간 리포트

악성코드/랜섬웨어 분석

월간 악성코드 리포트

연간 악성코드 리포트

01. 강점

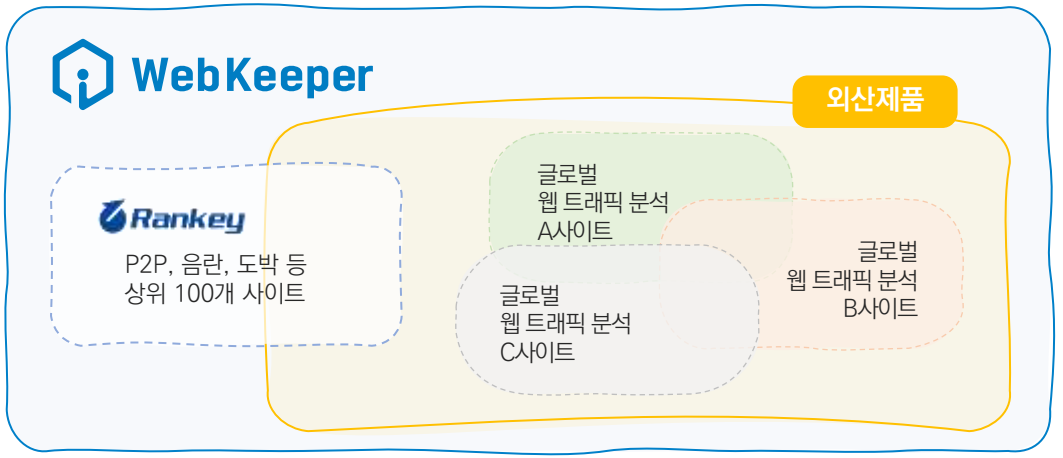
국내 최대 DB 수집, 분석, 배포 인프라

외산대비 50% 이상 정확한 DB분류체계 수립 구축

평판 사이트 상위 100개 사이트 모두 차단

- 외산은 한국사이트의 순위를 측정하는 랭키닷컴 상위 사이트 차단에 취약
- 웹키퍼는 랭키닷컴 뿐만 아니라 글로벌 상위 사이트 모두 100% 차단

분류대상	외산제품	웹키퍼
글로벌 웹 분석사이트	100%	100%
랭키닷컴	40%	



한국 인터넷 접속에 특화된 웹 카테고리 생성관리

외산 카테고리 중 일부: 자국 특성에 맞추어 제공하는 카테고리는 국내 정서와 부적합

- 마약 (illegal drugs)
- 영성/주술 (altrntive spirituality/occult)
- 대마 (marijuana)
- 안락사 (euthanasia)
- 주류/담배 (Alcohol/Tobacco)
- 입양 (adoption)

담당자의 수작업을 통한 블랙리스트 추가조치 없이
솔루션에서 실시간 제공되는 웹DB가
자동으로 사내 업데이트 서버에 반영되어야 함

분류대상	외산제품	웹키퍼
가상화폐	별도 카테고리 없음	별도 카테고리 보유
카카오서비스	수십개 서비스를 단일 카테고리로 분류	서비스별로 각각의 카테고리로 분류
불법웹툰	별도 카테고리 없음	별도 카테고리 있음

01. 강점

국내 최대 DB 수집, 분석, 배포 인프라

AI 인공지능기반 자동분석 및 분류시스템 구축
보안담당자 개입없이 유해/비업무 사이트 분류 및 업데이트

이미지 기반 자동분류

AI기반 분석 시스템이 웹사이트 내 이미지를 기반으로
음란사이트 여부 자동판단 및 30분 이내 분류

텍스트 기반 자동분류

생성형 AI기반 파운데이션 모델을 통해 웹사이트 내 텍스트 추출,
비업무/유해/음란사이트 자동판단 및 30분 이내 분류

웹사이트 URL을 입력하여
- **음란DB 등록여부 확인**
- **이미지 기반으로 사이트 카테고리 분석**
- **미등록시 30분 이내 업데이트**

웹사이트 URL을 입력하여
- **DB 등록여부 확인**
- **텍스트 기반으로 사이트 카테고리 분석**
- **미등록시 30분 이내 업데이트**

30분 이내 업데이트
- 동일 URL 접속 차단
- WebKeeper DB에 분류되어 1천여 고객사 DB서버에 업데이트

01. 강점

외산 대비 성능과 안정성 입증

외산 제품과 Secure Web Gateway BMT에서 4회 이상 승리
웹프락시 분야는 소만사 기술력으로 100% 외산 대체 가능

SAMSUNG LG SK HYUNDAI MOTOR GROUP

01. 강점

ChatGPT 통제 및 기록

IT 신기술 부작용 최소화 하도록 ChatGPT 접속 차단 및 통제

ChatGPT 긍정적 측면 : **업무 생산성 향상**

의료	영상판독, 임상질환 합성데이터 생성, 신약후보물질 발굴 등
마케팅	카피라이팅, 홍보콘텐츠 생성, 고객지원 서비스 등
금융	고객상담, 상품추천, 신용평가, 금융사고 감지 등
법률	법률대리인 서류작업 지원, 판사업무 보조 등

VS

ChatGPT 부정적 측면 : **기업 리스크 발생**

정확성	사실여부 검증과정 없음, 가짜정보 무분별하게 생산
실시간성	학습데이터 외 최신정보 반영불가
보안성	개인/기밀정보 유출위험 및 정보가공, 저작권 문제
윤리성	가치판단 문제에 있어 사이버공격/범죄 연루

별도 카테고리 보유하여 접속차단 또는 접속 허용하되 사용내역은 모두 로그저장

생성형 인공지능

- 생성형 AI기반 파운데이션 모델을 이용하여 사용자와의 대화를 통해 새로운 데이터를 생성해내는 웹서비스(웹사이트)
- 생성형 AI를 유용하게 활용할 경우 생산성이 강화될 수 있음.
- 그러나 개인정보유출, 저작권침해, 가치판단 문제 등 기업 경영관리에 부정적 측면도 존재하므로 금융/제조/교육기관 등은 생성형 AI 서비스를 차단하고 있음

Chat GPT, Gemini, CLOVA X 등
국내외 생성형 AI 서비스는
모두 카테고리 분류되어 접속차단

02. 기능

유해사이트 차단: 랜섬웨어 감염 리스크 최소화

- 음란, 도박, 불법정보, 저작권 침해사이트 차단
- 악성코드 배포사이트 접속 차단
- 구글 번역기 등 우회 사이트 접속 차단
- 웹응답값에 포함된 악성코드, 바이러스 차단

비업무사이트 차단: 업무환경 개선 생산성 확보

- 증권 웹트레이딩(WTS) 거래차단, 기타 서비스 허용
- 기타 금융서비스(가상화폐거래소 등) 차단
- SNS, 커뮤니티, 인터넷 방송, 동영상 서비스 등 차단
- 상용 웹메일/블로그 읽기 허용, 쓰기 차단
- 구글서비스 선별 차단 (검색 허용, 드라이브 차단 등)
- Tor, 젠메이트 등 우회접속앱 차단
- 토렌트/웹하드/클라우드앱 차단
- 금융 메신저(코스콤, 미스리) 및 상용 메신저(카카오톡, 라인, 네이트온) 차단
- 국내외 온라인게임(리그오브레전드, 서든어택, 배틀그라운드, 리니지 등) 차단
- PC원격제어(팀뷰어, MS원격데스크톱 등) 차단

관리/리포트

- 사용자, 시간대, 웹카테고리에 따른 접속차단 정책적용
- 요약 및 상세 분석 (드릴다운 검색)
- 자동 리포팅

02. 기능

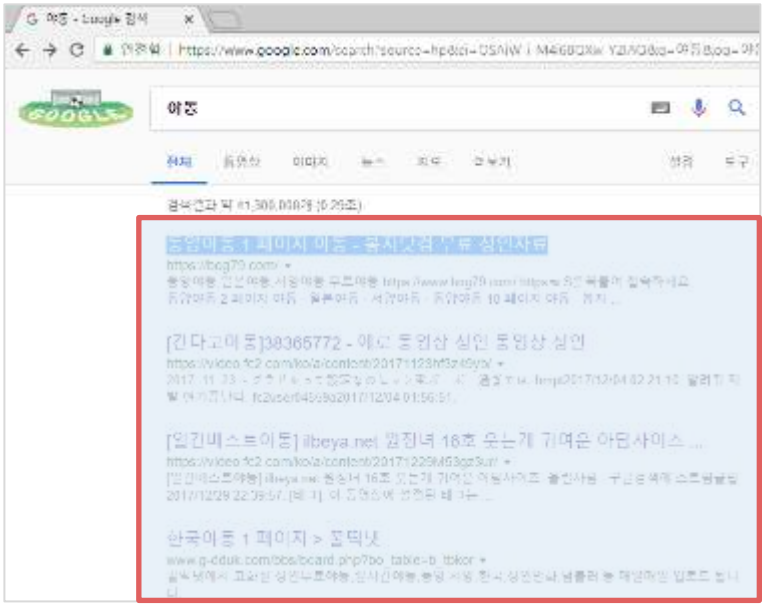
⊖ 유해사이트 차단

음란, 도박, 불법정보, 저작권 침해, 가상화폐거래 사이트 차단

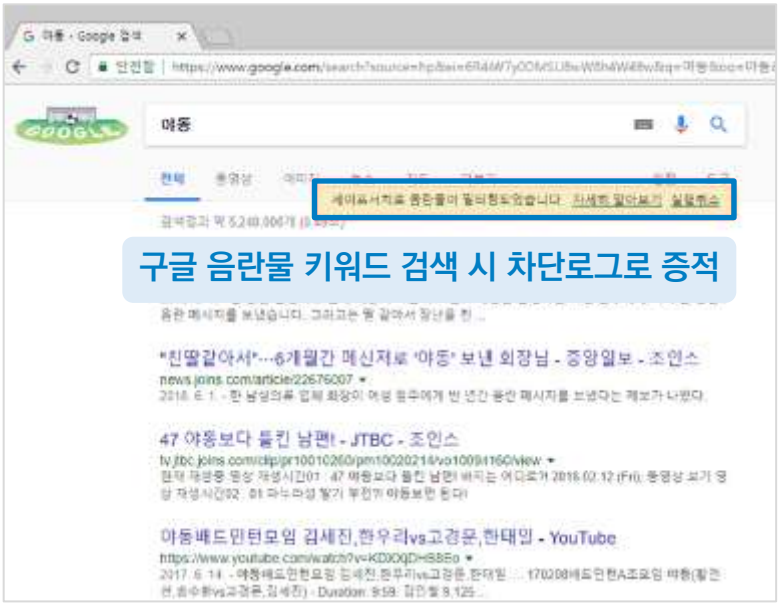
구글 세이프 서치 (검색 필터링) 강제화

· 웹키퍼 적용 환경에서는 성인인증 완료 후에도 세이프 서치 강제 활성화
· 음란물, 도박, 유해 컨텐츠 검색불가 접근차단

성인인증시 세이프 서치 기능 해제
음란물 컨텐츠 접근 원활



WebKeeper 세이프 서치 적용:
성인인증 후에도 음란물 컨텐츠 검색불가

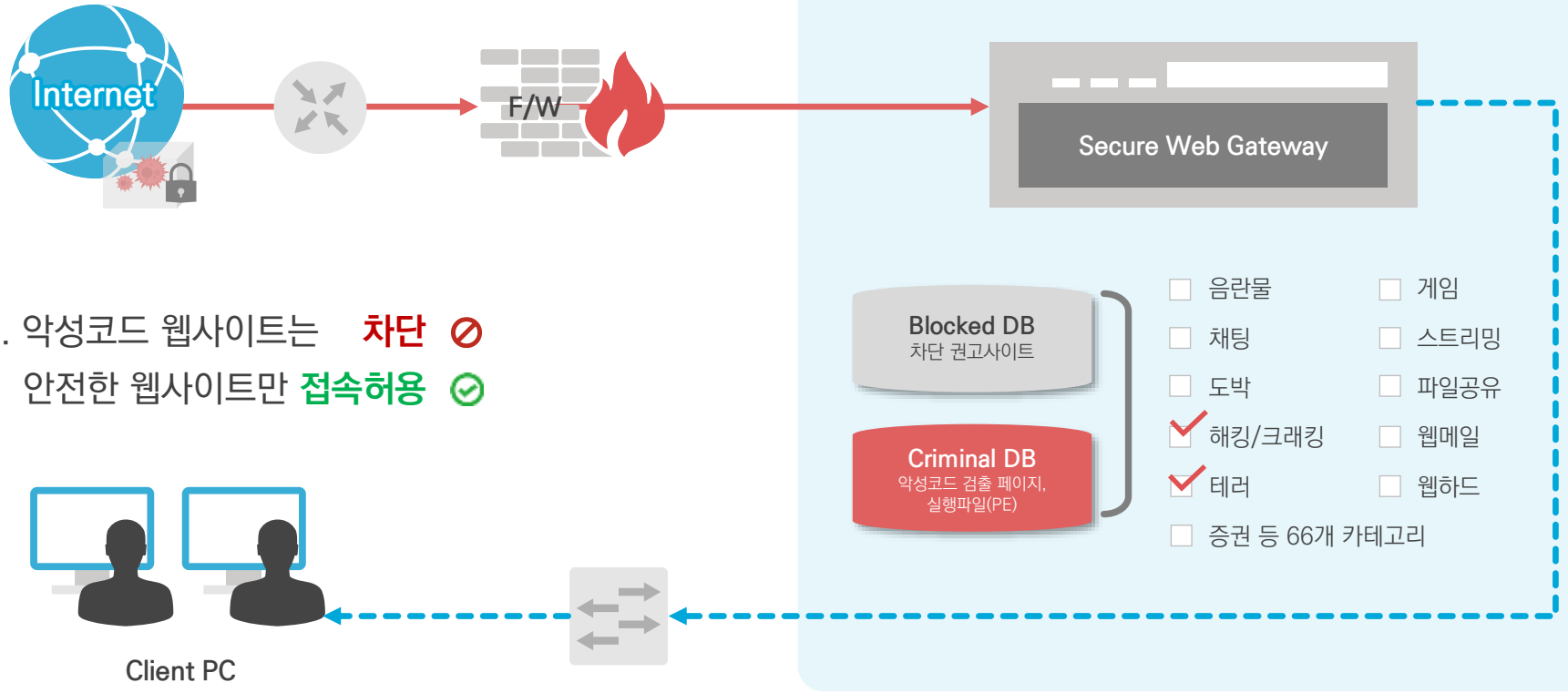


02. 기능

⊖ 유해사이트 차단 악성코드 배포사이트 접속 차단

1. 사내임직원 PC에서 웹사이트 접속

2. 웹사이트 데이터베이스와 대조하여
허용/차단여부 결정



3. 악성코드 웹사이트는 **차단** ⊘
안전한 웹사이트만 **접속허용** ✓

02. 기능

⊖ 유해사이트 차단

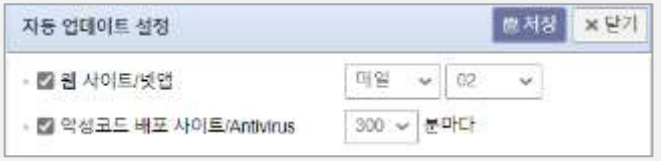
웹 응답값에 포함된 악성코드, 바이러스 차단

* 명시적 프록시 방식일 경우 적용

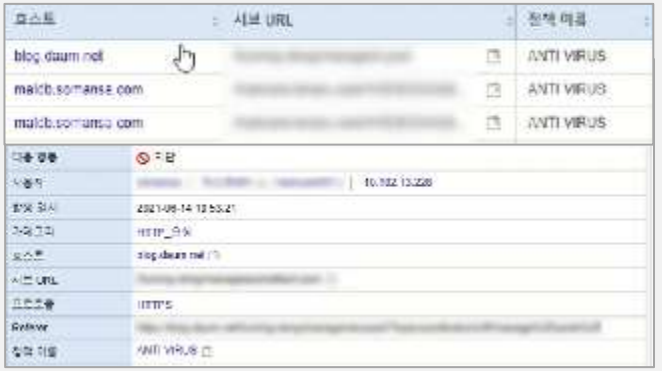
1차: URL 대조
기존 WebKeeper DB와
접속 URL을 대조하여
정책허용 여부 확인

2차: 웹 응답값 대조
시그니처 기반
안티 바이러스 엔진 탑재
웹 응답값 내 포함된
악성코드, 바이러스를 탐지하여
허용여부 결정

안티바이러스 엔진 탑재 및 업데이트 시스템 구축



주기적인 업데이트를 통해
신종/변종 바이러스 차단



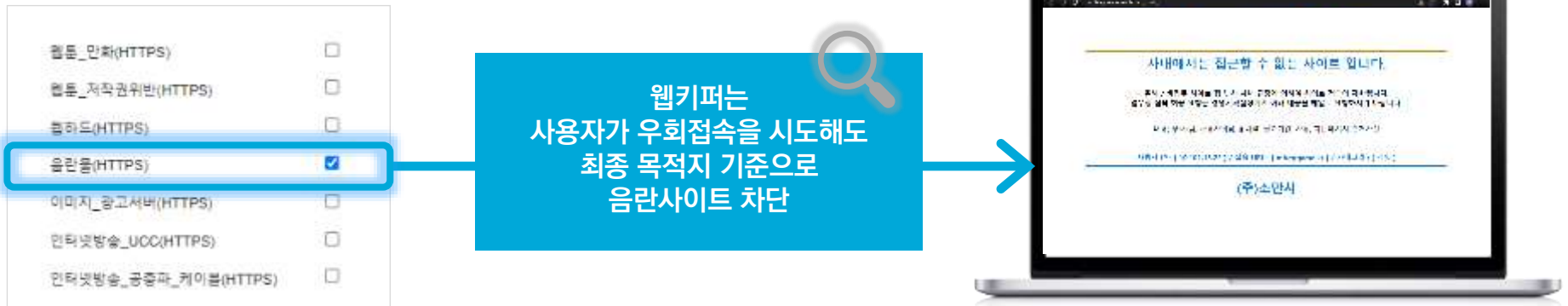
차단과 동시에 차단내역은 로그저장
이를 통해 통계자료 활용 및 보안대책 수립가능

02. 기능

⊖ 유해사이트 차단 — 구글 번역기 등 우회 사이트 접속 차단

- 프록시 서비스를 통해 유해사이트에 우회접속 시도하는 경우 차단
- WebKeeper는 최종 접속지를 기준으로 차단/허용 여부를 결정

웹페이지 기준 차단 설정



02. 기능

⊖ 유해사이트 차단 HTTP Header 기반 접속통제

- URL, 메소드, HTTP 버전, 요청/응답 헤더(호스트, 언어, 클라이언트 정보, 리퍼러, 메시지 길이 등) 기반으로 전송 차단

리퍼러 기반 통제

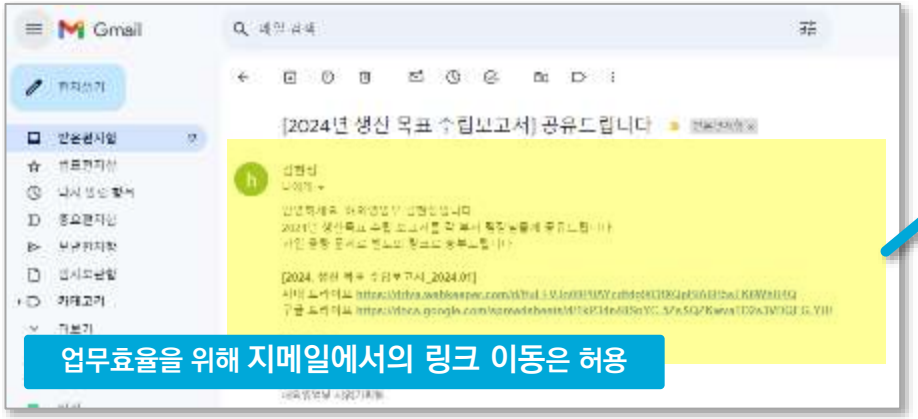
악성코드 감염예방을 위해 웹메일에 포함된
URL 접속은 모두 차단하나 업무효율을 위해
특정 웹메일(ex: 지메일)만 허용하고 싶은 경우

업무효율 및 생산성 향상을 위해
'클라우드 협업 서비스'를 사용하고 있는 경우
해당 웹메일 서비스에 한하여서는 링크이동 가능

메소드 기반 통제

내부 임직원의
기업 웹서버 이상 접속, 무단 조회, 리소스 변경행위 등
데이터 유출, 변조, 파괴 행위를 차단하고 싶은 경우

클라이언트-서버 간 전송되는 요청 메시지에서
웹서버 내 중요 리소스를 일부변경(Patch) 하거나
삭제(Delete) 행위를 수행하는 메소드는 탐지 및 차단



02. 기능

비업무사이트 차단

증권 웹트레이딩(WTS) 거래 차단, 기타 서비스 허용

국내 증권사 WTS 상위 30개 차단

삼성증권 · 한국투자증권 · 하나대투증권 · 현대증권 · 신한금융투자 · 미래에셋증권 · IBK투자증권 · NH투자증권 · KB증권 · KYOBO 교보증권 · 한화투자증권 · DB금융투자 · 유진투자증권 · 케이프투자증권 · 현대차증권 · 유안타증권 · 키움증권 · meritz 메리츠증권 · BEST · 토스증권 · pay 증권 · 대신증권 · 신영증권 · 부국증권 · LEADING · SK 증권 · ktb 투자증권 · 하이투자증권 · IM 아이엠투자증권 · 한양증권

OO증권 WTS 거래 차단

실시간 WTS 접속차단 및 로그기록

증권서비스 접속시 차단 및 기록
(일시, 부서, 접속자, ID, IP 등)

02. 기능

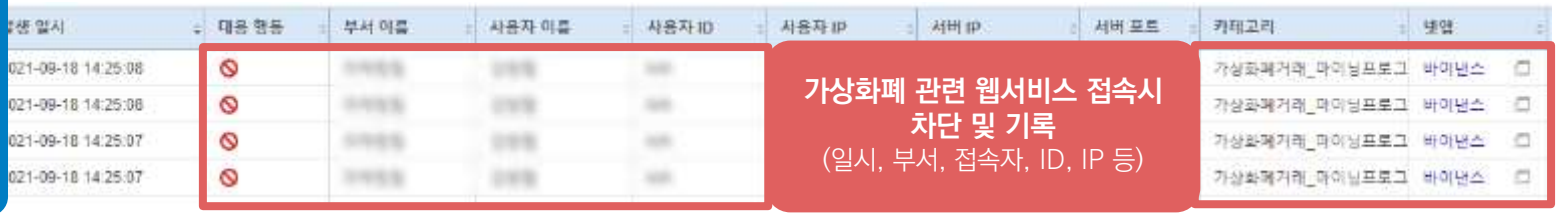
비업무사이트 차단 — 가상화폐 거래소 접속 차단

국내 가상화폐 투자자 587만명, 127兆 넣었다 105兆 뺐다

윤진호 기자 2021.05.27

국내 가상 화폐 투자자가 587만3000명으로 집계됐다. 올 들어 420만명 넘게 늘었다. 가상 화폐 투자 광풍(狂風)이 불었다고 할 정도인 지난달에만 191만명이 늘었다. 투자금액은 127조7000억원이 가상 화폐 거래소에 입금됐다가 그동안 105조원이 출금됐다. 587만명이 여전히 투자하고 있다고 가정하면 1인당 387만원을 투자하고 있는 셈이다.

가상화폐거래소 실시간 접속차단 및 로그기록



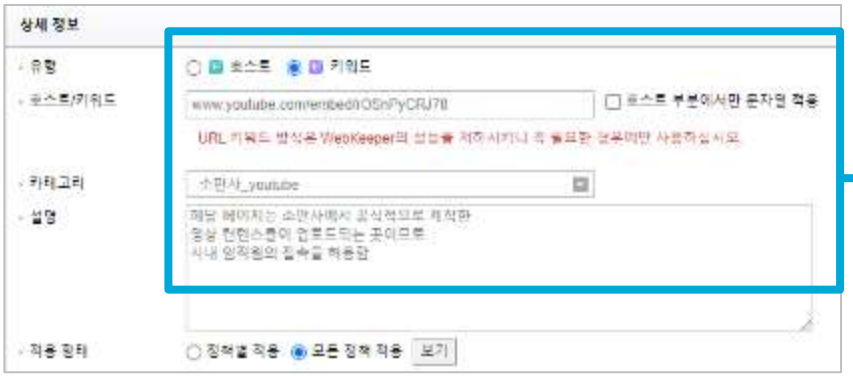
가상화폐 관련 웹서비스 접속시 차단 및 기록
(일시, 부서, 접속자, ID, IP 등)

02. 기능

비업무사이트 차단 SNS, 인터넷 방송, 동영상 서비스 등 선별 차단

- 업무와 연관 없는 웹서비스는 기본적으로 모두 차단됨
- 단, 회사 SNS 채널 등 자사업무와 연관성 있는 페이지는 허용하고 나머지 페이지는 차단

유튜브 사내 보안지침에 따라 사내 공식 SNS 페이지는 허용



접속

발생 일시	대응 행동	부서 이름	사용자 이름	사용자 ID	카테고리	호스트
2022-01-04 14:04:39	○				소만사_youtube	www.youtube.com
2022-01-04 17:20:40	○				소만사_youtube	www.youtube.com
2022-01-04 13:54:52	○				소만사_youtube	www.youtube.com
2022-01-06 11:50:21	○				소만사_youtube	www.youtube.com
2022-01-20 09:54:32	○				소만사_youtube	www.youtube.com

접속기록은
로그저장

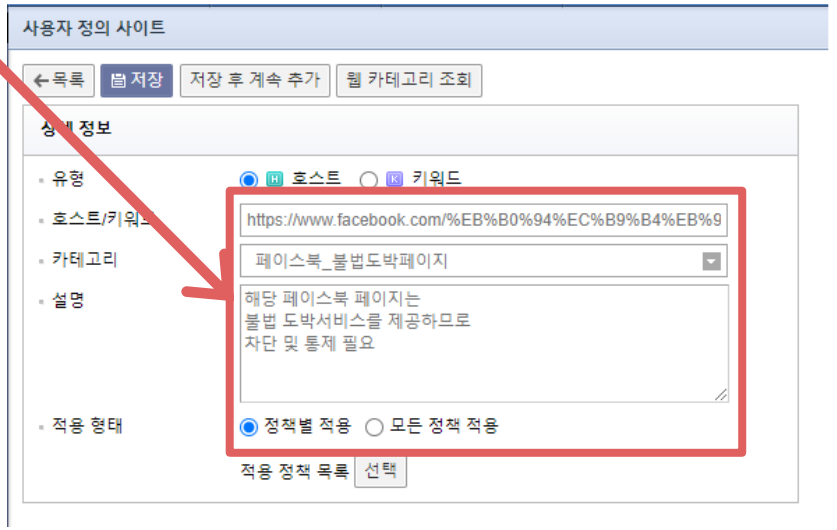
02. 기능

비업무사이트 차단 SNS, 인터넷 방송, 동영상 서비스 등 선별 차단

- 업무와 연관 없는 웹서비스는 기본적으로 모두 차단됨
- 단, 회사 SNS 채널 등 자사업무와 연관성 있는 페이지는 허용하고 나머지 페이지는 차단

페이스북 사내 보안 지침에 따라 불법도박 페이지는 차단하고 나머지는 허용

URL 호스트 추가로
도박 계정 접속 차단



02. 기능

비업무사이트 차단 상용 웹메일/블로그 읽기 허용, 쓰기 차단

- 암호화웹(SSL/TLS, HTTPS)를 사용하는 상용 웹메일을 허용할 경우
  [읽기 허용], [보내기 차단] 설정하여 수발신 관리

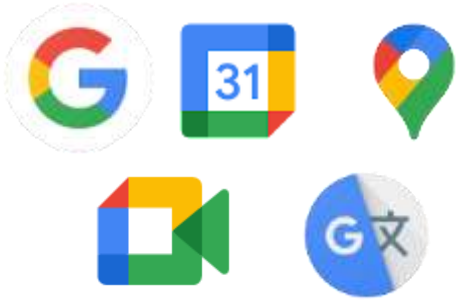
	대응 행동	부서 이름	사용자 이름	사용자 ID	카테고리	호스트
4 19:20:51	○	마케팅팀	김현정	hjkim	메일_주요웹메일읽기	mail.google.com
4 19:28:03	⊘	마케팅팀	김현정	hjkim	메일_주요웹메일쓰기	mail.google.com

02. 기능

비업무사이트 차단

구글서비스 선별 차단 (검색 허용, 드라이브 차단 등)

업무와 연관된 서비스는 허용

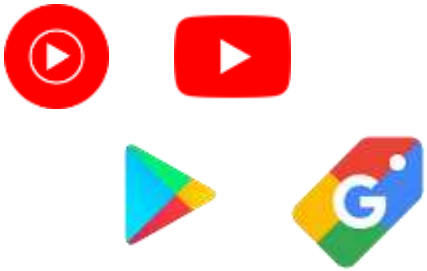


GoogleSearch	접근	○
	이미지검색	○
	뉴스검색	○
	비디오검색	○
Google Hangouts	접근	○
	업로드	○
	대화하기	○

악성코드감염 & 개인정보유출 위험이 높은 서비스는 차단

Gmail	접근	ⓘ
	다운로드	ⓘ
	보내기	⊘
	첨부하기	ⓘ
	읽기	○
Google Drive	접근	ⓘ
	업로드	⊘
	다운로드	⊘
	공유하기	⊘
	편집하기	○
	읽기	○

생산성을 저하하는 비업무 서비스는 차단



YouTube	접근	⊘
	업로드	⊘
	보내기	⊘
	게시하기	⊘
	재생하기	⊘
	비디오검색	⊘

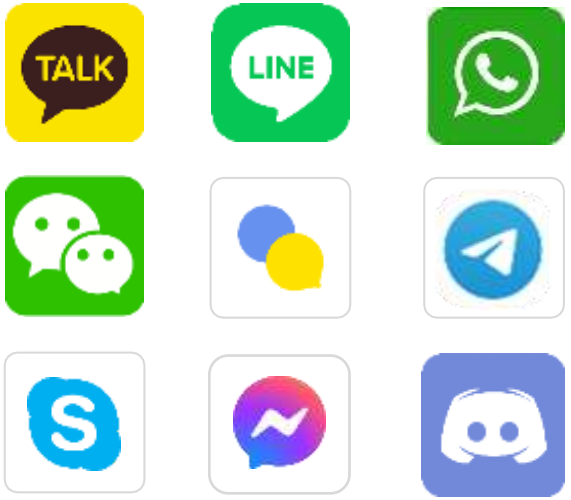
* 해당 차단 정책은 기본설정이며
회사지침에 따라 세부설정 가능

02. 기능

비업무사이트 차단 — 금융 및 상용 메신저차단

- 금융 메신저(미스리 메신저, 체크 메신저 등), 상용 메신저(카카오톡, 라인, 네이트온 등), 무설치 웹메신저 차단
- 업무용 메신저 (슬랙, 하이웍스, 밋톡, 공공/금융/기업 자체개발 메신저 등) 감사로그 저장 및 사후분석

주요 인스턴트 상용 메신저 실행차단



주요 금융 메신저 실행차단

업무용 메신저 감사로그 저장

02. 기능

관리/리포트

사용자, 시간대, 웹카테고리에 따른 접속차단 정책적용

사용자

- ✓ 부서, 직급, 담당업무에 따라
  웹 서비스 세부차단
- ✓ 재무팀은 업무와 연관된 증권매매,
  증권사 사이트 접속 허용 (이외 부서는 금지)

시간대

- ✓ 비업무 사이트의 경우
  업무시간 내에는 차단, 이외에는 허용
- ✓ 사내트래픽 사용현황에 따라
  특정 시간대 웹접속 Bypass 또는 차단

웹 카테고리

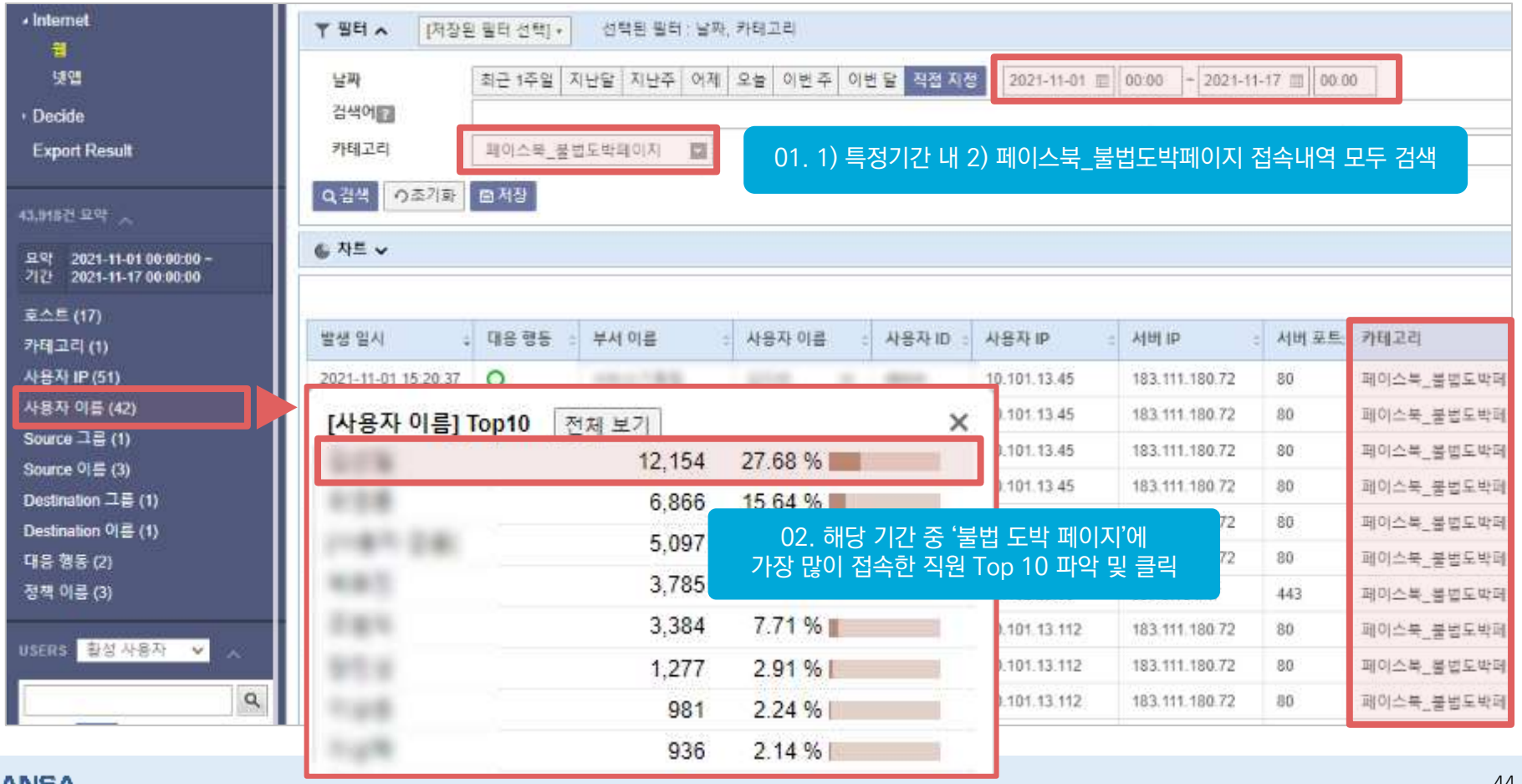
- ✓ 웹 카테고리 60개, 넷앱스 카테고리 27개 분류
- ✓ 웹메일의 경우 읽기는 허용, 쓰기는 차단하여
  금융감독원 〈내부통제 모범규준〉 준수

02. 기능

관리/리포트

요약 및 상세 분석 (드릴다운 검색)

- 특정 기간 내, 근무시간에 '페이스북 불법 도박 페이지'에 가장 많이 접속한 직원을 찾아서 보고하기

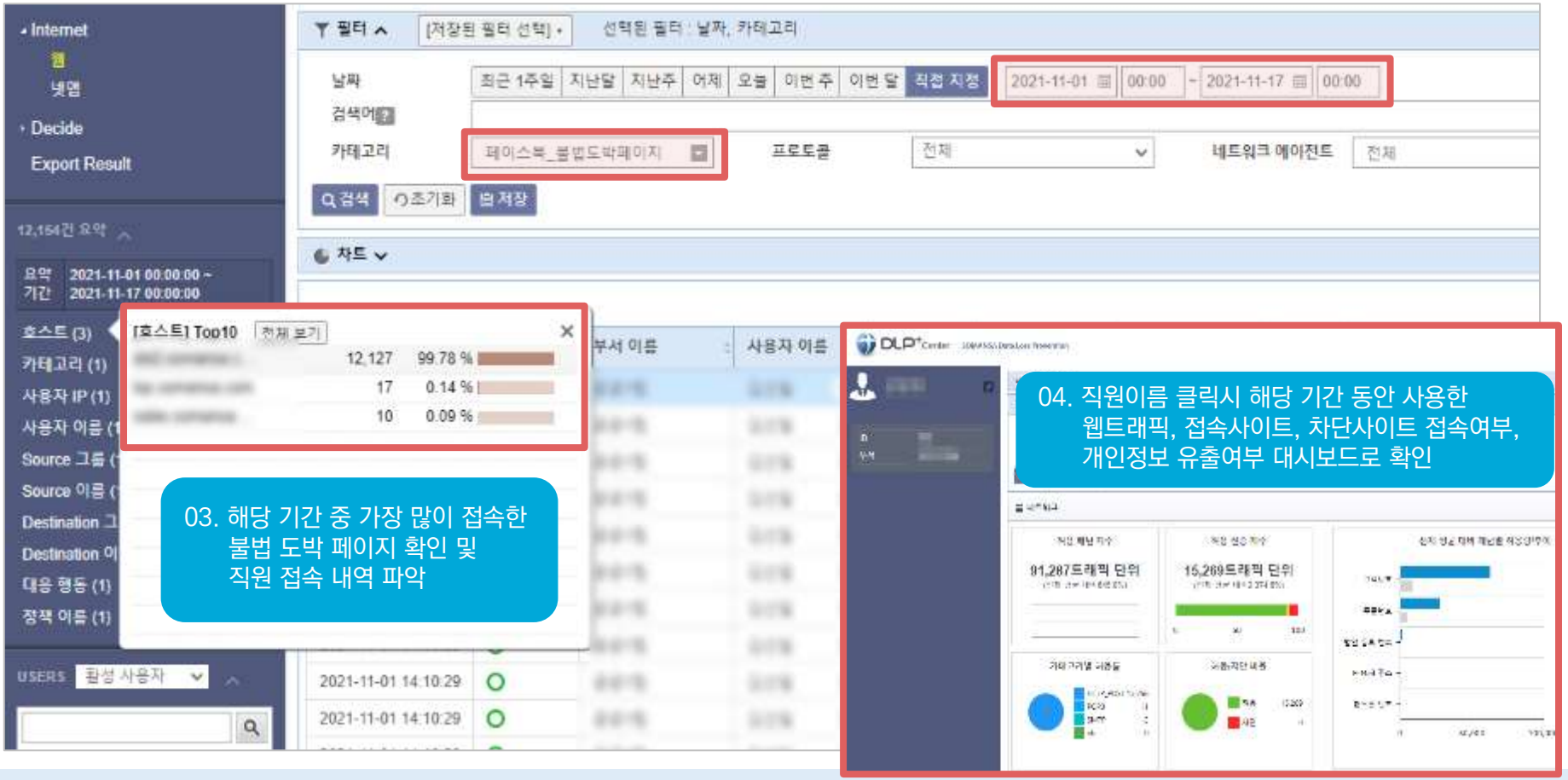


02. 기능

관리/리포트

요약 및 상세 분석 (드릴다운 검색)

- 특정 기간 내, 근무시간에 '페이스북 불법 도박 페이지'에 가장 많이 접속한 직원을 찾아서 보고하기

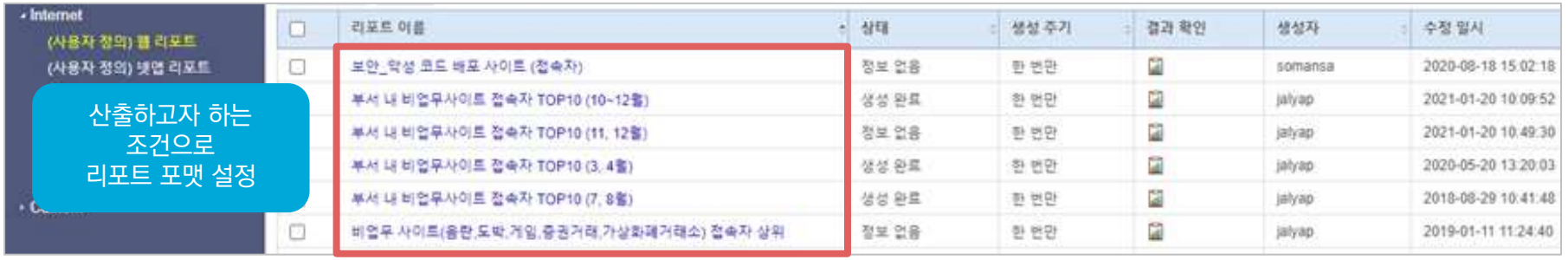


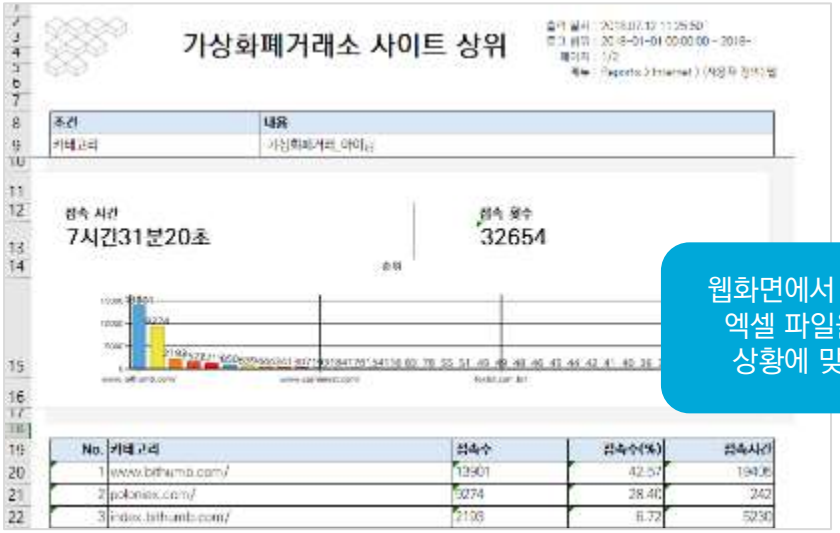
02. 기능

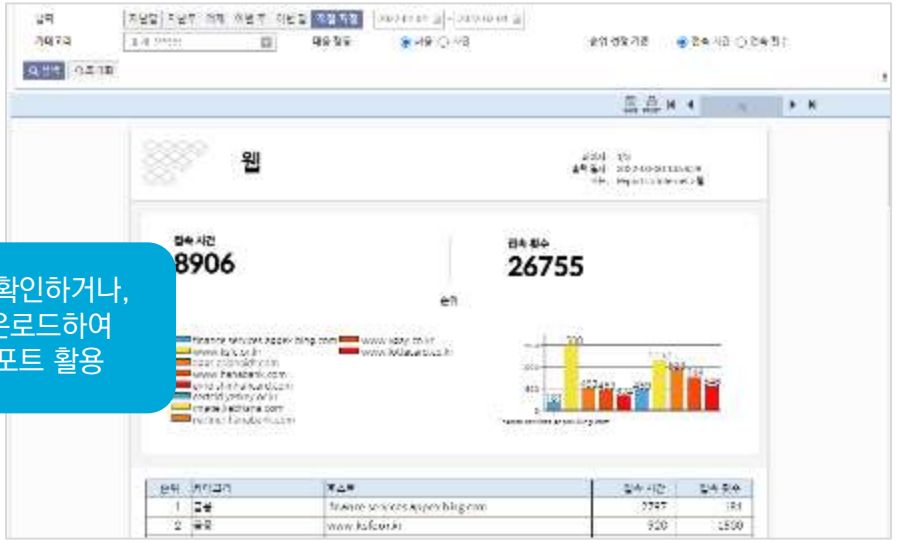
관리/리포트

자동 리포팅 및 문서산출

- 예약시간(매주, 매월, 분기별)에 통계데이터 자동산출 및 저장







웹화면에서 바로 확인하거나,
엑셀 파일을 다운로드하여
상황에 맞게 리포트 활용

4. 제품 비교표

제품비교표

항목		소만사 웹키퍼	S사 E제품	비고
ChatGPT 차단	ChatGPT 접속이력, 대화내용, 이용자, 날짜, 전송허용/차단여부 기록 및 저장	O	X	
	대화진행시 개인정보/기밀정보 포함여부 확인하여 오남용 발생시 경보 및 차단	O	X	
	ChatGPT 이외 생성형 AI서비스 카테고리 분류 및 차단	O	O	
유해사이트 DB 양과 품질 (Quantity& Quality)	연간 1천만 건 이상 **유해/악성 DB 업데이트** 여부	O	△	소만사는 매년 1천만 건 이상 차단
	AI 인공지능 기반 웹사이트 자동분류 시스템 적용여부	O	X	소만사는 웹사이트 이미지, 텍스트 기반 유해/음란/비업무 여부 자동판단
	30분 단위 DB 업데이트, 긴급/민감 이슈 발생시 **실시간 업데이트** 여부	O	△	
차단 커버리지	**평문/암호화 통신** 비업무·악성코드배포 사이트 모두 지원	O	O	
	가상화폐 거래 사이트 차단 / 증권거래 사이트 차단	O	O	
	웹 응답에 포함된 **악성코드·바이러스 차단**	O	X	명시적 프록시 방식에서만 지원
	HTTP Header 기준으로 웹사이트 **접속차단**	O	X	
악성코드 차단 연계	악성코드 차단 Endpoint EDR 솔루션 연계	O	X	
	네트워크 및 엔드포인트 악성코드 차단 XDR 로드맵	O	X	
보안 지속성 서비스	**악성코드/랜섬웨어 분석보고서** 월1회 발간	O	X	
	일간·월간·연간 DB 업데이트 목록제공	O	△	
사용자 편의성	2-Factor 인증 로그인 지원	O	O	
	사용자 웹접속 분석 대시보드 제공	O	O	

5. 프로젝트 관리 및 교육

01. 기술평가등급 T2

02. 프로젝트 수행

03. 기술지원 및 정기적 서비스

01. 기술평가등급 T2

- 기술평가등급 T2 → 기술력 상위 1% 이내
- 200여명 기술인력 보유
- 인프라 구축부터 유지관리까지 단일 벤더에서 일괄지원대응

기업체명	(주)소만사
대표자명	김대환
사업자등록번호	214-86-14882
법인등록번호	110111-1394115
본사주소	(07228) 서울 영등포구 영신로 220 (영등포동8가)
산업분류	[J58222] 응용 소프트웨어 개발 및 공급업
유효기한	2024년 08월 08일
제출처 및 용도	적격심사 및 공공기관 제출용

기술평가등급

T2

평 가 일	2023년 08월 09일

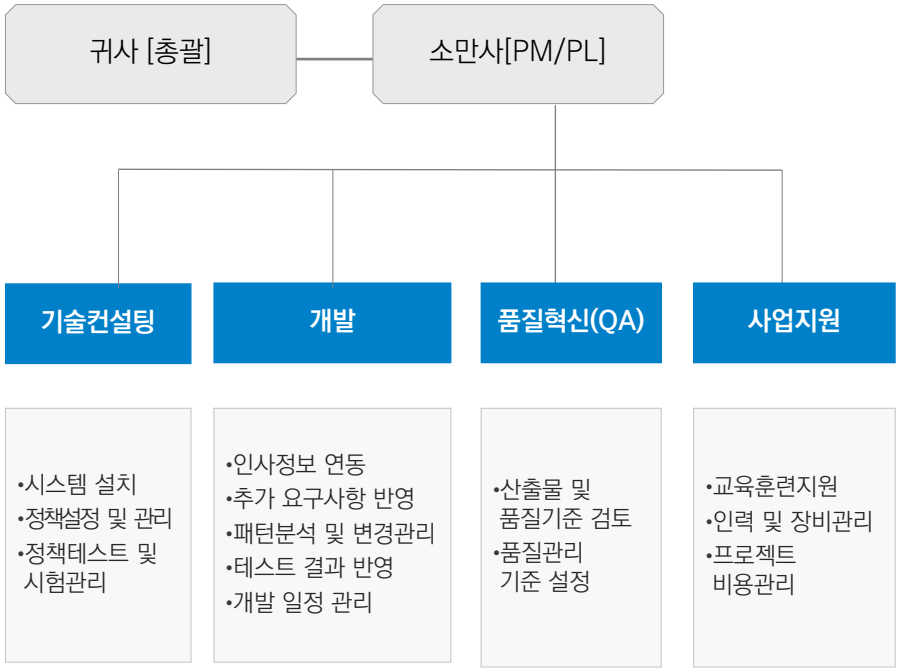
기술평가등급	매우취약	취약	미흡	보통이하	보통			보통이상			양호			우수			매우우수	최우수
	T10	T9	T8	T7	T6-	T6	T6+	T5-	T5	T5+	T4-	T4	T4+	T3-	T3	T3+	T2	T1
	기술력이 매우 우수한 수준으로 산업 및 시장환경의 급격한 변화에도 어느 정도 대응능력을 갖추고 있어 안정적임																	

02. 프로젝트 수행

성공적 사업수행을 위해 계약부터 완료까지 귀사와 유기적 관계를 유지할 수 있는 조직을 구성합니다.
완벽한 산출물이 생성되도록 품질혁신실의 지원을 받아 원활하고 효율적인 프로젝트 수행이 가능합니다.
프로젝트 관리자가 전체 프로젝트를 효율적으로 관리할 수 있도록 조직을 구성합니다.

인력확보 방안 및 인적 구성의 적정성

〈 수행 조직 〉



〈 업무분장 〉

조직	역할
귀사	▪ 계약체결, 사업관리 및 사업비 신청내역 확인 ▪ 검사 및 인수, 사후관리 ▪ OOO에서 담당할 필요가 있는 세부적인 업무
소만사 (PM)	▪ 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 품질보증, 투입인력, 자원 및 예산 관리 ▪ 주요 이해당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
소만사 (PL)	▪ 기술적인 프로젝트 총괄 진행, 프로젝트 추진활동 계획 조정 및 감독 ▪ 기술적인 품질보증, 투입인력, 자원 및 예산 관리 ▪ 기술 당사자와 의사소통 채널 및 긴밀한 관계 유지 ▪ 프로젝트 보고 및 산출물의 인도
기술컨설팅	▪ 시스템 설치 및 구축(하드웨어, 소프트웨어 - 운영체제, 로그서버 등) ▪ 정책설정, 관리 및 운영 지원 / 주요 산출물 작성
개발	▪ 추가요구사항 반영/ 패턴분석 및 변경관리/ 테스트 결과반영/ 개발일정관리
품질혁신 (QA)	▪ 산출물과 품질기준 검토 및 품질관리 기준 설정 ▪ 표준화가 필요한 업무에 대하여 프로세스 및 정보항목 도출 ▪ 표준화 추진방안 제시

03. 기술지원 및 정기적 서비스

교육지원 담당자의 책임아래 교육훈련을 진행합니다.
교육준비, 교육실시, 평가 및 분석 3단계로 나누어 시행하여 훈련효과를 극대화 합니다.
훈련 후 교육내용 활용도를 조사, 부족한 부분을 추가 교육하여 시스템 적응력과 운용능력을 극대화 합니다.

교육훈련 일정

교육과정	주요내용	교육일정	교육대상	관련자료/장소
기초교육	▪ 솔루션 사용법 – 사용자 환경설정 및 접속방법 – 로그조회 등 감사활동 방법 ▪ 솔루션 개념 및 구축 기법 ▪ 솔루션 시스템 운영 및 활용 방안 ▪ 집합교육	▪ 영업일 기준 1일 (2시간 소요) (프로젝트 초기: M) – 계약 후 4개월 이내	▪ 총괄 담당 직원	▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 기본 교육	▪ 솔루션의 운영관리 – 시스템 운영환경(H/W및 S/W)에 대한 이해 – 솔루션 운영교육 – 보안규칙 적용방법 – 모니터링 및 감사활동 방법 ▪ 운영 지침 ▪ 시스템 전반적인 이해 ▪ 각 모듈 별 요소 기술 ▪ 보안관리자 ▪ 매뉴얼 사용 방법 ▪ 집합교육 또는 쿠폰	▪ 영업일 기준 5일 (일 1시간) (솔루션 설치 완료시: M+1) – 계약 후 5개월 이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정 장소
시스템 운영자 심화 교육	▪ 운영단계에서 실제 운영 시 상세 제품교육 ▪ 보고서 활용 관련 리포트 활용법 ▪ 집합교육 또는 쿠폰	▪ 영업일 기준 1일 (3시간 소요) (시스템 안정화 단계시: M+2) – 계약 후 6개월 이내	▪ 총괄 담당 직원	▪ 사용자 매뉴얼 ▪ 운영자 매뉴얼 ▪ 소만사 자체 자료 ▪ 장소: 고객사 지정장소

03. 기술지원 및 정기적 서비스

제안사의 운영기술지원 서비스는 다음과 같이 5개 영역으로 나뉘어 제공됩니다.

유지관리 정책은 검수 후 1년간 무상 지원되며, 이후 별도의 유지관리 계약을 통해서 지속적인 서비스를 제공합니다.

운영기술지원 서비스

구 분	지원 방안	비고
예방정비 (PM)	• 전담 A/S 요원 정기점검 및 요청 시 방문 • 모듈 및 시스템 성능 검사 및 종합 테스트 • 정기적인 이론 실습 교육 • 전산 마인드 교육 • 업무시스템의 효율적인 사용을 위한 교육	• 전담 요원 확보 • 충분한 예비 시스템 확보
긴급정비 (EM)	• 유지관리를 위한 전담 엔지니어 확보 • Help Desk 운영을 통한 신속 정확한 장애 조치 • Diagnostic Program을 통한 정확한 고장부위 파악 및 조치	• 4시간 이내 착수하여 조치 이행
서비스망 접수처리	• Help Desk를 구축 신속한 장애 접수 처리	• 상시 지원 체제 구축
기술지원	• Version Upgrade 관련 최신 기술정보 제공 • 대상 업무 검토 및 협의 • 시스템 성능향상을 위한 기술자문 및 신기술 세미나	• 유지관리 전담팀 활용
무상유지관리 기간	• 시스템 구축 후 1년	

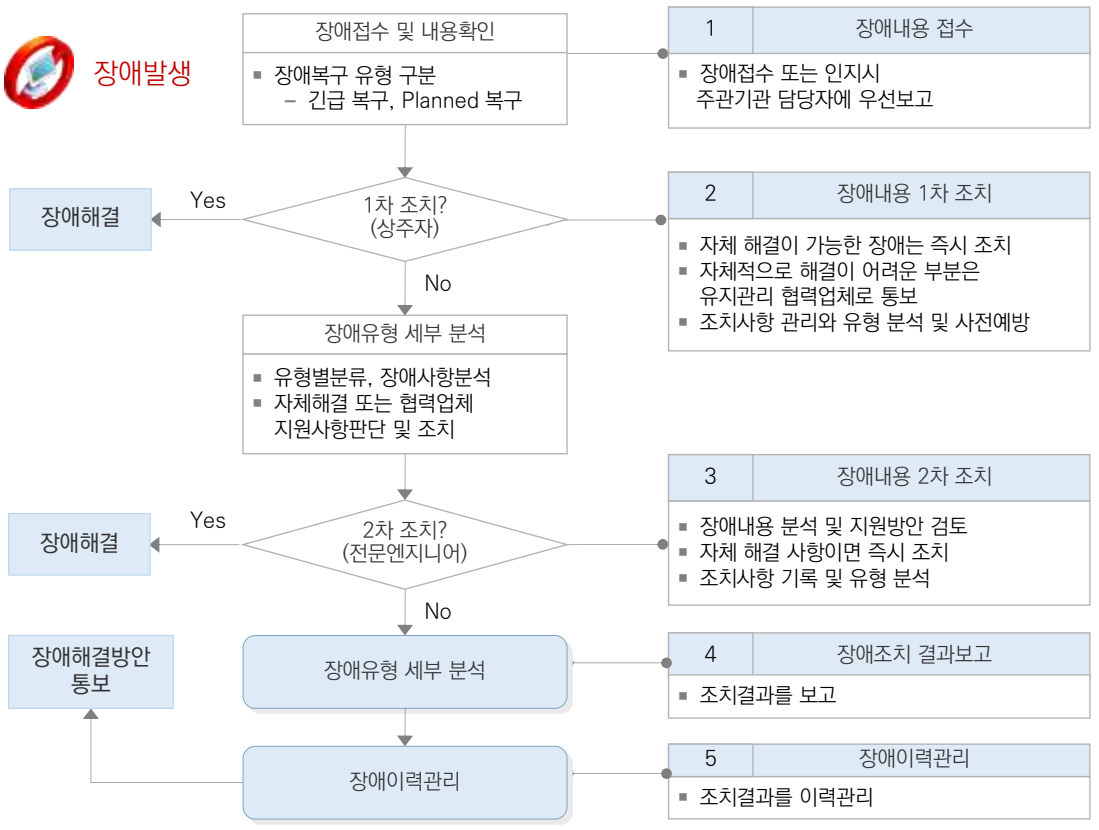
03. 기술지원 및 정기적 서비스

1,000여개 유지관리 사이트 지원경험과 200여명의 전문가를 통한 대응체계를 고객에게 제공합니다

03. 기술지원 및 정기적 서비스

제안사 기술컨설팅 단일창구를 통해 장애접수 후
유지관리팀 및 주관기관 내 자체 운영조직에 의한 해결 또는 협력업체 현장방문으로 신속히 장애문제를 조치합니다

절차에 의한 체계적이고 신속한 장애처리



장애복구 유형별 조치방안

구분	내용	조치 담당자	비고
긴급 복구	장애요소제거 및 교체	유지관리 담당자	유지관리 수행팀은 전단계에 걸쳐 지속적인 지원
	시스템 (HW 및 SW) 가동	시스템 및 SW 운영자	
	서비스 가동 및 확인	업무담당자	
Planned 복구	복구작업 계획수립	관련자 전체	
	서비스 및 시스템 중지	업무담당자, 시스템 및 SW 운영자	
	장애요소 제거 및 교체	유지관리 담당자	
	시스템 및 서비스 가동, 확인	시스템 및 SW 운영자, 업무담당자	

유해 & 악성코드 배포사이트 차단

WebKeeper SG

SECURE WEB GATEWAY

성공적인 프로젝트로 보답하겠습니다

감사합니다

SOMANSA

서울특별시 영등포구 영신로 220 KnK디지털타워 9층 소만사
대표번호 : 02-2636-8300 | 기술문의 : tech@somansa.com
제품구매 : 02-2655-4040 / sales@somansa.com